IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

DOI: 10.17148/IJIREEICE.2026.14382

QUANTUM SECURE BLOCKCHAIN ARCHITECTURE

Dr. Ashwini Kumar Jha[1], Kartik Patil[2], Abhishek Patil[3], Pramod Patil[4], Shreyansh Patel[5]

Associate Professor, Department of Artificial Intelligence & Data Science, Parul University, Vadodara,Gujrat[1]

ORCID: 0000-0002-6607-21681[1]

Student, Department of B.Tech CSE-AI, Parul University, Vadodara,Gujrat[2-5]

Abstract: We live in a world where billions of devices are connected to the internet from smart home gadgets to hospital monitors to factory machines. All of these devices rely on security systems built with traditional encryption (methods for scrambling data so only the right person can read it). These encryption methods have protected us well for decades. But a new type of computer, called a quantum computer, is on the horizon and it could break most of today's encryption in a matter of seconds. That's a very serious problem.

This review paper brings together findings from several research studies to explain the problem clearly and to explore the solutions being developed. We look at how quantum computers threaten our current systems. what new types of encryption(called post-quantum cryptography, or PQC) are being created to replace them, and how blockchain technology the same technology behind cryptocurrencies can be made quantum-safe. We also explore how a technique called Quantum Key Distribution (QKD) can share secret keys in a way that is guaranteed to be safe by the laws of physics. Finally, we look at how Artificial Intelligence (AI) can both help protect systems and, in the wrong hands, help attack them. The paper ends with an honest look at what still needs to be solved and where researchers should focus their efforts next.

Keywords: Quantum Computers, Post-Quantum Cryptography (PQC),Blockchain Security, Internet of Things (IoT), Quantum Key Distribution (QKD), 6G Networks, Artificial Intelligence Security

1. INTRODUCTION

1.1 Why This Topic Matters

Think about how much of your life depends on secure internet connections your bank account, your medical records, your private messages. Now think about all the sensors, cameras, and smart devices in hospitals, power plants, and self-driving cars[1], [2]. All of these systems trust a set of mathematical "locks" to keep their data private. These locks are called encryption algorithms, and the most common ones today are RSA and ECC (Elliptic Curve Cryptography)[3], [4].They work by using very large numbers that are nearly impossible to figure out at least for a regular computer.

But quantum computers work differently. Instead of processing information one bit at a time (like a regular computer), a quantum computer can process many possibilities at once[6], [7]. A specific quantum technique called Shor's Algorithm can crack RSA and ECC encryption[8], [9].

The same way you'd easily open a lock once you know combination. Researchers estimate that a powerful enough quantum computer perhaps within the next 10–20 years could break the encryption protecting most of the world's digital infrastructure. This review paper explains this threat in simple terms and explores the best solutions researchers have developed so far.

1.2What This Paper Covers

This paper draws from several academic studies to cover five main topics: (1) understanding exactly how quantum computers threaten today's security systems[9], [10];

(2) reviewing new quantum-resistant encryption methods and how they are being built into blockchain systems[11]; (3) exploring Quantum Key Distribution (QKD), which uses physics instead of math to secure communication[6]; (4) looking at new types of blockchain designed specifically for quantum-resistant security in IoT, 6G networks, and smart vehicles[12],

[13]; and (5) examining both the benefits and dangers of using Artificial Intelligence in quantum security contexts[5].

Throughout the paper, we aim to make complex ideas easy to understand without losing their meaning[14]. Our goal is for students, engineers, policymakers, and anyone curious about the future of digital security to walk away with a clear picture of where things stand and what needs to be done[15], [16], [17].

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

DOI: 10.17148/IJIREEICE.2026.14382

2.How We Conducted This Review

Finding and Selecting the Research

To write this paper, we studied multiple academic research papers published in respected journals, including IEEE Transactions, IEEE Access, Future Generation Computer Systems, and other technology publications[4], [9], [18]. We specifically looked for papers that covered quantum threats to security systems, new

new encryption methods that can resist quantum attacks, blockchain designs that incorporate quantum safety features, and privacy-protecting tools[2], [19], [20] relevant to IoT and cloud computing .

We used a step-by-step approach (inspired by what researchers call the PRISMA method) to make sure we were thorough and fair. First, we gathered the papers. Then, we sorted them by topic[9], [10]. After that, we checked each paper for quality making sure claims were backed up with evidence or sound reasoning. Finally, we compared the findings across papers to identify patterns, agreements, and areas where more work is needed[21].

How We Organized the Information

Rather than summarizing each paper one by one, we grouped their ideas into five major themes that naturally emerged from the research[22], [24]. This way, instead of getting a list of paper summaries, you get a connected story about the entire field[1], [23]. The five themes are: the quantum threat, post-quantum encryption, quantum communication (QKD), blockchain architectures, and privacy plus AI. This structure helps readers understand how all the pieces fit together[25]. We carefully distinguished between systems that have been tested in real experiments, systems tested only in computer simulations, and systems that are still just theoretical designs on paper[10],, [27]. This distinction matters because a clever idea on paper is very different from a working prototype.

3.What the Research Tells Us Five Key Theme

Theme 1: How Quantum Computers Threaten Today's Security

The Problem with Shor's Algorithm

Today's internet security relies on the idea that certain maths problems are so hard, even the world's fastest computers would take billions of years to solve them[3], [9]. RSA encryption, for example, uses the difficulty of factoring enormous numbers (splitting a huge number into its prime components)[3]. ECC uses a related concept called the discrete logarithm[8], [19]. Both problems are genuinely impossible for classical computers to crack in reasonable time.[9], [28] Shor's Algorithm, designed specifically for quantum computers, solves both of these problems easily. When a real quantum computer is powerful enough to run Shor's Algorithm at scale, both RSA and ECC encryption will become useless overnight[3], [25]. This doesn't just affect internet browsers it threatens blockchain wallets, smart contracts, digital IDs, and any system that uses digital signatures. Every piece of data currently protected by these methods becomes vulnerable the moment such a quantum computer arrives[4], [21].

Grover's Algorithm: The Quieter Threat

A second quantum technique, Grover's Algorithm, doesn't break encryption outright but weakens it significantly. Imagine you have a padlock with a ten-digit combination. Normally, guessing it would take an enormous number of tries. Grover's Algorithm lets a quantum computer do the same job with only the square root of that num 8-bit password, this means the effective security drops to 64-bit much easier to crack. Hash functions (used in blockc in to "fingerprint" data) are particularly at risk from this attack[7], [16].Perhaps the sneakiest threat of all is something alled Store Now, Decrypt Later (SNDL)[4], [9]. This is where an attacker collects encrypted data today even without bei ; able to read it and stores it until a powerful quantum computer becomes available in the future[21], [25]. By then, th y can decrypt everything they collected[9]. This means that sensitive data encrypted today with old methods might already be at risk, even if quantum computers are still years away[4], [6]. This is why experts say we cannot afford to wait[9], [25].

