IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Quantum Computing And The Future Of Cybersecurity In Industry 5.0:

Implications on RSA/ECC Encryption and Strategic Countermeasures Against Shor's Algorithm

[1]Mr. Neelotpal Dey, [2]Mr. Madhup Kumar Srivastava
[1]Head Of Department CS & TnP, [2]Assistant Professor
[1]Computer Science, [2]Physics
[1 2]Microtek Group of Institution, Varanasi, India

Abstract: Quantum computing is a breakthrough in computational science and has the potential to overcome classical computing systems in solving complex mathematical and optimization problems. The growing relevance of quantum computing is closely aligned with the shift toward Industry 5.0-a technological paradigm that emphasizes intelligent collaboration among automated systems and human decision-making. At the same time, however, this constitutes a critical cybersecurity challenge. The reliability of contemporary digital security frameworks relies fundamentally on public-key cryptosystems-RSA and ECC-which are based on the computational infeasibility of integer factorization and discrete logarithmic problems. Shor's algorithm can perform this task with incredible speed on scalable quantum processors and, when it is launched, will make such encryption mechanisms obsolete. This development puts sensitive communication, financial systems, digital identity frameworks, and blockchain infrastructures at considerable risk. Simultaneously, however, quantum computing opens new avenues for defense, such as QKD and emerging PQC schemes, which have been designed to resist quantum-driven attacks. This paper critically analyzes the dual impact of quantum computing on cybersecurity, assesses the vulnerability of RSA and ECC encryption under quantum attack conditions, and outlines strategic migration frameworks for secure adoption of quantum technologies in Industry 5.0 environments. In doing so, the study emphasizes that governments, enterprises, and technological institutions urgently need to proactively invest in quantum-resilient security infrastructures that ensure long-term data integrity and secure digital transformation.

Keywords: Quantum Computing; Cybersecurity; RSA Encryption; Elliptic Curve Cryptography; Shor's Algorithm; Post-Quantum Cryptography; Quantum Key Distribution; Industry 5.0; Cryptographic Vulnerabilities; Digital Security Framework.

I. Introduction

The global digital ecosystem is undergoing significant technological transformation driven by advancements in computation, networked systems, and intelligent automation [1]. Quantum computing is recognized as a crucial enabler of this shift due to its ability to leverage quantum mechanical principles such as superposition and entanglement to perform operations in parallel, enabling exponentially faster problem-solving compared to classical computing architectures [2]. This capability is expected to play a foundational role in Industry 5.0, where the objective is to integrate autonomous systems with human-driven innovation and real-time computational intelligence [3]. Current cybersecurity frameworks are based on public-key cryptography, mainly RSA and Elliptic Curve Cryptography (ECC), enabling secure online communication, authentication protocols, banking transactions, cloud environments, and blockchain networks. Their security is based on the impossibility of solving some mathematical problems with classical computational resources, such as large integer factorization and computation of discrete logarithms [4]. Nevertheless, owing to the discovery of quantum algorithms like Shor’s Algorithm, this system faces a serious threat because it solves such problems in polynomial time if run on sufficiently powerful quantum processors [5][6].

The impact of such a cryptographic break is huge, as has been estimated, from destroyed national security systems to worldwide leakage of personal and financial data [7]. While the risk is present, quantum computing at the same time increases cybersecurity by offering methods and technologies like QKD (Quantum Key Distribution) providing theoretically secure communications due to the laws of quantum mechanics [8]. Research in Post-Quantum Cryptography (PQC) is underway with a view to coming up with cryptography that remains secure against quantum-enabled adversaries too [9][10]. The challenge for organizations is to strategically migrate from these vulnerable classical encryption systems to quantum-resilient security architectures in preparation for Industry 5.0. Coordinated policy planning, upgrading infrastructure, training the workforce, and phased migration strategies are required for this [11][12].

