Integrations in Engineering and Technology
Online ISSN: XXXX-XXXX
An Online, Peer-Reviewed, Refereed, Open Access Journal

Review Article

COGNITIVE-INSPIRED EXPLAINABLE MACHINE LEARNING: ADVANCING HUMAN-CENTRIC, TRUSTWORTHY, AND PREDICTIVE ARTIFICIAL INTELLIGENCE-A COMPREHENSIVE REVIEW

G ASHOK

Assitant Professor, Departmnet of Mathematics, Adikavi Nannaya University, Rajahmanudry, India

***CORRESPONDING AUTHOR**
G Ashok

ARTICLE HISTORY: 24.03.2026 RECEIVED: 14.04.2026 REVISED: ACCEPTED: 03.05.2026

ABSTRACT
The rapid advancement of quantum computing and artificial intelligence (AI) is fundamentally transforming the cybersecurity landscape, creating unprecedented opportunities as well as critical threats to modern cryptographic infrastructures. Conventional cryptographic algorithms such as Rivest–Shamir–Adleman (RSA), Elliptic Curve Cryptography (ECC), and Diffie–Hellman are increasingly vulnerable to quantum-enabled attacks, particularly through Shor's and Grover's algorithms, which threaten the confidentiality, integrity, and authenticity of digital communication systems. Simultaneously, the proliferation of blockchain technologies and Internet of Things (IoT) ecosystems has expanded the attack surface of cyber-physical environments, necessitating intelligent and quantum-resistant security mechanisms. This review article comprehensively investigates the convergence of AI-assisted post-quantum cryptography (PQC), blockchain security, and IoT protection frameworks within emerging quantum-safe architectures. The paper critically analyzes the evolution of classical and post-quantum cryptographic algorithms, including lattice-based, code-based, hash-based, multivariate, and isogeny-based schemes standardized by the National Institute of Standards and Technology (NIST). Furthermore, the study explores the role of AI and machine learning in cryptanalysis, anomaly detection, adaptive authentication, automated threat intelligence, and intelligent defense orchestration. Special emphasis is placed on lightweight PQC techniques suitable for resource-constrained IoT environments and quantum-resistant blockchain infrastructures employing zero-knowledge proofs and decentralized trust mechanisms. The article also identifies major research gaps, scalability challenges, interoperability limitations, privacy concerns, and future opportunities associated with intelligent quantum-safe ecosystems. Finally, the review presents future research directions involving 6G security, federated learning, homomorphic encryption, quantum internet architectures, and self-adaptive cryptographic systems for next-generation cybersecurity resilience.
Keywords: *Post-Quantum Cryptography, Artificial Intelligence, Blockchain Security, Internet of Things (IoT), Quantum-Safe Architecture, Cryptanalysis.*

1. INTRODUCTION

The digital transformation of modern society has significantly increased dependence on secure communication systems, distributed computing environments, and interconnected cyber-physical infrastructures. Over the last three decades, cryptography has played a central role in ensuring confidentiality, integrity, authentication, and non-repudiation across digital platforms [1]. Traditional cryptographic systems such as RSA, Advanced Encryption Standard (AES), Diffie–Hellman key exchange, and Elliptic Curve Cryptography (ECC) have formed the foundation of secure internet communications, financial systems, e-governance platforms, military networks, healthcare infrastructures, and industrial automation systems [2].

However, the emergence of quantum computing introduces severe challenges to classical cryptographic assumptions. Quantum computers exploit quantum mechanical principles such as superposition and entanglement to solve computationally intensive problems significantly faster than classical computers [3]. In particular, Shor's algorithm demonstrates the ability to

efficiently factor large integers and compute discrete logarithms, thereby compromising RSA and ECC-based systems [4]. Grover's algorithm further reduces the effective security strength of symmetric cryptographic algorithms by accelerating brute-force attacks [5].

Simultaneously, the rapid adoption of blockchain technology and IoT ecosystems has generated complex cybersecurity concerns. Blockchain networks rely heavily on asymmetric cryptographic primitives for transaction validation, wallet authentication, and decentralized consensus [6]. Quantum attacks against blockchain infrastructures may lead to large-scale compromise of digital assets, smart contracts, and decentralized finance ecosystems [7]. Similarly, IoT systems consist of billions of interconnected resource-constrained devices vulnerable to cyberattacks, unauthorized access, identity theft, and data manipulation [8].

Artificial Intelligence (AI) has emerged as both a cybersecurity enabler and a potential threat amplifier. Machine learning and deep learning techniques are increasingly employed for intrusion detection, malware analysis, adaptive authentication, behavioral analytics, and predictive threat intelligence [9]. Conversely, AI-assisted cryptanalysis and automated attack generation have raised serious concerns regarding the resilience of existing cryptographic systems [10].