AI Makes Attacks Even Harder to Stop

On top of Shor's and Grover's threats, researchers have identified a newer danger: Quantum Artificial Intelligence (Quantum AI, or QAI)[15],[17]. AI programs called Quantum Generative Adversarial Networks (QGANs) can create fake network traffic that is specifically designed to trick security systems into thinking an attack is not happening[17]. Meanwhile, AI-enhanced attacks can listen to tiny physical signals leaking from hardware (called side-channel attacks) and figure out secret keys much faster than before[16], [29]. This means future attackers won't just have quantum computers they'll have smart quantum computers that can outsmart our defenses[15], [30].

Section Summary: Quantum computers threaten today's security through three main methods: Shor's Algorithm (breaks encryption outright), Grover's Algorithm (weakens it), and the Store-Now-Decrypt-Later strategy (steals data today for future decryption)[3], [7], [9]. Quantum AI adds a further layer of threat by enabling smarter, harder-to-detect attacks[17],

Quantum Threats

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

DOI: 10.17148/IJIREEICE.2026.14382

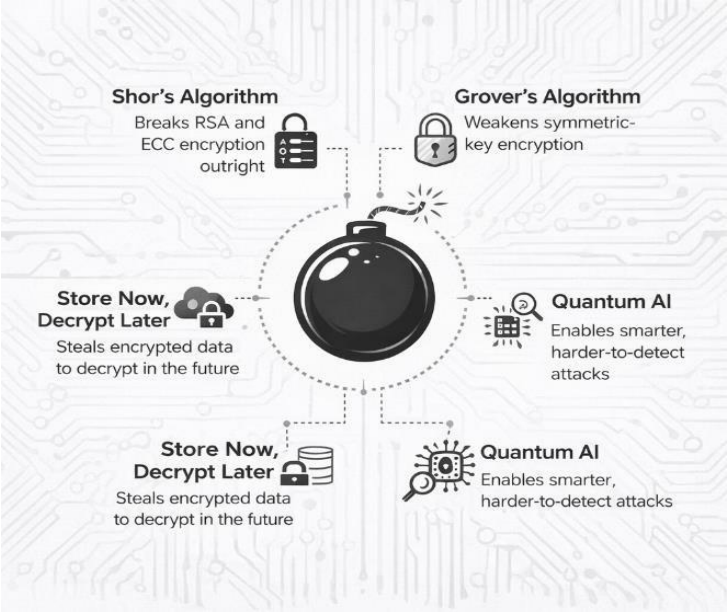


Figure 3.1

Theme 2: Post-Quantum Cryptography New Locks for a Quantum World

What Is Post-Quantum Cryptography?

Post-Quantum Cryptography, or PQC, refers to a new generation of encryption methods that even quantum computers cannot crack[3], [9], [19]. The key advantage of PQC is that these methods run on normal, everyday computers no special quantum hardware needed[2], [9]. This means they can be gradually rolled out as software updates to existing systems, making them a practical near-term solution. In 2024, the United States government body NIST (National Institute of Standards and Technology) officially approved the first set of PQC standards, which is a major milestone. The approved methods include lattice-based cryptography (which relies on mathematical problems involving complex grid structures that are hard even for quantum computers), hash-based cryptography (using layered fingerprint functions), and code-based cryptography (based on error-correcting codes from information theory)[3], [19], [31]. Each method has different strengths and trade-offs in terms of speed, key size, and security level[32], [33].

PQC Meets Blockchain: The Quantum Shield-BC Example

One of the most impressive examples from the reviewed research is Quantum Shield-BC a blockchain system redesigned from scratch using PQC instead of old encryption[25]. The system replaced the traditional digital signatures (which would be vulnerable to quantum attacks) with lattice-based PQC signatures. In tests, this redesigned blockchain processed over 7,000 transactions per second across a network of 100 computers[25]. That's significantly faster than the baseline of 3,000–4,000 transactions per second for standard blockchains, which shows that security and speed don't have to be trade-offs[2], [34], [35].

The secret to this performance is a design philosophy called crypto-agility meaning the system was built so that its cryptographic tools can be swapped out in the future without rebuilding the entire system[2], [14]. This is important because cryptographic standards will continue to evolve as quantum computers get more powerful[25]. A crypto-agile system stays relevant longer and doesn't require a costly full redesign every time standards change[11].

Adding Privacy: Zero-Knowledge Proofs and SMPC Another important research contribution found in the review is the PP-PQB framework, which adds privacy-preserving tools on top of PQC-secured blockchain[11], [36]. One of these tools is called Zero-Knowledge Proof (ZKP)[11]. Here's a simple way to understand it: imagine you want to prove to your bank that you have enough money to cover a purchase, but you don't want to reveal your exact balance[35]. ZKP lets you do exactly that prove something is true without revealing the underlying information[37]. This is incredibly useful for financial transactions, healthcare data, and anywhere else privacy matters.

Another tool is Secure Multi-Party Computation (SMPC). Suppose three hospitals want to find out if a certain drug is effective across their combined patient databases, but none of them is willing to share their patients' private data with the others. SMPC allows them to run the calculation together and get the correct[38], [39].

answer without any single hospital ever seeing the other hospitals' data. Both ZKP and SMPC are valuable complements to PQC because, while PQC protects the encryption, these tools protect the privacy of the data itself once it enters the system.

Section Summary: PQC provides new encryption methods that even quantum computers cannot crack, and they run on

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

DOI: 10.17148/IJIREEICE.2026.14382

ordinary computers. The Quantum Shield-BC system showed that a quantum-safe blockchain can be fast and practical. Privacy tools like ZKP and SMPC add an extra layer of protection for sensitive data[11], [29], [36] .

Data Security Matrix

Figure 3.2

Theme 3: Quantum Key Distribution Security Guaranteed by Physics

How QKD Works

Every encrypted communication system requires that the two parties share a secret key a piece of information used to lock and unlock the data. The challenge is: how do you share that key safely in the first place? Traditional methods involve sending the key over the internet using encryption that could, in theory, be broken. Quantum Key Distribution (QKD) solves this problem in a completely different and far more powerful way it uses the fundamental laws of quantum physics[6]. The most widely used QKD protocol is called BB84. In BB84, the secret key is encoded in individual particles of light (photons) and sent from one person to another. The magical property of quantum physics is that any attempt to intercept or copy a quantum particle inevitably disturbs it and this disturbance is detectable[6]. So if an eavesdropper tries to spy on the key exchange, both parties immediately know about it and can discard that key and try again. This makes QKD theoretically unbreakable[40] not because the maths is hard, but because the laws of physics make undetected eavesdropping impossible.

Beyond Key Sharing: QSDC and Quantum Consensus The research also introduces an advanced of QKD called Quantum Secure Direct Communication (QSDC)[33], [41]. While QKD only distributes keys (which are then used to encrypt separate messages), QSDC sends the actual message directly through quantum channels that are making the entire communication process quantum-safe from end to end[41]. This eliminates the separate step of key management, which is itself a potential weak point[2], [14]. In blockchain systems, decisions about which transactions are valid are made through a process called consensus[25]. A new quantum consensus mechanism called Proof-of-Quantum Key Stake (PoQKS) has been proposed, which uses QSDC to make the consensus process both more secure and more energy-efficient than the Proof-of-Work method used by Bitcoin[33]. Alongside this, a tool called Quantum Random Number Generation (QRNG) uses true quantum randomness (generated from quantum physical processes, not predictable computer formulas) to select blockchain validators making it impossible for attackers to predict or manipulate[6] who gets chosen.