II. Literature Review

Quantum computing and its security implications have been a widening area of research over the last ten years. Early foundational work by Shor showed that quantum computation could solve integer factorization and discrete logarithm problems in polynomial time, directly challenging the security basis of RSA and ECC cryptosystems [5]. This discovery initiated global research interest in the vulnerabilities of classical cryptography. Bernstein, Buchmann, and Dahmen pointed out the transition to PQC as very necessary for long-term security of data in applications ranging from national security to the protection of financial systems [9]. Chen et al. documented the rise of lattice-based, hash-based, and multivariate cryptographic systems as viable alternatives able to resist quantum attacks [10]. These works collectively highlight the urgency in developing cryptographic mechanisms that remain secure under quantum computational models. In parallel, the research on Quantum Key Distribution, driven by the BB84 protocol, came to the conclusion that secure communication could indeed be based on the very principles of quantum mechanics rather than computational difficulty [8]. Scalability challenges and infrastructure costs are the current limitations to wide industrial adoption.

Industry 5.0, as projected in European and Asian technological policy frameworks, envisages a future environment that shall be characterized by human-centric automation with real-time intelligent computing systems [3]. In such an ecosystem, cybersecurity will not be just a protective mechanism; rather, it is a structural requirement for system integrity and trust. Scholars have argued that given the maturing quantum computing landscape, parallel evolution in cybersecurity governance, risk assessment, infrastructure investment, and workforce capability are sorely needed [11][12].

Collectively, the literature points to a convergence of three strategic challenges:

1. The imminent vulnerability of RSA and ECC encryption

2. The race to develop quantum-secure cryptographic systems, and

3. The need for structured migration planning aligned with Industry 5.0 transformation.

III. Methodology / Framework

This study follows a **qualitative analytical research approach**, synthesizing theoretical models, cryptographic security principles, and strategic technological adaptation frameworks. The methodology involves three structured phases:

3.1 Phase 1: Cryptographic Vulnerability Analysis

This phase examines the mathematical foundations of RSA and ECC to evaluate the extent of vulnerability under Shor’s Algorithm and emerging quantum-capable architectures. Comparative assessment is performed using:

- Key size equivalence charts,
- Computational complexity evaluations,
- Known quantum attack feasibility thresholds.

This establishes the *risk exposure timeline* associated with cryptographic failure.

3.2 Phase 2: Defensive Capability Assessment

This phase evaluates quantum-capable cybersecurity mechanisms, focusing on:

- **Quantum Key Distribution (QKD)** as a mechanism for secure communication,
- **Post-Quantum Cryptography (PQC)** algorithms being standardized by major international bodies (e.g., NIST),
- Industry case studies demonstrating early-stage adoption.

The intention is to analyse feasibility, performance implications, and scalability constraints.

3.3 Phase 3: Strategic Adoption Framework for Industry 5.0

This phase leads to the formulation of a **Quantum-Secure Transformation Roadmap**, which includes:

1. **Risk Identification and Prioritization** (systems most vulnerable to cryptographic failure),
2. **Infrastructure Upgrade Planning** (hardware and software transition pathways),
3. **Hybrid Cryptographic Deployment** (combination of classical + post-quantum algorithms during migration period),
4. **Governance and Workforce Strategy** (standards compliance, training, operational transition).

This framework ensures **structured, low-risk migration** rather than abrupt replacement of existing systems.

IV. RSA and ECC Cryptography: Mathematical Foundations and Security Assumptions

Public-key cryptographies form the basis of security in modern digital communication infrastructures. It allows secure key exchange over untrusted communication channels, authenticates data transactions, maintains their confidentiality, and ensures integrity. RSA and Elliptic Curve Cryptography are among the public-key systems that form the backbone of global encryption standards for banking, cloud services, defense networks, and blockchain-based platforms.