The convergence of AI, post-quantum cryptography, blockchain security, and IoT protection has therefore become an urgent research priority. Intelligent quantum-safe architectures capable of adaptive defense, lightweight encryption, scalable authentication, and automated anomaly detection are essential for securing next-generation digital ecosystems [11].

This review article aims to provide a comprehensive analysis of AI-assisted post-quantum cryptographic systems for blockchain and IoT applications. The primary objectives of this paper are as follows:

1. To analyze the evolution of classical and post-quantum cryptographic systems.
2. To investigate the role of AI in cryptanalysis and intelligent cybersecurity.
3. To evaluate quantum threats against blockchain and IoT infrastructures.
4. To explore lightweight quantum-resistant architectures for resource-constrained environments.
5. To identify research gaps, implementation challenges, and future directions for intelligent quantum-safe systems.

The major contributions of this review include:

- A unified analysis of AI, PQC, blockchain, and IoT security.
- Comparative evaluation of post-quantum cryptographic algorithms.
- Investigation of AI-driven cryptanalysis and defense mechanisms.
- Identification of emerging threats and intelligent mitigation strategies.
- Presentation of future research opportunities in quantum-safe cybersecurity.

2. FUNDAMENTALS OF CRYPTOGRAPHY

Cryptography refers to the science of securing communication and information through mathematical transformations and computational mechanisms [12]. It enables secure data transmission over insecure channels by converting plaintext into unintelligible ciphertext accessible only to authorized entities possessing cryptographic keys.

Cryptographic systems are broadly classified into:

- Symmetric cryptography
- Asymmetric cryptography
- Hash functions
- Digital signatures
- Cryptographic protocols

2.1 Symmetric Cryptography

Symmetric encryption employs a single shared secret key for both encryption and decryption processes [13]. These algorithms are computationally efficient and suitable for high-speed communication systems.

Common symmetric algorithms include:

- AES
- DES
- Triple DES
- Blowfish
- ChaCha20

AES remains one of the most widely adopted symmetric encryption standards globally due to its high efficiency and resistance to classical attacks [14].

Advantages of Symmetric Cryptography

- Fast computation
- Low computational overhead
- Suitable for large-volume data encryption

Limitations

- Key distribution challenges
- Scalability issues in large networks
- Vulnerability to brute-force attacks under quantum environments

Grover's algorithm significantly impacts symmetric cryptography by effectively reducing the security strength of cryptographic keys by half [15].

2.2 Asymmetric Cryptography

Asymmetric cryptography utilizes a pair of mathematically related keys:

- Public key
- Private key

The public key is openly distributed, while the private key remains confidential [16].

Popular asymmetric algorithms include:

- RSA
- ECC
- Diffie–Hellman
- ElGamal

RSA security depends on the computational difficulty of prime factorization.

The RSA mathematical relationship is represented as:

c=memodnc = m^e \bmod nc=memodn

where:

- mmm = plaintext
- ccc = ciphertext
- eee = public exponent
- nnn = modulus

ECC provides equivalent security using smaller key sizes compared to RSA, making it suitable for mobile and IoT environments [17].

However, Shor's quantum algorithm threatens both RSA and ECC by enabling polynomial-time factorization and discrete logarithm computation [18].

2.3 Hash Functions

Hash functions generate fixed-length outputs from arbitrary input data [19]. They ensure:

- Data integrity
- Password security
- Blockchain immutability

Common hash algorithms include:

- SHA-256
- SHA-3
- BLAKE2
- Whirlpool

Blockchain technologies heavily depend on cryptographic hash functions for linking blocks and maintaining decentralized trust [20].

2.4 Digital Signatures

Digital signatures provide:

- Authentication
- Integrity verification
- Non-repudiation

RSA and ECC-based digital signature schemes are widely implemented in secure communication systems [21].

The basic digital signature process includes:

1. Message hashing
2. Signature generation using private key
3. Signature verification using public key

Quantum computing poses substantial risks to current digital signature infrastructures [22].

Table 01: Comparison of Classical Cryptographic Techniques

Cryptographic Method	Key Type	Security Basis	Advantages	Limitations
AES	Symmetric	Substitution-Permutation	Fast and efficient	Vulnerable to Grover's algorithm
RSA	Asymmetric	Integer Factorization	Strong authentication	Vulnerable to Shor's algorithm
ECC	Asymmetric	Elliptic Curve Discrete Logarithm	Small key sizes	Quantum vulnerable
SHA-256	Hash Function	One-way transformation	Integrity protection	Collision concerns under quantum attacks

Table 01 illustrates the fundamental differences between major classical cryptographic techniques and their vulnerabilities under quantum computing environments.

2.5 Cryptographic Protocols

Cryptographic protocols define secure communication procedures between entities [23]. Examples include:

- TLS/SSL
- IPSec
- Kerberos
- SSH

These protocols integrate encryption, authentication, and key exchange mechanisms to establish secure channels over public networks.