QKD's Practical Challenges

Despite its theoretical perfection, QKD faces real-world challenges. The hardware is expensive and specialised, requiring quantum optical components. Signals weaken over distance in optical fibre, which limits how far a QKD link can reach without special repeaters. Environmental noise can disrupt the fragile quantum signals[7]. These limitations mean QKD is best suited for high-security fixed connections like between government buildings or bank headquarters rather than for millions of portable IoT devices scattered across a city[13].This is exactly why the reviewed research converges on a hybrid approach: combine PQC (cheap, software-based, runs everywhere) with QKD (expensive but physically perfect, for

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

DOI: 10.17148/IJIREEICE.2026.14382

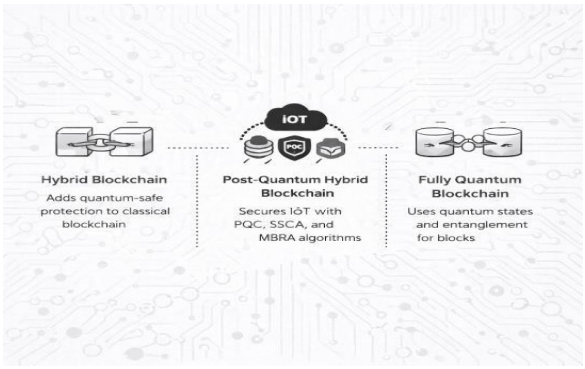
the most sensitive links). Together, they cover each other's weaknesses. PQC handles the scale; QKD handles the highest-stakes connections[9], [17], [42].

Section Summary: QKD uses quantum physics to share secret keys in a way that makes eavesdropping physically detectable. It is theoretically unbreakable but expensive and limited in range. Combining QKD with PQC gives the best of both worlds security at scale and perfect security for critical links[2], [6].

Theme 4: New Blockchain Architectures for IoT, 6G, and Smart Vehicles

Three Types of Quantum-Safe Blockchain

The reviewed research describes three architectural approaches to making blockchain quantum-safe[21], [43]. The first and most practical is the hybrid approach keeping the existing blockchain infrastructure but adding quantum protections at the communication and key management layers. The SSCA (Secure and Scalable Cloud Architecture) is a good example: IoT sensors send their data to a cloud system that encrypts it with PQC, stores it on a blockchain for tamper-proof record-keeping, and manages secret keys using an algorithm called MBRA (Multi-Blockchain Routing Algorithm). This approach can be deployed without replacing existing hardware.The second approach is the fully quantum blockchain, where the blocks themselves are made of quantum states rather than classical bits, and they are linked using quantum entanglement (a property where two particles remain connected even when far apart, so that changing one instantly affects the other)[41]. This makes the chain incredibly secure any tampering with one block .



Quantum Blockchain Types
Figure3.4

Quantum Blockchain for 6G and Autonomous Vehicles

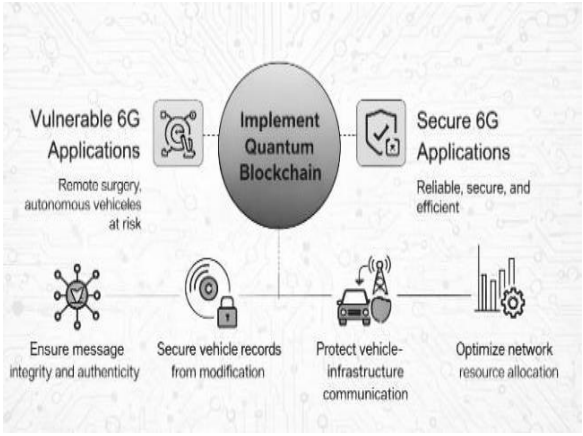
The coming generation of mobile networks, called 6G, will support applications like remote surgery, fully autonomous vehicles, and real-time holographic communication. These applications demand not just speed, but extreme reliability and security[41], [45]. A self- driving car that receives a tampered navigation command, or a robot surgeon that receives a hacked instruction, could cause loss of life. The reviewed research shows how quantum blockchain can address these challenges by providing quantum-authenticated messages, tamper-proof vehicle identity records, and quantum-secured communication between vehicles and infrastructure even in the absence of a central server. The research also introduces Quantum Reinforcement Learning a form of AI that uses quantum computation to make better decisions about how to allocate network resources (like bandwidth and processing power) in real time[46]. This technique can reduce delays and save energy in vehicular edge computing environments, where decisions need to be made in milliseconds.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

DOI: 10.17148/IJIREEICE.2026.14382



6G Security Model

Figure 3.4.1

A Shared Architecture Across All Systems

Across all the reviewed frameworks, one consistent architecture emerged, structured in four layers. The first layer is the device layer: the sensors, smart appliances, wearables, and vehicles that generate data. The second is the quantum cryptography layer: where QKD, PQC, and digital signatures protect communication[12]. The third is the blockchain layer: where data is recorded permanently and validated by a quantum-safe consensus mechanism. The fourth is the application layer: where users access data through authenticated interfaces, and where privacy tools like ZKP and SMPC enable private analytics.

This layered model is important because it shows that quantum security is not a single technology it is a complete ecosystem of tools working together. No single layer can be removed without weakening the whole system[5].

Theme 5: Protecting Privacy And the Double-Edged Sword of Quantum AI

Privacy Tools for the Quantum Age

Security is about keeping data safe from attackers. Privacy is about keeping data safe even from the systems that are supposed to be helping you. In healthcare, your test results should be accessible to your doctor but not to insurers or advertisers. In genomics (DNA research), your genetic data is uniquely sensitive because it is permanent and shared by your family members. The reviewed research highlights several tools that protect privacy in quantum-era IoT systems.

Differential privacy adds carefully calculated "noise" (random disturbances) to datasets so that individual records cannot be identified, while the overall statistical pattern remains useful[39]. Federated learning allows AI models to be trained across many hospitals or devices without the raw data ever leaving those devices only the learned patterns are shared[18]. Together with ZKP, SMPC, and blockchain-based consent management[2] (where patients control who can access their data via a transparent ledger), these tools create a comprehensive privacy framework that goes beyond just encrypting communications.

Quantum AI: A Powerful Defender

One of the most exciting findings in the reviewed research is the use of Quantum Support Vector Machines (QSVMs) a type of AI powered by quantum computation for detecting cyber attacks. In tests, a QSVM-based intrusion detection system achieved 98% accuracy in identifying attacks, compared to 89% for traditional AI systems[15].

impressively, the false alarm rate dropped from 6% to just 2%. This means fewer legitimate users get incorrectly blocked, and fewer real attacks slip through. The quantum advantage comes from the AI's ability to analyse a much larger "feature space" essentially, it can consider many more patterns simultaneously.

Quantum AI also improves QKD itself[46]. A technique called quantum reinforcement learning can continuously tune the QKD system to work better in noisy or changing environments, generating more usable secret keys per second. And continuous anomaly detection on quantum randomness generators ensures that the randomness they produce has not been compromised, providing an extra layer of integrity checking.