4.1 RSA Cryptography

RSA cryptography was introduced in 1977 and is grounded in the mathematical difficulty of the **Integer Factorization Problem** (IFP). RSA relies on selecting two sufficiently large prime numbers $p$and q, computing their product $n = p \times q$, and deriving a public key pair $(n, e)$and a private exponent d, where:

$$\boxed{d \equiv e^{-1} \pmod{\phi(n)}, \quad \phi(n) = (p-1)(q-1)}$$

The fundamental assumption underlying RSA security is that, although it is easy to multiply two large primes, factoring the resulting composite number $n$is computationally infeasible for classical computers when $n$is large enough [1]. The fastest known classical algorithms for factorization, such as the General Number Field Sieve (GNFS), still require super-polynomial time for cryptographically significant key lengths [2]. To mitigate brute-force or computational factorization attempts, RSA implementations typically use key lengths of **2048 bits** or greater. However, as quantum computing progresses, RSA's security is expected to weaken substantially. **Shor's Algorithm**, operating on a sufficiently stable and scalable quantum computer, can factor such large integers in **polynomial time**, effectively breaking RSA encryption by reconstructing private keys from public information [5].

4.2 Elliptic Curve Cryptography (ECC)

ECC offers stronger security per bit and was designed to achieve cryptographic strength using smaller key lengths. It is based on the **Elliptic Curve Discrete Logarithm Problem (ECDLP)**:

Given P and Q=kP, determine k

where $P$and $Q$are points on an elliptic curve defined over a finite field [3].

ECC is widely used in:

- **Secure web communication (TLS/SSL)**
- **Mobile and IoT devices** (due to low processing overhead)
- **Blockchain and cryptocurrency signatures** (e.g., Bitcoin's secp256k1 curve)
- **Smart cards, embedded systems, and secure access control modules**

The efficiency advantage is significant:

A **256-bit ECC key** offers approximately the same security strength as a **3072-bit RSA key**, reducing computational load and bandwidth requirements [6]. However, ECC—similar to RSA—is also vulnerable to Shor's Algorithm. Once practical quantum processors achieve adequate qubit stability and error correction, ECC-based systems will be breakable within operationally feasible time frames [7].

4.3 Structural Dependence and Vulnerability Risk

The global dependency on RSA and ECC creates a systemic cybersecurity exposure. The following sectors would face **high-impact compromise** if quantum attacks become operational:

Sector	Technology Reliance	Cryptographic Dependency	Risk Level
Banking & Finance	Online payments, SWIFT, UPI, digital wallets	RSA/ECC Certificates	High
Defence & Government	Secure radio, satellite, classified data	RSA/ECC PKI	Critical
Cloud Computing	Data-at-rest & in-transit encryption	TLS/SSL (RSA/ECC)	High
Blockchain & Cryptocurrency	Transaction signing & wallets	ECC-based signatures	Severe

Any quantum-enabled compromise of these systems could enable:

- Decryption of confidential historical communication
- Impersonation of digital entities
- Large-scale financial fraud
- De-anonymization of blockchain users
- Breaches of national security operations [7][8]

4.4 Strategic Need for Quantum-Resilient Transition

Given the breach window that is likely to occur in the near future, security agencies and research organizations such as NIST and ETSI have stressed shifting to Post-Quantum Cryptography (PQC)-a set of cryptographic algorithms impervious even to quantum computers [10][11]. The migration process is intricate and requires:

- Inventory of cryptographic dependencies
- Hybrid encryption deployment
- Gradual replacement of the vulnerable PKI infrastructures
- Workforce upskilling and governance restructuring

This strategic shift is necessary for enabling digital systems to ensure confidentiality, integrity, and authentication robustness against the emergence of quantum.

V. SHOR'S ALGORITHM: COMPUTATIONAL MECHANICS AND SECURITY IMPLICATIONS

Shor's Algorithm stands as one of the most significant breakthroughs in quantum computation, primarily because it demonstrates how quantum computers can solve problems that have long been considered practically impossible for classical systems. The algorithm's ability to efficiently factorize large numbers and compute discrete logarithms poses a direct and profound threat to the cryptographic systems we rely on daily—specifically RSA and Elliptic Curve Cryptography (ECC)—both of which depend entirely on the assumption that these mathematical problems remain computationally infeasible [5].