Modern cybersecurity infrastructures increasingly require quantum-safe cryptographic protocols capable of resisting future quantum attacks [24].

Classical Cryptography → Public-Key Cryptography → Blockchain Security

↓

Quantum Computing Threats

↓

Post-Quantum Cryptography + AI Security

Figure 01: Evolution of Cryptographic Systems

Figure 01 depicts the evolutionary transition from classical cryptography toward intelligent quantum-safe security architectures.

3. POST-QUANTUM CRYPTOGRAPHY (PQC)

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to resist attacks from both classical and quantum computers [25]. Unlike quantum cryptography, PQC can operate on classical hardware infrastructures while providing security against quantum adversaries.

3. POST-QUANTUM CRYPTOGRAPHY (PQC)

Post-Quantum Cryptography (PQC) has emerged as one of the most critical research domains in modern cybersecurity due to the anticipated capabilities of large-scale quantum computers [25]. Conventional public-key cryptographic systems such as RSA, ECC, and Diffie-Hellman rely on mathematical problems that can be efficiently solved using quantum algorithms, rendering current security infrastructures vulnerable [26]. Consequently, governments, industries, financial institutions, healthcare organizations, and cloud service providers are actively exploring quantum-resistant cryptographic mechanisms.

The objective of PQC is to develop algorithms that:

- Resist quantum attacks,
- Operate efficiently on classical hardware,
- Maintain interoperability with existing digital infrastructures,
- Support scalable deployment across heterogeneous environments.

The National Institute of Standards and Technology (NIST) initiated the Post-Quantum Cryptography Standardization Project to identify secure and efficient quantum-resistant algorithms for future deployment.

3.1 Quantum Threats to Classical Cryptography

Quantum computing fundamentally alters computational complexity assumptions underlying modern cryptography.

Two major quantum algorithms threaten existing systems:

3.1.1 Shor's Algorithm

N=p×qN = p \times qN=p×q

Shor's algorithm efficiently factors large integers and computes discrete logarithms in polynomial time [26]. As shown above, RSA security depends on the difficulty of factoring NNN into prime factors ppp and qqq. Quantum computation breaks this assumption.

Impacted systems include:

- RSA
- ECC
- Diffie–Hellman
- DSA

Shor's algorithm directly threatens:

- Secure web communication,
- Blockchain wallets,
- Digital certificates,
- VPN infrastructures,
- National security systems.

3.1.2 Grover's Algorithm

Grover's algorithm accelerates brute-force search processes.

The effective complexity reduction is represented as:

O(2n)→O(2n/2)O(2^n) \rightarrow O(2^{n/2})O(2n)→O(2n/2)

This impacts symmetric algorithms such as AES and hash functions by reducing their effective security levels.

For example:

- AES-128 security becomes approximately equivalent to 64-bit security under Grover's attack.

However, symmetric cryptography remains comparatively more resilient than public-key systems because security can be increased through larger key sizes. Figure 02: Quantum Threat Model Against Classical Cryptography

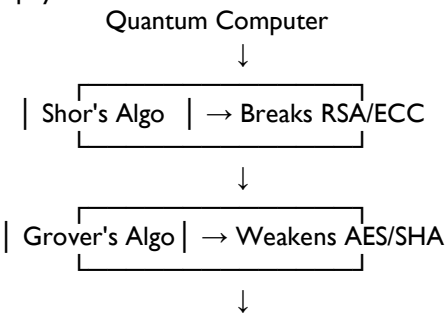

Figure 02 depicts the primary quantum algorithms responsible for compromising classical cryptographic systems.

3.2 NIST Post-Quantum Standardization

NIST launched its PQC standardization initiative in 2016 to identify practical quantum-resistant algorithms suitable for global adoption [27].

After multiple evaluation rounds, NIST selected several algorithms for standardization based on:

- Security,
- Performance,
- Scalability,
- Implementation efficiency,
- Resistance to cryptanalysis.

The primary selected algorithms include:

- CRYSTALS-Kyber
- CRYSTALS-Dilithium
- Falcon
- SPHINCS+

Table 02: NIST-Selected Post-Quantum Cryptographic Algorithms

Algorithm	Category	Purpose	Security Foundation	Advantages
CRYSTALS-Kyber	Lattice-based	Key Encapsulation	Learning With Errors (LWE)	Efficient and scalable
CRYSTALS-Dilithium	Lattice-based	Digital Signatures	Module-LWE	High security and speed
Falcon	Lattice-	Digital	NTRU	Compact

	based	Signatures	lattices	signatures
SPHINCS+	Hash-based	Digital Signatures	Hash trees	Conservative security

Table 02 summarizes the major post-quantum algorithms selected by NIST for future quantum-safe deployments.