Quantum AI: Also a Powerful Attacker

Here is the uncomfortable truth the research makes clear: the same quantum AI capabilities that defenders can use, attackers canuse too[15]. Quantum Generative Adversarial Networks (QGANs) can generate fake network traffic that is designed specifically to fool quantum-enhanced security systems[15]. Traditional AI-powered attacks can already learn

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

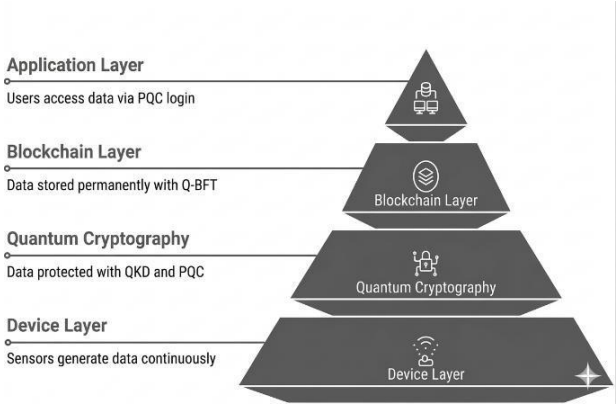
DOI: 10.17148/IJIREEICE.2026.14382

to mimic normal behaviour to avoid detection; quantum AI makes this evasion dramatically more effective. Meanwhile, quantum-enhanced side- channel attacks can extract secret information from the tiny physical signals emitted by hardware (heat, electromagnetic radiation, power fluctuations) with far fewer measurements than before. This creates what researchers call an arms race dynamic: as defensive systems become smarter using quantum AI, offensive systems become smarter too, using the same tools. The reviewed frameworks have not yet fully resolved this challenge[47]. The most promising defensive responses include using a combination of quantum and classical AI detectors (so that evading one doesn't guarantee evading the other), continuously retraining detection systems on new attack patterns, and using physical-level quantum measurements that attackers cannot replicate from the software layer.

2. *Diagrams: Visual Explanations*

Figure 1: How a Quantum-Secure IoT System Is Structured (Four Layers)

Imagine the security system as a building with four floors. Each floor has a specific job, and they all work together to keep data safe from the moment it is created to the moment it reaches the user.



IoT Security Architecture

Figure 4.1

1. The Device Layer (Bottom): This is where data is born. Sensors in a factory, health monitors on a patient's wrist, cameras in a smart city, or sensors in an autonomous vehicle all of these generate data continuously. These devices communicate using either quantum-secured channels (where hardware allows) or PQC-encrypted connections[2], [5].
2. The Quantum Cryptography Layer: Before data moves anywhere, it is protected here. QKD is used for the most sensitive links (like between hospitals or government systems). PQC encryption is used everywhere else. A Quantum Random Number Generator ensures that all secret keys are genuinely random and unpredictable. Quantum digital signatures prove that data came from the right source[6], [19].
3. The Blockchain Layer: Once data is secured, it is stored here permanently. The blockchain keeps an uneditable record of every transaction and data entry. The Q-BFT consensus mechanism (using true quantum randomness to select validators) ensures no one can cheat the system. Every block in the chain is linked using quantum hashing, making tampering immediately obvious[13], [25].
4. The Application/Cloud Layer (Top): This is where users and organisations access the data. Access is controlled through PQC-secured login systems. Homomorphic encryption and SMPC allow analysis of sensitive data without ever exposing the raw information. Zero-Knowledge Proofs allow users to verify their credentials without revealing them. Blockchain-based consent management gives individuals control over their own data[11], [18].

The key insight from this diagram is that quantum security is not just about changing one thing it requires all four layers to be protected[12]. A chain is only as strong as its weakest link.

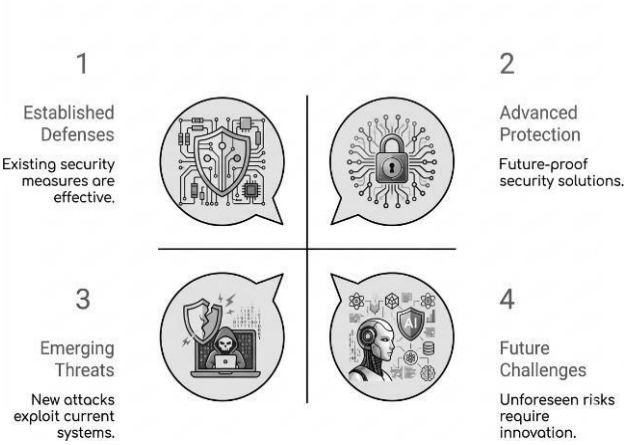
Figure 2: The Threat Landscape and How We Fight It

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

DOI: 10.17148/IJIREEICE.2026.14382



Security Framework

Figure4.2

This diagram organises all the attacks identified in the research into four groups, and maps each group to the defences designed to stop them. Think of it as a battlefield map.

1. Quantum Cryptanalytic Attacks (Breaking Encryption): Shor's Algorithm and Grover's Algorithm attack the mathematical foundations of encryption. These are countered by PQC signatures and key exchange, and by QKD for sharing keys through quantum physics instead of maths[9].

2.Network Attacks (Interception and Impersonation): Man-in-the-Middle attacks (where someone intercepts your message), Replay attacks (where old messages are resent to trick the system), and impersonation attacks are countered by QKD (which makes eavesdropping detectable), quantum digital signatures, and timestamped authentication sessions[48].

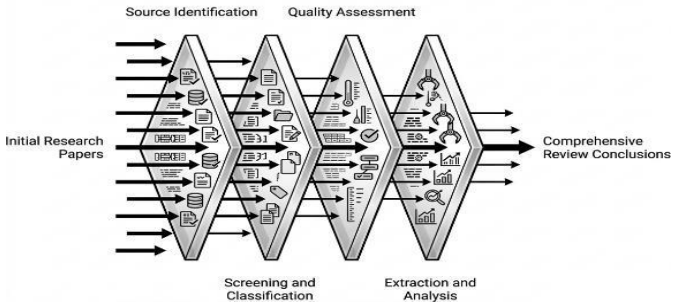
3.Blockchain-Specific Attacks (Cheating the System): A 51% attack (where someone takes control of the majority of a blockchain network to reverse transactions) and double-spending (spending the same digital currency twice) are countered by the Q-BFT consensus mechanism and quantum digital signatures on every transaction[21], [25].

4.AI-Powered Attacks (The Evolving Frontier): QGAN-generated fake traffic and AI- enhanced side-channel attacks are the most difficult to counter. The best current defences combine quantum and classical AI detectors (ensemble detection), continuous retraining on new attack patterns, and physical-layer quantum monitoring that attackers cannot manipulate from the software side. This group represents the most significant remaining challenge[29].

The critical lesson from this diagram is that Group D attacks are only partially addressed by current systems. This is the area where future research is most urgently needed[15].

Figure 3: How We Conducted This Review (Step by Step)

This diagram shows the four-step process used to produce this review similar to a cooking recipe, where



Review Process

Figure 4.3

Step 1: Find the Ingredients (Source Identification): We searched for research papers from respected journals covering quantum cryptography, blockchain security, IoT protection, and related topics. Search terms included 'quantum blockchain,' 'post-quantum cryptography IoT,' '6G quantum security,' and 'quantum AI security[1].'