5.1 Mathematical and Computational Foundation

To understand why Shor's Algorithm is so powerful, we must first examine how it transforms the factorization problem. Rather than attempting to divide a large number directly, the algorithm reframes factorization as a problem of finding periodic patterns. Given an integer *n* that we wish to factor, we select a random integer *a*

$$\boxed{a^r \equiv 1 \pmod{n}}$$

where gcd (*a*, *n*) = 1. The algorithm then searches for the smallest positive integer *r* that satisfies:

This value *r* represents the order, or period, of *a* modulo *n*. Once we determine *r*, we can extract the factors of *n* using the expressions:

$$\boxed{\gcd(a^{r/2} - 1, n) \quad \text{and} \quad \gcd(a^{r/2} + 1, n)}$$

For classical computers, identifying this period *r* requires time that grows exponentially with the size of *n*—making it impractical for large numbers. However, Shor's Algorithm leverages the Quantum Fourier Transform (QFT), which exploits the interference patterns created by qubits in superposition to detect periodicity with remarkable efficiency [6].

The algorithm's elegance lies in its hybrid structure, which combines:

- **Quantum Parallelism**: The ability to evaluate multiple computational states simultaneously
- **Quantum Fourier Transform**: A mechanism for rapidly identifying periodic structures embedded in the data
- **Classical Post-Processing**: Traditional computational methods that convert the quantum results into usable prime factors

This integration of quantum and classical techniques has led many researchers to characterize Shor's Algorithm as a quantum-assisted cryptanalytic attack rather than a purely quantum process.

5.2 Hardware Requirements for Real-World Implementation

While Shor's Algorithm is theoretically sound, implementing it at a scale capable of breaking modern encryption faces substantial engineering challenges. To successfully factor a 2048-bit RSA modulus—the standard used in much of today's secure communication—a quantum computer would require:

Parameter	Approximate Requirement	Primary Limiting Factor
Logical Qubits	~4,000+	Qubit coherence and stability
Physical Qubits (with error correction)	~20 million+	Quantum error correction overhead
Gate Fidelity	>99.9%	Noise tolerance
Qubit Connectivity	High	Circuit depth and crosstalk

Current quantum devices, often referred to as "Noisy Intermediate-Scale Quantum" (NISQ) systems, fall considerably short of these thresholds. However, the gap continues to narrow as researchers make steady progress in qubit technology, error correction methods, and system architecture [7].

5.3 Experimental Progress and Milestone Demonstrations

Although we have not yet achieved the capability to break cryptographically relevant key sizes, researchers have successfully validated Shor's Algorithm through several proof-of-concept demonstrations:

Year	Achievement	Significance
2001	Factorization of 15 using 7 qubits	First physical demonstration by IBM
2012	Photonic implementation on small numbers	Demonstrated feasibility of modular circuit design
2022	Development of scaling techniques for Shor-like circuits	Reduced circuit depth for near-term devices
2023-2024	Superconducting and trapped-ion platforms achieved 100+ qubit stability	Established foundations for practical deployment

These experimental results suggest that the barriers to large-scale implementation are fundamentally engineering challenges rather than theoretical impossibilities. As quantum hardware continues to mature, the question is increasingly becoming "when" rather than "if" Shor's Algorithm will threaten current encryption standards.

5.4 Implications for RSA and ECC Security

The security of RSA encryption rests entirely on a single assumption: that factoring the product $n = pq$ of two large primes is computationally prohibitive. Once quantum computers capable of running Shor's Algorithm at scale become available, this assumption collapses, and with it, the confidentiality guarantees that RSA provides [5]. Similarly, Elliptic Curve Cryptography, which relies on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), faces equivalent vulnerability. Shor's Algorithm efficiently solves discrete logarithm problems as well, meaning ECC will fall alongside RSA [7]. The conclusion is stark: both RSA and ECC are mathematically destined for obsolescence in the quantum computing era. This is not a question of strengthening existing systems—it requires complete replacement with quantum-resistant alternatives.