3.3 Lattice-Based Cryptography

Lattice-based cryptography is currently the most promising PQC category due to its strong security proofs and computational efficiency.

Its security depends on hard mathematical problems such as:

- Shortest Vector Problem (SVP)
- Learning With Errors (LWE)
- Ring-LWE
- Module-LWE

The Learning With Errors problem is mathematically represented as:

b=As+eb = As + eb=As+e

where:

- AAA = random matrix,
- sss = secret vector,
- eee = error term,
- bbb = generated output.

The intentional inclusion of small error values makes solving the equation computationally infeasible even for quantum adversaries [28].

Advantages

- Strong quantum resistance,
- Efficient implementation,
- Suitable for IoT environments,
- Parallelizable computations.

Limitations

- Large public key sizes,
- Memory overhead,
- Complex implementation requirements.

Lattice-based systems are increasingly integrated into:

- Secure cloud systems,
- Blockchain architectures,
- 6G communication frameworks,
- IoT ecosystems.

3.4 Code-Based Cryptography

Code-based cryptography derives security from the difficulty of decoding random linear error-correcting codes.

The most notable example is:

- McEliece cryptosystem.

Advantages

- Long history of cryptanalytic resistance,
- High security confidence.

Limitations

- Extremely large key sizes,
- Storage inefficiency,
- Limited applicability in constrained environments.

Despite storage challenges, code-based cryptography remains highly resilient against known quantum attacks [35].

3.5 Hash-Based Cryptography

Hash-based cryptography relies on the security of cryptographic hash functions [29].

Popular schemes include:

- XMSS,
- LMS,
- SPHINCS+.

Hash-based digital signatures utilize Merkle tree structures for secure authentication.

Advantages

- Minimal mathematical assumptions,
- Strong theoretical security,
- Long-term cryptographic resilience.

Limitations

- Large signature sizes,
- Computational overhead,
- State management complexity.

Hash-based cryptography is particularly attractive for:

- Firmware authentication,
- Government systems,
- Long-term archival protection.

3.6 Multivariate Cryptography

Multivariate cryptography is based on solving systems of multivariate polynomial equations over finite fields [37].

General form:

Pi(x1,x2,...,xn)=0P_i(x_1,x_2,...,x_n)=0Pi(x1,x2,...,xn)=0

where:

- PiP_iPi represents multivariate polynomial equations.

Advantages

- Fast signature generation,
- Efficient verification.

Challenges

- Large public keys,
- Structural weaknesses discovered in some schemes.

Several multivariate schemes were eliminated during NIST evaluations due to successful cryptanalytic attacks.

3.7 Isogeny-Based Cryptography

Isogeny-based cryptography utilizes mathematical mappings between elliptic curves [30].

The most well-known approach:

- Supersingular Isogeny Key Encapsulation (SIKE).

Advantages

- Extremely compact key sizes,
- Efficient communication overhead.

Limitations

- High computational complexity,
- Recent cryptanalytic vulnerabilities.

Recent attacks against SIKE highlighted the difficulty of balancing security and efficiency in isogeny-based systems.

3.8 Hybrid Cryptographic Architectures

Transitioning directly from classical cryptography to PQC poses substantial operational risks. Consequently, hybrid cryptographic architectures combine:

- Classical cryptography,
- Post-quantum algorithms.

Example:

- RSA + Kyber
- ECC + Dilithium

Hybrid systems provide:

- Backward compatibility,
- Gradual migration,
- Enhanced operational resilience.

However, hybrid implementations also introduce:

- Increased computational complexity,
- Communication overhead,
- Key management challenges.

3.9 Challenges in PQC Deployment

Despite significant progress, several barriers hinder widespread PQC adoption:

3.9.1 Computational Overhead

PQC algorithms often require:

- Larger keys,
- Increased memory usage,
- Higher processing power.

3.9.2 IoT Limitations

Resource-constrained IoT devices struggle with:

- Energy consumption,
- Storage limitations,
- Real-time processing constraints.

3.9.3 Interoperability

Integrating PQC into existing infrastructures remains difficult due to compatibility issues with:

- TLS,
- VPN systems,
- Legacy hardware,
- Embedded systems.

3.9.4 Standardization Delays

Global adoption requires:

- Regulatory consensus,
- Vendor compatibility,
- Secure implementation guidelines.

Table 03: Comparative Analysis of PQC Categories

PQC Category	Security Level	Key Size	Computational Cost	IoT Suitability
Lattice-based	High	Medium	Moderate	High
Code-based	Very High	Very Large	Moderate	Low
Hash-based	High	Large Signature	High	Moderate
Multivariate	Moderate	Large	Low	Moderate
Isogeny-based	Moderate	Small	Very High	Low

Table 03 compares the security and implementation characteristics of major PQC categories.