DOI: 10.17148/IJIREEICE.2026.14382

Step 2 : Sort and Check (Screening and Classification): Each paper was evaluated to confirm it contained genuine technical substance. Papers were then grouped into five thematic categories corresponding to the five themes in Section 3 of this paper[12].

Step 3 : Test for Quality (Assessment): We assessed whether each paper's claims were backed by experiments, simulations, or sound theoretical argument. We noted the maturity level (theoretical, simulation, prototype, or production-ready) as this directly affects how much confidence we can place in the results[2].

Step 4 : Compare and Synthesise (Extraction and Analysis): Key findings from all papers were extracted and placed into comparison tables. Patterns were identified where papers agreed, where they disagreed, and where there were obvious gaps[9]. This synthesis forms the basis of Sections 3, 4, 7, and 8 of this paper.

This structured approach helps ensure that the conclusions of this review are based on a fair and complete reading of the available research, rather than selective[9].

4.Discussion What Does It All Mean?

4.1Why Combining PQC and QKD Is the Smartest Approach

The clearest finding across all the research is this: no single security tool is enough[25]. QKD is theoretically perfect, but it requires expensive hardware and can only work over limited distances[6]. PQC works on any computer and can be deployed in software, but it rests on mathematical assumptions that might however unlikely be proven wrong in the future[9]. Blockchain provides a tamper-proof record and distributed trust, but it needs both QKD and PQC to protect its underlying cryptographic operations[21], [49]. None of these works alone. Together, they create a defence-in-depth strategy where breaking one layer does not compromise the whole system[9], [25].

The crypto-agility principle adds a crucial dimension: build your system so you can swap out the cryptographic tools without rebuilding everything from scratch[2]. Given that PQC standards only started being finalised in 2024, and that both quantum computing capabilities and cryptographic research are advancing rapidly, any system built today must be designed to evolve[9]. A system locked into a single cryptographic approach even a one risks becoming obsolete in five to ten years.

4.2AI Security: The New Arms Race

The dual use of Quantum AI is one of the most thought-provoking findings in this review. On one side, QSVM-based intrusion detection dramatically outperforms classical systems 98% accuracy versus 89%[15]. On the other side, QGAN-based adversarial traffic generation can potentially defeat those very same systems[15]. This is not just a theoretical concern: as quantum computers become more accessible, both defenders and attackers will have access to the same quantum AI tools[15].

Current security frameworks are not yet fully prepared for this reality. Most systems are designed with fixed attack models in mind they're built to stop specific known attacks. But Quantum AI attackers are adaptive they learn and evolve. The solution is not to build a bigger wall, but to build a system that learns as fast as the attackers do. Ensemble detection (using multiple independent AI systems simultaneously), continuous adversarial retraining, and physical-layer quantum anomaly detection (which detects threats at the quantum channel level, beyond the reach of software-based attackers) are the most promising directions identified in the research[29].

4.3The IoT Dilemma: Too Much Security for Small Devices

Here is a frustrating paradox the research reveals: the IoT devices most in need of strong securityare often the least capable of running it[5]. A tiny environmental sensor in a factory might have a weak processor and a small battery[50]. Installing a full lattice-based PQC signature scheme might drain its battery in hours or crash its processor altogether. Yet this sensor might be part of a critical industrial control network where a security breach could cause a physical disaster.

This challenge called the lightweight security problem is one of the most important unsolved problems in the field[2]. Possible solutions being explored include stripped-down versions of PQC algorithms that trade some security margin for much lower computational cost, hierarchical architectures where small IoT devices communicate with more powerful gateway nodes that handle the heavy cryptographic lifting, and co-designed hardware and software where PQC acceleration is built directly into the IoT chip. None of these approaches is fully mature yet[2], [24].

4.4 The Privacy-vs-Permanence Problem Blockchain's immutability the fact that once data is written to a blockchain it cannot be deleted is both its greatest strength and a legal liability [35]. The European Union's General Data Protection Regulation (GDPR) gives individuals the right to have their personal data erased[35]. How do you erase data from a system specifically designed to prevent erasure?

The reviewed research does not fully resolve this tension, but it points to some partial solutions: storing only cryptographic commitments (fingerprints) on the blockchain and keeping actual personal data off-chain with proper erasure rights; using ZKP-based selective disclosure (revealing only what is necessary); and developing redactable blockchain systems that allow special deletion operations with appropriate governance controls. Each solution involves

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

DOI: 10.17148/IJIREEICE.2026.14382

trade-offs, and this remains an open research question at the intersection of law, ethics, and computer science.

5 .What Still Needs to Be Done Research Gaps and Future Directions

5.1.Lightweight Algorithms for Small Devices

The most urgent practical challenge is developing quantum-resistant encryption methods that work on small, battery-powered IoT devices[2]. Current PQC algorithms were designed for general-purpose computers and are too heavy for many IoT applications[50]. Researchers need to create slimmer versions of these algorithms or entirely new approaches that provide adequate quantum resistance without requiring excessive processing power or energy[2]. This work needs to be done urgently, given how rapidly IoT adoption is growing across hospitals, factories, and smart cities[5].

5.2More Real-World Testing

A striking gap in the current research is the lack of real-world performance data[9]. Most proposed frameworks have been evaluated only through simulation or theoretical analysis[1]. We need actual pilot deployments in hospitals, power grids, autonomous vehicle networks, and other critical environments where these systems can be tested under realistic conditions[41]. Only then can we know for certain whether they will perform as expected when it actually matters[9].

5.3 Formal Security Proofs for Quantum Consensus

New consensus mechanisms like Q-BFT are very promising, but they have not yet been formally proven secure against adversaries equipped with quantum AI[25]. Formal security **proofs are mathematical guarantees they don't just say 'we** think this is secure,' they prove it cannot be broken under specific, clearly stated assumptions[9]. This kind of rigorous validati is essential before these systems can be trusted with critical applications[25].

5.4 Standardized Performance Benchmarks

Right now, different research teams test their systems in different ways, making it impossible to directly compare results. One paper might measure throughput using 10 nodes while another uses 100. One might run its tests on high-end servers while another uses consumer hardware[26]. The field needs agreed-upon benchmarking standards like standardised test networks, traffic models, and reporting formats so that results from different research groups can be fairly compared and progress can be tracked over time[9].

5.5 Solving the Blockchain-Privacy-Regulation Conflict

As discussed in the previous section, the conflict between blockchain's permanent record-keeping and data privacy laws like GDPR is a real and unresolved problem. Research is needed into privacy

-preserving on-chain data models technical approaches that reconcile immutability with individuals' legal rights to have their data deleted[11]. This requires collaboration between technologists, lawyers, and ethicists not just computer scientists[46].

5.6 Quantum AI Arms Race Preparedness

Given that Quantum AI will be accessible to both defenders and attackers, security systems must be specifically designed to anticipate adaptive, learning-enabled adversaries[15]. This means studying how QGAN- based attacks evolve over time, developing defences that combine multiple AI systems (so fooling one does not fool all), and building systems that automatically retrain and adapt as attack patterns change. This is an active and urgent research frontier[15], [29].