5.5 The "Harvest Now, Decrypt Later" Threat

Perhaps the most pressing concern regarding Shor's Algorithm is not the immediate threat it poses, but rather the long-term vulnerability it creates. Intelligence agencies and security experts have identified a troubling strategy: adversaries are likely already collecting and archiving encrypted communications with the intention of decrypting them once sufficiently powerful quantum computers become available. This strategy, known as:

Harvest Now, Decrypt Later (HNDL)

It poses serious risks to any data that must remain confidential for extended periods, including:

- Diplomatic correspondence and treaty negotiations
- Military operational directives and strategic planning
- Biomedical and genetic research databases
- Corporate intellectual property and trade secrets
- Long-term R&D initiatives and innovation pipelines

This reality transforms quantum-resistant encryption from a future consideration into an urgent present-day necessity. Organizations cannot afford to wait until quantum computers become operational; by then, years or decades of sensitive communications may already be compromised [9].

5.6 Strategic and Policy Implications

The implications of Shor's Algorithm are profound and multidimensional:

1. **Cryptographic standards (RSA/ECC) must be replaced**, not strengthened.
2. **Quantum-resilient algorithms should be integrated now**, due to multi-year migration timelines.
3. **Industries operating under Industry 5.0 frameworks must embed quantum safety into architecture design**, not as a post-deployment upgrade.

These requirements align with emerging guidance from defence agencies, government digital infrastructure bodies, and international cryptographic standards organizations, all of which now emphasize proactive transition to post-quantum cryptography [10][11][12]. The window for preparation is narrowing, and the consequences of delay could prove catastrophic for organizations whose security models remain anchored to soon-to-be-obsolete cryptographic assumptions.

VI. QUANTUM-SAFE SECURITY SOLUTIONS: QKD AND POST-QUANTUM CRYPTOGRAPHY

As quantum computing continues to advance, with recommended public-key cryptography systems (RSA and ECC) vulnerable to Shor's Algorithm, organizations and governments need to put in place quantum-safe cryptographic systems. Quantum-safe cryptographic systems either avoid quantum attacks altogether or remain secure when quantum computing becomes widely available [10]. Two major strategic defense approaches stand out: Quantum Key Distribution, QKD; and Post-Quantum Cryptography, PQC.

6.1 Quantum Key Distribution (QKD)

Quantum Key Distribution is the security method of using the principles of quantum physics to exchange encryption keys securely between two parties. In contrast to the principle behind classical encryption systems, QKD does not depend on the difficulty of solving a mathematical problem but rather on the physical properties of quantum particles, particularly the behavior of photons. The most common QKD protocol is that of BB84. In BB84, the encryption keys become encoded in photon states. If a third party tries to intercept the photons, measuring them will change the state of the particles and, therefore, alert the communicating parties that the channel has been compromised. That is, eavesdropping can be detected in real time [10][11].

Advantages of QKD

- It offers provable security based on quantum physics.
- Eavesdropping attempts are detectable immediately.
- Suitable for critical sectors of defense, banking, and governmental communication networks.

Limitations of QKD

- It requires special hardware and optical fiber or satellite channels.
- Expensive and not yet suitable for widespread commercial use on the internet.
- Without quantum repeaters, communication distance can be limited.

Despite limitations, QKD is already being deployed:

- For their part, the Chinese demonstrated secure satellite-based QKD communication in 2017.
- Major financial institutions in Europe and Asia are already piloting QKD-secured data centers.
- Both US and Indian government agencies are funding national quantum communication networks.

QKD can thus be considered the solution for high-value and high-risk communication environments even without the advent of large-scale quantum computers.

6.2 Post-Quantum Cryptography (PQC)

While QKD focuses on securing the communication channel, in Post-Quantum Cryptography, the focus is to develop mathematical algorithms for encryption resistant to quantum attacks, such as Shor's and Grover's algorithms [12]. In 2022, **U.S. National Institute of Standards and Technology (NIST)** announced **CRYSTALS-Kyber** and **CRYSTALS-Dilithium** as leading PQC standards for encryption and digital signatures, respectively. Many governments and industries are now preparing their migration strategies based on these algorithms.