3.10 Future Directions in PQC

Future PQC research focuses on:

- Lightweight quantum-safe encryption,
- AI-assisted cryptographic optimization,
- Quantum-safe blockchain systems,
- Secure 6G communication,
- Quantum internet security.

Emerging trends include:

- Adaptive cryptography,
- Self-healing cryptographic infrastructures,
- AI-driven key management,
- Homomorphic encryption integration.

The next section explores the role of Artificial Intelligence in cryptography and cybersecurity systems.

4. ARTIFICIAL INTELLIGENCE IN CRYPTOGRAPHY

Artificial Intelligence (AI) has become a transformative force in cybersecurity and cryptography by enabling intelligent automation, adaptive decision-making, predictive analytics, and real-time threat detection. The integration of AI into cryptographic systems has significantly enhanced defensive capabilities; however, it has simultaneously introduced sophisticated attack vectors powered by machine learning and deep neural networks [31].

The convergence of AI and cryptography is now reshaping:

- Cryptanalysis,
- Intrusion detection systems,
- Behavioral authentication,
- Malware analysis,
- Threat intelligence,
- Blockchain security,
- Quantum-safe communication infrastructures.

AI-driven cybersecurity frameworks are especially important in large-scale distributed systems such as:

- Smart cities,
- Cloud computing,
- Industrial IoT,
- Autonomous vehicles,
- Healthcare systems,
- Decentralized finance ecosystems.

4.1 Artificial Intelligence Fundamentals in Cybersecurity

Artificial Intelligence refers to computational systems capable of simulating intelligent human behavior, including:

- Learning,
- Reasoning,
- Pattern recognition,
- Decision-making,
- Adaptation.

AI technologies relevant to cybersecurity include:

- Machine Learning (ML),
- Deep Learning (DL),
- Reinforcement Learning,
- Natural Language Processing,
- Generative AI.

Machine learning systems are categorized into:

1. Supervised learning,
2. Unsupervised learning,
3. Reinforcement learning.

These AI techniques enable automated identification of anomalous activities, malicious behaviors, and network intrusions.

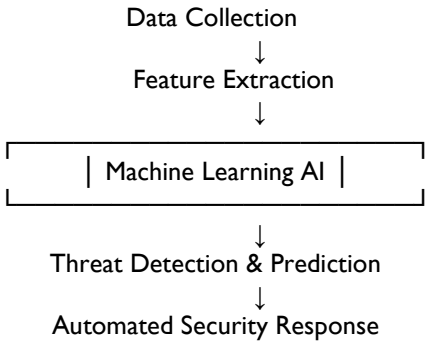

Figure 04: AI-Driven Cybersecurity Architecture

Figure 04 depicts the general architecture of AI-assisted cybersecurity systems.

4.2 AI-Assisted Cryptanalysis

Cryptanalysis refers to techniques used to compromise cryptographic systems without direct access to secret keys [45].

AI-assisted cryptanalysis leverages:

- Neural networks,
- Deep learning,
- Evolutionary algorithms,
- Pattern recognition models.

These systems can identify hidden relationships and statistical weaknesses within encrypted datasets more efficiently than conventional methods.

Applications of AI in Cryptanalysis

- Ciphertext pattern analysis,
- Side-channel attack enhancement,
- Password prediction,
- Key recovery,
- Traffic analysis,
- Differential cryptanalysis automation.

Deep learning models can analyze massive encrypted datasets to infer hidden structures and cryptographic vulnerabilities [46].

4.3 Machine Learning-Based Side-Channel Attacks

Side-channel attacks exploit physical leakage generated during cryptographic operations, including:

- Power consumption,
- Electromagnetic emissions,
- Timing information,
- Acoustic signals.

Machine learning significantly improves side-channel attack efficiency by automatically identifying hidden leakage patterns [32].

Common ML algorithms used include:

- Support Vector Machines (SVM),
- Random Forests,
- Convolutional Neural Networks (CNN),
- Recurrent Neural Networks (RNN).

Table 04: AI Techniques Used in Cryptanalysis

AI Technique	Application Area	Advantages	Limitations
CNN	Side-channel analysis	High pattern recognition	Computationally intensive
RNN	Sequential attack modeling	Temporal learning capability	Training complexity
SVM	Key classification	High accuracy	Scalability limitations
Reinforcement Learning	Adaptive attacks	Dynamic optimization	Requires extensive training

Table 04 summarizes major AI techniques utilized in modern cryptanalysis frameworks.

4.4 Deep Learning for Intrusion Detection Systems

Intrusion Detection Systems (IDS) monitor networks and systems for malicious activities [33]. Traditional IDS approaches often suffer from:

- High false positives,
- Limited scalability,
- Inability to detect zero-day attacks.