5.7 Quantum-Secure Privacy-Preserving AI (Federated Learning)

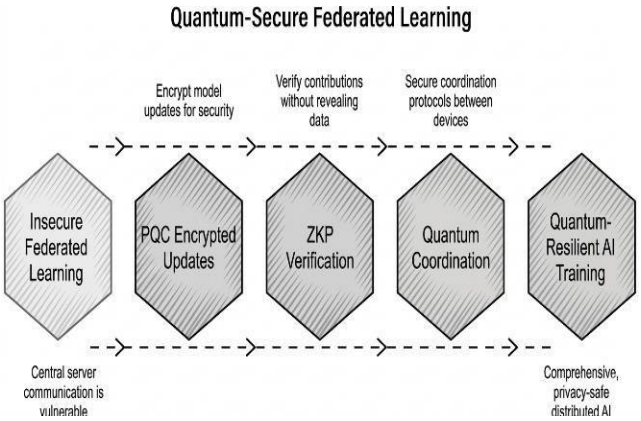
Finally, federated learning where AI models are trained across many devices without centralizing data is a powerful privacy tool[12]. But the communication between devices and the central server still needs to be quantum-secured[9]. Research into combining PQC-encrypted model updates, ZKP-based verification of contributions, and quantum-secured coordination protocols would create a comprehensive, privacy-safe, quantum-resilient distributed AI training framework[28]. This could transform healthcare, finance, and industrial analytics[9], [11].

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

DOI: 10.17148/IJIREEICE.2026.14382



Quantum Safe AI Training Model
Figure 5.7

7. Performance and Security Comparison.

TABLE 1

ANALYSIS OF QUANTUM-SECURE BLOCKCHAIN FRAMEWORKS

Source	Focus	Security Mechanisms	Target Domain	Key Outcomes
[41], [48]	Threat Identification; Blockchain Design	Dilithium, Kyber, SPHINCS+	6G, V2X, IoT	Designed a hybrid classical–quantum secure blockchain architecture
[21]	Secure IoT; AI Integration	QKD, PQC, Q-BFT, QRNG, QSVM	IoT, Healthcare	Achieved 7000+ TPS with 98% threat detection accuracy
[11]	Cloud Security; Privacy Protection	PQC, ZKP, SMPC, QKD	Cloud, Finance	Developed SSCA architecture for enhanced data secure cloud operations.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

DOI: 10.17148/IJIREEICE.2026.14382

TABLE 2
SECURITY EVALUATION OF BLOCKCHAIN FRAMEWORKS AGAINST VARIOUS ATTACKS

Attack Type	Traditional Blockchain	QKD Only	PQC Only	Hybrid (QKD+PQC)	Full Quantum
Shor [8]	Vulnerable	Protected	Protected	Protected	Protected
Grover [9]	Vulnerable	Partial	Partial	Protected	Protected
SNDL [6]	Vulnerable	Protected	Partial	Protected	Protected
MITM [46]	Partial	Protected	Partial	Protected	Protected
Replay [27]	Partial	Partial	Partial	Protected	Protected
51% Attack [51]	Partial	Resistant	Partial	Protected	Resistant

TABLE 3
COMPARISON OF CRYPTOGRAPHIC TOOLS FOR QUANTUM-SECURE BLOCKCHAIN SYSTEMS

Tool	Core Mechanism	Quantum Safe	Primary Use	Key Strength	Primary Weakness
RSA [8]	Integer factorization	No	Digital signatures	High computational efficiency	Vulnerable to Shor's algorithm
QKD [6], [33]	Photon-based key distribution	Yes	Secure key exchange	Information-theoretic security	Requires specialized quantum hardware
Lattice-based PQC [19]	Shortest vector problem	Yes	Encryption, authentication	NIST standardization support	Large key sizes
Quantum Hash [32]	Quantum-resistant hashing	Yes	Data integrity	Strong tamper resistance	Lack of standardization

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2026

DOI: 10.17148/IJIREEICE.2026.14382

Zero-Knowledge Proof (ZKP) [11]	Knowledge verification without disclosure	Yes	Privacy preservation	Zero data leakage	High computational overhead
Homomorphic Encryption (HE) [11]	Computation on encrypted data	Yes	Secure data processing	Enables privacy-preserving computation	Very high computational cost

TABLE 4

PERFORMANCE AND EVALUATION COMPARISON OF QUANTUM-SECURE BLOCKCHAIN SYSTEMS

System	Architecture	Speed (TPS)	Accuracy	False Rate	Evaluation Environment and Research Stage
SSCA [2]	Cloud-based secure architecture	N/A	N/A	N/A	Simulation; design phase
QuantumShield [4], [19]	Hybrid quantum-secure blockchain	7000+	N/A	N/A	Real-world laboratory prototype
PP-PQB [11]	Privacy-preserving blockchain framework	N/A	N/A	N/A	Analytical review; theoretical model
QSVM [15]	Quantum machine learning model	N/A	98%	2%	Research dataset; near-real deployment
Standard Blockchain [4]	Classical blockchain system	3000–4000	89%	6%	Benchmark testing; production-level
Full Quantum [9]	Fully quantum blockchain model	Unknown	N/A	N/A	Theoretical model; early-stage concept

DOI: 10.17148/IJIREEICE.2026.14382

CONCLUSION

Quantum computers are not just a futuristic concept they represent a genuine and coming threat to the security systems that protect our digital world today. The reviewed research makes this abundantly clear. Traditional encryption methods like RSA and ECC will be broken by quantum algorithms. Blockchain systems that rely on those methods will become vulnerable. The personal, financial, and safety-critical data they protect will be at risk. And waiting until quantum computers actually arrive to start preparing is not an option because some attackers may already be collecting data today to decrypt later.

The good news is that the research community is responding. Post-Quantum Cryptography (PQC) has been standardised and can be deployed today. Quantum Key Distribution (QKD) offers physically guaranteed security for the most critical communication links. New blockchain architectures like QuantumShield-BC show that quantum-safe systems can be fast and efficient. Privacy tools like Zero-Knowledge Proofs, SMPC, and federated learning protect sensitive data even inside secure systems. And Quantum AI, used wisely, can dramatically improve our ability to detect and respond to attacks.

However, the research also shows that much work remains. Lightweight algorithms for small IoT devices don't yet fully exist. Real-world deployments are rare. Formal security proofs for new consensus mechanisms are incomplete. The Quantum AI arms race is accelerating. And the conflict between blockchain's permanence and individuals' privacy rights has not been resolved. These are the frontiers that researchers, engineers, and policymakers must tackle together urgently, and with collaboration across disciplines.

In short: the quantum threat is real, the solutions are promising, and the window of opportunity to act before quantum computers arrive is narrowing. The four key lessons from this review are: (1) combine PQC and QKD neither alone is sufficient; (2) build for adaptability your security must be able to evolve as quickly as threats do; (3) take Quantum AI seriously on both sides of the security equation; and (4) close the gap between theory and practice through real-world testing and standardised evaluation. The future of digital security depends on getting these things right.