Unlike RSA and ECC, PQC algorithms are designed based on mathematical problems that quantum computers cannot solve efficiently. Some of the most promising PQC families include:

PQC Category	Core Principle	Example Algorithms	Security Reason
Lattice-Based Cryptography	Hard lattice vector problems	CRYSTALS-Kyber, Dilithium	No known quantum-efficient solution
Hash-Based Signatures	One-way hash functions	SPHINCS+	Simple and quantum-resistant
Code-Based Cryptography	Error-correcting codes	Classic McEliece	Resistant to quantum decoding attacks
Multivariate Polynomial Cryptography	Non-linear algebraic equations	Rainbow (reduced)	Hard quantum algebraic solving

Why PQC is Practical

- It can be implemented using existing computer and network hardware.
- Compatible with today's internet protocols.
- Scalable for both consumer and enterprise communications.

Challenges of PQC Adoption

- Some PQC algorithms require larger key sizes that affect performance.
- Standardization requires global coordination across industries.
- Migration from legacy PKI infrastructures may take years, not months.

6.3 Hybrid Cryptography for Industry 5.0 Environments

The security strategy for organizations transitioning into Industry 5.0 ecosystems needs to allow:

- Human–machine collaboration,
- Cloud–edge interconnected environments,
- AI-driven cyber defense
- Long-term data confidentiality.

Addressing these needs, several experts consequently advocate for a hybrid model of cryptography, wherein classical encryption (RSA/ECC) is combined with PQC: to immediately protect while the infrastructure is gradually upgraded.

This ensures the following:

- Security against current threats
- Protection from future quantum attacks
- Business continuity without abrupt system disruptions [11][12].

Strategic Insight

It is not optional to move towards quantum-safe security; it is a proactive risk management necessity. Organizations that delay transition will face avoidable vulnerabilities, especially when "Harvest Now, Decrypt Later" attacks become widespread Therefore, early planning and phased migration are important.

VII. STRATEGIC ADOPTION ROADMAP FOR INDUSTRY 5.0 ORGANIZATIONS

The migration to quantum-resistant security needs to be carefully planned, structured, and phased, considering Industry 5.0 environments where human–machine collaboration, automation, and interconnected data ecosystems form the operational core. The organizations cannot just replace RSA or ECC overnight but need a roadmap that would balance continuity, scalability, cost, and risk mitigation.

7.1 Phase 1: Awareness and Risk Assessment

This involves creating organizational awareness about the quantum security challenge. Most enterprises still believe that current encryption will be viable for decades to come, whereas in fact it will not.

Key activities within this stage include:

- Identifying systems utilizing **RSA, ECC, TLS, SSH, VPN, or blockchain wallets**.
- Mapping of **data assets requiring long-term confidentiality**: health records, IP repositories, legal contracts, defense data.
- Assess the risk of **Harvest Now, Decrypt Later (HNDL)** threats.
- Risk-based categorization of systems into critical, moderate, and low categories.
- This phase focuses on the identification of what needs protection and how urgently.

7.2 Phase 2: Pilot Testing of PQC and Hybrid Encryption

Once risk areas are identified, organizations begin pilots and deployments of PQC. To be sure, these need to be performed in controlled environments ahead of their full-scale deployment.

Recommended steps:

- Implement hybrid cryptographic protocols where PQC algorithms work in combination with classical methods.
- Test PQC algorithms such as CRYSTALS-Kyber for encryption and CRYSTALS-Dilithium for digital signatures.
- Performance overhead, storage impact, and interoperability with existing IT infrastructure should be considered.
- Ensure that backups and system recovery capabilities remain intact.

This pilot stage provides clarity on the technical adjustments and resource needs before wider implementation.

7.3 Phase 3: Integration of Quantum-Safe Key Management Systems

In quantum-era security architectures, secure key management becomes more critical. Organizations should update

- **Public Key Infrastructure (PKI)** in support of PQC certificates
- Key storage systems,
- Identity and access management solutions,
- Authentication tokens and signing tools.

Moving to hybrid chains of certificates allows for migration in steps without breaking compatibility with current networks and devices. This phase ensures that digital identity and authentication mechanisms remain trustworthy across the transition period.

7.4 Phase 4: QKD Deployment for Critical Communication Networks

While PQC will be able to protect almost all industrial and commercial systems, some high-value communication channels might require the utilization of QKD because of its real-time eavesdropping detection properties.