Deep learning-based IDS architectures provide:

- Automated feature extraction,
- Real-time analysis,
- Adaptive learning,
- Improved anomaly detection.

Popular deep learning models include:

- CNNs,
- Long Short-Term Memory (LSTM),
- Autoencoders,
- Generative Adversarial Networks (GANs).

LSTM models are particularly effective for sequential network traffic analysis due to their memory capabilities [49].

4.5 Neural Cryptography

Neural cryptography explores the use of neural networks for secure key generation and synchronization [34].

In neural cryptographic systems:

- Two neural networks synchronize through mutual learning,
- Shared secret keys are generated dynamically,
- Eavesdroppers struggle to reproduce synchronization behavior.

Neural synchronization models include:

- Tree Parity Machines,
- Feedforward neural architectures,
- Chaotic neural systems.

Advantages

- Adaptive key generation,
- Dynamic security,
- Resistance to certain brute-force attacks.

Challenges

- Synchronization delays,
- Training instability,
- AI-based attack vulnerability.

4.6 AI-Driven Threat Intelligence

Threat intelligence involves collecting, analyzing, and interpreting cyber threat information.

AI-driven threat intelligence systems utilize:

- Big data analytics,
- Natural language processing,
- Behavioral analytics,
- Real-time monitoring.

These systems can:

- Predict attacks,
- Identify malware families,
- Detect phishing campaigns,
- Correlate distributed attack patterns.

AI-powered Security Information and Event Management (SIEM) systems improve response efficiency through automated threat prioritization.

4.7 Explainable AI in Cybersecurity

Explainable Artificial Intelligence (XAI) addresses transparency and interpretability challenges associated with complex AI models.

In cybersecurity applications, explainability is essential because:

- Security decisions require accountability,
- Analysts must understand AI reasoning,
- Regulatory compliance demands transparency.

XAI techniques include:

- SHAP values,
- LIME,
- Attention visualization,
- Rule extraction.

Explainable systems improve trust and operational acceptance of AI-driven security mechanisms.

4.8 Adversarial AI Attacks

Adversarial AI attacks manipulate machine learning systems using carefully crafted malicious inputs.

Examples include:

- Adversarial malware,
- Poisoned training datasets,
- Evasion attacks,
- Model inversion attacks.

Attackers can exploit AI systems to:

- Evade intrusion detection,
- Manipulate authentication systems,
- Corrupt behavioral analysis models.

Table 05: Adversarial AI Threats in Cybersecurity

Attack Type	Description	Impact
Evasion Attack	Manipulates inputs to bypass AI detection	IDS failure
Poisoning Attack	Corrupts training data	Model degradation
Model Inversion	Extracts sensitive training information	Privacy breach
Adversarial Examples	Small perturbations fool AI systems	Misclassification

Table 05 presents major adversarial AI attack categories affecting intelligent cybersecurity infrastructures.

4.9 Generative AI and Cybersecurity Risks

Generative AI technologies such as large language models and GANs have introduced new cybersecurity challenges [35].

Potential malicious applications include:

- Automated phishing generation,
- Deepfake impersonation,
- AI-generated malware,
- Automated vulnerability discovery,
- Synthetic social engineering attacks.

AI-generated cyberattacks exhibit:

- High scalability,
- Adaptive behavior,
- Human-like deception capabilities.

Conversely, generative AI can also support:

- Malware analysis,
- Threat simulation,
- Security training,

- Vulnerability assessment.

4.10 AI for Blockchain Security

AI enhances blockchain security through:

- Fraud detection,
- Smart contract auditing,
- Transaction anomaly analysis,
- Consensus optimization.

Machine learning models analyze blockchain transaction patterns to identify:

- Money laundering,
- Fraudulent wallets,
- Sybil attacks,
- Double-spending attempts.

AI-powered smart contract analysis tools can automatically detect vulnerabilities such as:

- Reentrancy attacks,
- Integer overflow,
- Logic flaws.

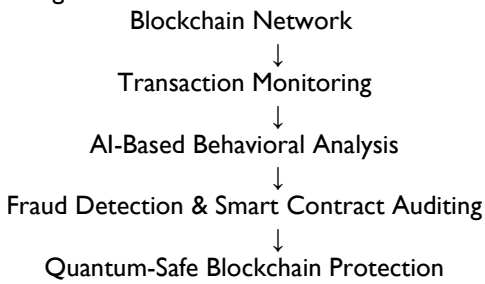

Figure 06: illustrates the integration of AI within blockchain security architectures.

Figure 06: AI-Integrated Blockchain Security Framework

4.11 AI for IoT Security

IoT systems generate enormous volumes of heterogeneous and real-time data. AI improves IoT security through:

- Device behavior analysis,
- Botnet detection,
- Network traffic monitoring,
- Predictive maintenance,
- Intelligent authentication.