REFERENCES

[1] A. K. Jha, M. P. Patel, and T. D. Pawar, "Computation offloading using K-nearest neighbour time critical optimisation algorithm in fog computing," *Int. J. Wirel. Mob. Comput.*, vol. 23, no. 3–4, pp. 281–292, 2022, doi: 10.1504/IJWMC.2022.127593.

[2] R. R. Irshad *et al.*, "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing," *IEEE Access*, vol. 11, pp. 105479–105498, 2023, doi: 10.1109/ACCESS.2023.3318755.

[3] E. Fathalla and M. Azab, "Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations," *IEEE Access*, vol. 12, pp. 175969–175987, 2024, doi: 10.1109/ACCESS.2024.3485602.

[4] Y. Baseri, A. Hafid, Y. Shahsavari, D. Makrakis, and H. Khodaiemehr, "Blockchain Security Risk Assessment in Quantum Era, Migration Strategies, and Proactive Defense," *IEEE Commun. Surv. Tutor.*, vol. 28, pp. 2925–2964, 2026, doi: 10.1109/COMST.2025.3621113.

[5] A. Attkan and V. Ranga, "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security," *Complex Intell. Syst.*, vol. 8, no. 4, pp. 3559–3591, Aug. 2022, doi: 10.1007/s40747-022-00667-z.

[6] S. Bajrić, "Enabling Secure and Trustworthy Quantum Networks: Current State-of-the-Art, Key Challenges, and Potential Solutions," *IEEE Access*, vol. 11, pp. 128801–128809, 2023, doi: 10.1109/ACCESS.2023.3333020.

[7] A. Andreou, C. X. Mavromoustakis, G. Mastorakis, A. Bourdena, and E. K. Markakis, "Quantum Computing in Semantic Communications: Overcoming Optimization Challenges With High-Dimensional Hilbert Spaces," *IEEE Access*, vol. 13, pp. 157942–157964, 2025, doi: 10.1109/ACCESS.2025.3603338.

[8] V. Puneyani and K. V. Bhat, "Quantum-Resistant Blockchain Protocols for Secure Transactions," *IEEE Access*, vol. 13, pp. 108984–108991, 2025, doi: 10.1109/ACCESS.2025.3581955.

[9] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020, doi: 10.1109/ACCESS.2020.2968985.

[10] Taylor and Francis Group, "QBUILD: Quantum-Resistant Blockchain Architecture for Secure Supply Chains," *J.*

DOI: 10.17148/IJIREEICE.2026.14382

Appl. Artif. Intell., 2026.

[11] B. Bugra Sezer, S. Akleylek, and U. Nuriyev, "PP-PQB: Privacy-Preserving in Post-Quantum Blockchain-Based Systems: A Systematization of Knowledge," *IEEE Access*, vol. 13, pp. 41382–41405, 2025, doi: 10.1109/ACCESS.2025.3545943.

[12] M. S. Peelam, V. Chamola, and B. Sikdar, "Enhancing Security Using Quantum Blockchain in Consumer IoT Networks," *IEEE Trans. Consum. Electron.*, vol. 71, no. 2, pp. 4819–4837, May 2025, doi: 10.1109/TCE.2024.3512791.

[13] M. Wazid, A. K. Das, and Y. Park, "Generic Quantum Blockchain-Envisioned Security Framework for IoT Environment: Architecture, Security Benefits and Future Research," *IEEE Open J. Comput. Soc.*, vol. 5, pp. 248–267, 2024, doi: 10.1109/OJCS.2024.3397307.

[14] R. Vadisetty and others, "AI-Driven Post-Quantum Cryptographic Key Management Techniques," *IEEE Trans. Inf. Forensics Secur.*, 2025.

[15] M. T. Gençoğlu, "Quantum artificial intelligence and cryptographic security from a quantum cryptography perspective," *Discov. Quantum Sci.*, vol. 2, no. 1, p. 4, Feb. 2026, doi: 10.1007/s44464-026-00008-w.

[16] S. I. Ali, G. P. Kale, M. S. Shaikh, S. Ponnusamy, and P. S. Chouhan, "AI Applications and Digital Twin Technology Have the Ability to Completely Transform the Future," in *Harnessing AI and Digital Twin Technologies in Businesses*, IGI Global, 2024, pp. 26–39. doi: 10.4018/979-8-3693-3234-4.ch003.

[17] D. Gowda and others, "Robust Optimization Methods for Ensuring AI System Reliability in Quantum-Resistant Networks," *J. Math Optim. AI*, 2025.

[18] A. K. Jha, M. P. Patel, and T. D. Pawar, "A proposed model of computation offloading in fog environment," *Sambodhi UGC Care J.*, vol. 43, no. 03(IV), pp. 1–6, 2020.

[19] D. Chaudhary, P. Santhi, M. S. P. Durgarao, A. Padmavathi, M. Mehedi Hassan, and B. Fahad Alkhamees, "Module Lattice-Based Post Quantum Secure Blockchain Empowered Authentication Framework for Autonomous Truck Platooning," *IEEE Access*, vol. 12, pp. 105219–105233, 2024, doi: 10.1109/ACCESS.2024.3434691.

[20] S. I. Ali, B. A. Salunke, S. Salunke, P. S. Chouhan, and S. Shahane, "Decentralized Smart Grids With AI and Blockchain," in *Advancing Energy Production and Distribution With Blockchain and AI*, IGI Global, 2026, pp. 163–200. doi: 10.4018/979-8-3373-6996-9.ch006.

[21] M. Wazid, A. K. Das, and Y. Park, "Generic Quantum Blockchain-Envisioned Security Framework for IoT Environment: Architecture, Security Benefits and Future Research," *IEEE Open J. Comput. Soc.*, vol. 5, pp. 248–267, 2024, doi: 10.1109/OJCS.2024.3397307.

[22] A. K. Jha, M. P. Patel, and T. D. Pawar, "Fog offloading: Review, research opportunity and challenges," in *Proceedings of the International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2019, pp. 1224–1227. doi: 10.1109/ICSSIT46314.2019.8987905.

[23] A. K. Jha, M. P. Patel, and T. D. Pawar, "Extended hybrid cluster algorithm for computation offloading in fog computing," *Int. J. Tech. Phys. Probl. Eng.*, vol. 14, no. 2, pp. 176–182, 2022.

[24] S. I. Ali, H. K. Ravuri, V. T. Lakshmi, A. Ramya, K. Lavanya, and S. Bahade, "The role of nanomaterials in the development of high-performance batteries," *Nanotechnol. Percept.*, vol. 20, no. S11, pp. 1125–1140, 2024.

[25] N. R. Reddy, S. Suryadevara, K. G. R. Reddy, R. Umamaheswari, R. Guttula, and R. Kotoju, "Quantum secured blockchain framework for enhancing post quantum data security," *Sci. Rep.*, vol. 15, no. 1, p. 31048, Aug. 2025, doi: 10.1038/s41598-025-16315-8.

[26] M. S. Shaikh, A. K. Jha, B. R. Soni, R. N. K. Patel, and D. P. M, "Flying Edge Intelligence: UAV-Driven Edge Computing for Autonomous Precision Farming," in *Proceedings of the International Conference on Emerging Technologies in Engineering Applications (ICETEA)*, 2025, pp. 1–6. doi: 10.1109/ICETEA64585.2025.11099749.