Machine learning-based IoT defense mechanisms can identify:

- Abnormal communication patterns,
- Unauthorized access attempts,
- Device hijacking,
- Distributed denial-of-service attacks.

Edge AI architectures further enable localized threat analysis with reduced latency [36-37].

4.12 Federated Learning and Privacy Preservation

Federated Learning (FL) enables decentralized AI training without transferring raw data to centralized servers [38]. The federated learning objective function is represented as:

F(w)=∑k=1KnknFk(w)F(w)=\sum_{k=1}^{K} \frac{n_k}{n} F_k(w)F(w)=∑k=1KnnkFk(w)

where:

- F(w)F(w)F(w) = global optimization objective,
- Fk(w)F_k(w)Fk(w) = local model objective,
- nkn_knk = local dataset size.

Federated learning improves:

- Data privacy,
- Scalability,
- Regulatory compliance.

However, federated systems remain vulnerable to:

- Model poisoning attacks,
- Inference attacks,
- Communication leakage.

Combining federated learning with:

- Homomorphic encryption,
- Secure multi-party computation,
- Differential privacy, significantly improves security [39-4].

4.13 AI Challenges in Cryptography

Despite its advantages, AI integration introduces several concerns:

4.13.1 Data Dependency

AI systems require large training datasets that may contain:

- Biases,
- Incomplete information,
- Security vulnerabilities.

4.13.2 Computational Complexity

Deep learning systems require:

- High-performance GPUs,
- Large memory resources,
- Extensive training time.

4.13.3 Privacy Concerns

Sensitive cybersecurity data may be exposed during:

- AI training,
- Data aggregation,
- Collaborative learning.

4.13.4 Explainability Limitations

Black-box AI models reduce transparency and trustworthiness in critical security systems.

Table 06: Benefits and Challenges of AI in Cryptography

Benefits	Challenges
Automated threat detection	High computational overhead
Adaptive defense systems	Adversarial AI attacks
Intelligent anomaly detection	Data privacy concerns
Predictive cybersecurity	Explainability limitations
Real-time analytics	Training complexity

Table 06 summarizes the major advantages and limitations associated with AI-assisted cryptographic systems.

4.14 Future Directions of AI in Cryptography

Future AI-driven cryptographic systems are expected to include:

- Self-adaptive encryption,
- Autonomous security orchestration,
- AI-assisted PQC optimization,
- Intelligent blockchain governance,
- Quantum-aware threat prediction.

Emerging research areas include:

- Explainable AI for cryptographic decision-making,
- Federated cybersecurity architectures,
- AI-driven zero-trust frameworks,
- Autonomous quantum-safe infrastructures.

The next section examines blockchain security challenges and quantum-safe architectures in decentralized systems.

5. CONCLUSION

This review has examined AI-assisted post-quantum cryptography (PQC) in blockchain and IoT systems, emphasizing the urgent need to develop quantum-resistant security frameworks for next-generation digital infrastructures. The rapid progress of quantum computing poses a serious threat to conventional cryptographic algorithms such as RSA, ECC, and Diffie–Hellman, making the transition toward post-quantum solutions essential for long-term security. Post-quantum cryptographic approaches, particularly lattice-based schemes, have emerged as strong candidates due to their robustness and suitability for standardization efforts. These techniques provide a foundation for securing communications against both classical and quantum attacks. Artificial intelligence enhances cybersecurity by enabling adaptive and predictive defense mechanisms, improving capabilities in intrusion detection, anomaly detection, and automated threat response. However, AI systems also introduce new risks, including adversarial manipulation and model-based attacks, which must be carefully managed. In blockchain and IoT environments, the integration of AI with post-quantum cryptography strengthens system resilience by enabling intelligent threat detection, dynamic key management, and lightweight security solutions suitable for resource-constrained devices. Despite these advancements, challenges such as computational overhead, scalability limitations, interoperability issues, and the lack of global implementation standards remain significant barriers. Overall, the convergence of AI, post-quantum cryptography, blockchain, and IoT represents a promising pathway toward building secure, adaptive, and quantum-resistant digital infrastructures for the future.