[27] M. Patel, A. Mehta, A. K. Jha, A. Patel, and A. Nayak, "A deep reinforcement prediction model for live VM migration in fog," *Int. J. Tech. Phys. Probl. Eng.*, vol. 16, no. 1, pp. 277–283, 2024.

[28] V. Soni and A. Jha, "IoT Botnet Attacks Detection Using Deep Learning Approaches: A Review," *IET Conf. Proc.*, vol. 2025, no. 7, pp. 253–260, 2025.

[29] S. I. Ali, "Algorithmic Justice: Navigating AI's Role in Cybersecurity and Legal Transformation," in *Moral and Legal Aspects of Artificial Intelligence*, IGI Global, 2026, pp. 229–264. doi: 10.4018/979-8-3373-3114-0.ch007.

[30] S. I. Ali, "Reinforcement Learning for Autonomous Optimization in Intelligent Engineering," in *AI-Driven Approaches for Fully Automated Smart Engineering*, IGI Global, 2026, pp. 313–344. doi: 10.4018/979-8-3373-4839-1.ch011.

[31] D. S. C. Putranto, R. W. Wardhani, H. T. Larasati, and H. Kim, "Space and Time-Efficient Quantum Multiplier in Post Quantum Cryptography Era," *IEEE Access*, vol. 11, pp. 21848–21862, 2023, doi: 10.1109/ACCESS.2023.3252504.

[32] K. Nilesh and P. K. Panigrahi, "Quantum Blockchain Based on Dimensional Lifting Generalized Gram-Schmidt

DOI: 10.17148/IJIREEICE.2026.14382

Procedure," *IEEE Access*, vol. 10, pp. 103212–103222, 2022, doi: 10.1109/ACCESS.2022.3208123.

[33] Z.-Z. Sun *et al.*, "Quantum Blockchain Relying on Quantum Secure Direct Communication Network," *IEEE Internet Things J.*, vol. 12, no. 10, pp. 14375–14385, May 2025, doi: 10.1109/JIOT.2025.3526443.

[34] S. I. Ali, P. T. Kalaivaani, S. Ambigaipriya, and M. D. Rafeeq, "Evaluation of AI model performance," in *Toward Artificial General Intelligence*, De Gruyter, 2023, p. 125.

[35] Y. Farooqui, S. I. Ali, K. Shekokar, P. K. Patidar, K. Bhushanwar, and P. K. Nandi, "A secure framework for decentralized digital lockers using blockchain technology," *J. Comput. Sci.*, vol. 21, no. 9, pp. 2105–2112, 2025, doi: 10.3844/jcssp.2025.2105.2112.

[36] P. Peris-Lopez and others, "PP-PQB: Privacy-Preserving in Post-Quantum Blockchain-based Systems: A Systematization of Knowledge," *ACM Comput. Surv.*, 2025.

[37] A. Mahmud and A. Abdelhadi, "Artificial Intelligence in Quantum Communications: A Comprehensive Survey," *IEEE Commun. Surv. Tutor.*, 2025.

[38] A. K. Jha and T. Pawar, "Computation Offloading for Smart Healthcare Applications," in *IoT Applications for Healthcare Systems*, Cham: Springer, 2022, pp. 121–136. doi: 10.1007/978-3-030-91096-9_7.

[39] R. Annan, J. Noland, K. Perkins, X. Yuan, K. Roy, and L. Qingge, "Genomic privacy and security in the era of artificial intelligence and quantum computing," *Discov. Comput.*, vol. 28, no. 1, p. 108, Jun. 2025, doi: 10.1007/s10791-025-09627-w.

[40] V. K. Ralegankar *et al.*, "Quantum Cryptography-as-a-Service for Secure UAV Communication: Applications, Challenges, and Case Study," *IEEE Access*, vol. 10, pp. 1475–1492, 2022, doi: 10.1109/ACCESS.2021.3138753.

[41] A. Farouk, B. K. Behera, and E. A. Ahmed, "Design and Implement a Quantum Blockchain Framework to Secure 6G Communication for Consumer Applications," *IEEE Trans. Consum. Electron.*, vol. 71, no. 3, pp. 8417–8424, Aug. 2025, doi: 10.1109/TCE.2025.3580583.

[42] Y. Wang and others, "Generative-AI, Blockchain, and Federated Learning Enabled Data Security Architecture for Metaverse on 6G," *IEEE J. Sel. Areas Commun.*, 2025.

[43] A. Gbadebo, "Quantum-Resistant Blockchain Architectures for Securing Financial Data Governance," *Int. J. Inf. Manag. Data Insights*, 2025.

[44] R. Rahmati and M. Rahmati, "AI-Powered Quantum-Resistant Blockchain for Secure Financial Transactions: A Privacy-Preserving Approach," *J. Financ. Data Sci.*, 2025.

[45] R. Shankar, I. Kumar, M. Kashyap, A. K. Jha, and B. P. Chaudhary, "A Review on NOMA scheme for emerging 6G wireless networks: State of the Art, Key Schemes, Future scope and Security Issues," *Radioelectron. Commun. Syst.*, vol. 68, no. 5, pp. 271–284, 2025, doi: 10.3103/S0735272725010017.

[46] K. Zhang, C. K. M. Lee, Y. P. Tsang, and C. H. Wu, "Variational Quantum Reinforcement Learning for Joint Resource Allocation of Blockchain-Based Vehicular Edge Computing and Quantum Internet," *IEEE Trans. Veh. Technol.*, vol. 74, no. 10, pp. 15831–15847, Oct. 2025, doi: 10.1109/TVT.2025.3568158.

[47] S. Malhotra and others, "AI-Blockchain Integration for Real-Time Cybersecurity: System Design and Evaluation," *IEEEMDPI Jt. Spec. Issue Cyber-Phys. Syst.*, 2025.

[48] S. Prajapat, P. Kumar, S. Kumar, A. K. Das, S. Shetty, and M. S. Hossain, "Designing High-Performance Identity-Based Quantum Signature Protocol With Strong Security," *IEEE Access*, vol. 12,
pp. 14647–14658, 2024, doi: 10.1109/ACCESS.2024.3355196.

[49] A. Mishra and others, "Lightweight Authentication Scheme Based on ECC and PQC for IoT-Blockchain," *IEEE Internet Things J.*, 2025.

[50] A. K. Jha, "Sensing and Supervising through IoT," *Int. J. Comput. Appl.*, vol. 152, no. 9, pp. 7–9, 2016, doi: 10.5120/ijca2016911723.

[51] A. K. Jha, A. Khatri, K. Kanda, A. Haider, and R. Shah, "A review of security, privacy, and authentication mechanisms in social media web applications," *PUXplore Multidiscip. J. Eng.*, vol. 2, no. 1, 2026, doi: 10.62373/3n8bxz70.

[52] S. I. Ali, A. Dubey, S. Salunke, B. A. Salunke, and P. N. Chopkar, "Advancing Energy Production and Distribution With Blockchain and AI," in *Advancing Energy Production and Distribution With Blockchain and AI*, IGI Global, 2026, pp. 83–112. doi: 10.4018/979-8-3373-6996-9.ch004.