6. REFERENCES

1. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science; 1994. p. 124-34.
2. Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing; 1996. p. 212-19.
3. National Institute of Standards and Technology. Post-Quantum Cryptography Standardization Project [Internet]. Gaithersburg (MD): NIST; 2024 [cited 2026 May 24]. Available from: https://csrc.nist.gov/projects/post-quantum-cryptography
4. Bernstein DJ, Buchmann J, Dahmen E, editors. Post-quantum cryptography. Berlin: Springer; 2009.
5. Chen L, Jordan S, Liu YK, Moody D, Peralta R, Perlner R, et al. Report on post-quantum cryptography. Gaithersburg (MD): National Institute of Standards and Technology; 2016. Report No.: NISTIR 8105.
6. Katz J, Lindell Y. Introduction to modern cryptography. 3rd ed. Boca Raton (FL): CRC Press; 2020.
7. Stallings W. Cryptography and network security. 8th ed. Harlow: Pearson; 2022.
8. Paar C, Pelzl J. Understanding cryptography. Berlin: Springer; 2010.
9. Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theory. 1976;22(6):644-54.
10. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120-26.
11. National Institute of Standards and Technology. FIPS 197: Advanced Encryption Standard (AES). Gaithersburg (MD): NIST; 2001.
12. National Institute of Standards and Technology. Secure Hash Standard (SHA-2). FIPS PUB 180-4. Gaithersburg (MD): NIST; 2015.
13. Merkle RC. A certified digital signature. In: Advances in Cryptology—CRYPTO '89 Proceedings; 1989. p. 218-38.
14. Boneh D, Shoup V. A graduate course in applied cryptography [Internet]. 2020 [cited 2026 May 24]. Available from: https://crypto.stanford.edu/~dabo/cryptobook/
15. Katz J, Yung M. Threshold cryptosystems. In: Advances in Cryptology; 2001.
16. Menezes AJ, van Oorschot PC, Vanstone SA. Handbook of applied cryptography. Boca Raton (FL): CRC Press; 1996.
17. Koblitz N. Elliptic curve cryptosystems. Math Comput. 1987;48(177):203-9.
18. Miller VS. Use of elliptic curves in cryptography. In: Advances in Cryptology—CRYPTO '85 Proceedings; 1985. p. 417-26.

19. National Security Agency. SHA-3 competition report. Fort Meade (MD): NSA; 2012.
20. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [Internet]. 2008 [cited 2026 May 24]. Available from: https://bitcoin.org/bitcoin.pdf
21. Wood G. Ethereum: a secure decentralised generalised transaction ledger (Ethereum Yellow Paper) [Internet]. 2014 [cited 2026 May 24]. Available from: https://ethereum.github.io/yellowpaper/paper.pdf
22. Zohar A. Bitcoin: under the hood. Commun ACM. 2015;58(9):104-13.
23. Antonopoulos AM. Mastering Bitcoin. 2nd ed. Sebastopol (CA): O'Reilly Media; 2017.
24. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access. 2016;4:2292-303.
25. Tapscott D, Tapscott A. Blockchain revolution. New York (NY): Penguin; 2016.
26. Atzori M. Blockchain technology and decentralized governance: is the state still necessary? [Internet]. 2017 [cited 2026 May 24]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713
27. Zheng Z, Xie S, Dai H, Chen X, Wang H. Blockchain challenges and opportunities: a survey. Int J Web Grid Serv. 2017;14(4):352-75.
28. Dai W. Crypto++ library documentation [Internet]. 2020 [cited 2026 May 24]. Available from: https://www.cryptopp.com/
29. Liskov M, Rivest RL. Public key cryptography standards. 2018.
30. Bernstein DJ. Introduction to post-quantum cryptography. In: Bernstein DJ, Buchmann J, Dahmen E, editors. Post-quantum cryptography. Berlin: Springer; 2009. p. 1-14.
31. Alagic G, et al. Status report on the second round of the NIST post-quantum cryptography standardization process. Gaithersburg (MD): NIST; 2022.
32. Regev O. On lattices, learning with errors, random linear codes, and cryptography. J ACM. 2009;56(6):1-40.
33. Peikert C. A decade of lattice cryptography. Found Trends Theor Comput Sci. 2016;10(4):283-424.
34. McEliece RJ. A public-key cryptosystem based on algebraic coding theory. Pasadena (CA): Jet Propulsion Laboratory; 1978.
35. Berlekamp E, McEliece R, van Tilborg H. On the inherent intractability of certain coding problems. IEEE Trans Inf Theory. 1978;24(3):384-86.
36. Damgård I. A design principle for hash functions. In: Advances in Cryptology—CRYPTO '89 Proceedings; 1989. p. 416-27.
37. Buchmann J, Ding J, editors. Post-quantum cryptography. Berlin: Springer; 2009.
38. Patarin J. Hidden field equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: Advances in Cryptology—EUROCRYPT '96 Proceedings; 1996. p. 33-48.
39. De Feo L. Mathematics of isogeny-based cryptography [Internet]. 2017 [cited 2026 May 24]. Available from: https://arxiv.org/abs/1711.04062
40. Jao D, De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Post-Quantum Cryptography. Berlin: Springer; 2011. p. 19-34.
41. Costello C, Longa P, Naehrig M. Efficient algorithms for supersingular isogeny Diffie-Hellman. In: Advances in Cryptology—CRYPTO 2016 Proceedings; 2016. p. 572-601.