- Suitable environments include:
- Core data centers of financial institutions,
- Defense and intelligence networks,
- National research grids,
- Telecommunication backbones.

This is not a phase that aims to deploy QKD everywhere, but where risk is highest and the confidentiality duration is longest.

7.5 Phase 5: Policy, Compliance, and Workforce Training

Successful adoption is not purely technological; it requires organizational capability and policy reinforcement.

Actions:

- Update organizational cybersecurity policies and standard operating procedures.
- Conform to emerging national and international PQC norms, like NIST recommendations and national cybersecurity guidelines.
- Provide training for IT administrators, cybersecurity teams, management, and operational staff.

Establish continuous monitoring and threat intelligence frameworks to detect the emerging quantum attack vectors. This phase ensures that the security culture of an organization grows hand in hand with its technology.

VIII. Discussion

Quantum computing changes the landscape in which digital systems have their security based. In fact, conventional cryptography, including RSA and ECC, has been the backbone of secure communication for decades, relying implicitly on the fact that the problems at the base of these algorithms are not computationally feasible using classical computing. However, the already demonstrated capabilities of Shor's Algorithm mark a clear indication that this presumption will no longer be valid as soon as large-scale quantum processing becomes viable. That has wide implications, other than technological disruption, directly touching organizational risk management, national security preparedness, and global data governance frameworks [5][7].

In other words, considering Industry 5.0, with increased utilization of cyber-physical systems, human–machine collaboration, and intelligent automation in core operational environments, the integrity of data and communication becomes further critical. Industry 5.0 systems are highly dependent upon real-time data exchange among distributed networks, cloud infrastructures, IoT devices, and human interfaces. A fault in cryptographic security could therefore result not only in data breaches but also in operational failures related to safety, the accuracy of decisions, industrial reliability, and even physical process control [10][11]. The discussion on cybersecurity must, therefore, extend from technical vulnerability to strategic vulnerability. Even though quantum computers that can break RSA-2048 and ECC are not yet available, the HNDL threat indicates that the collection of encrypted data by adversaries may already be done with a view to decryption at some future date. This means that the "future risk" of quantum decryption is effectively a present-day exposure for any data requiring long-term confidentiality, such as healthcare archives, defense communication, diplomatic correspondence, and financial ledgers [9].

The two defence strategies considered here-QKD and PQC-play different but complementary roles. On the one hand, QKD provides physics-based security guarantees, making it best suited for the protection of high-value communication channels that remain confidential indefinitely. However, QKD deployment is currently too complex and expensive for mass-market systems. PQC, on the other hand, is more scalable and practical; it can be easily implemented with existing hardware, software, and networking. Most importantly, selection of secure PQC algorithms, especially recommended by on-going global standardization efforts, enables organizations to begin transitioning without operational disruption [12].

The strategic adoption roadmap proposed earlier aligns technical migration steps with business continuity considerations. This phased model reflects the reality that organizations vary greatly in system architecture maturity, risk exposure, and security budgeting. By approaching the transition incrementally—starting with risk assessment, followed by pilot testing, hybrid encryption deployment, and eventual integration of QKD in high-security domains—organizations can manage cost, complexity, and interoperability challenges while maintaining continuous protection. Overall, it is clear that the transition to quantum-safe security will not simply be a future technological upgrade but an immediate strategic priority. Organizations can avoid abrupt, high-cost responses later, protect their long-term confidentiality of data, and continue to operate with integrity in rapidly evolving digital ecosystems by taking early, informed action. Conversely, delayed adaptation risks exposing critical infrastructures to systemic vulnerability at the very point when Industry 5.0 systems become most deeply embedded in societal and economic operations.

IX. Conclusion

Quantum computing is not an incremental evolution in capability but a fundamental change in how complex problems could be solved. Whereas classical computing shows linear scaling, quantum computing uses quantum parallelism to enable the solution of specific mathematical problems exponentially faster. It is just this capability that makes Shor's Algorithm such a critical threat to the cryptographic infrastructure underlying secure digital communication: RSA and ECC are not guaranteed to provide long-term confidentiality in light of scalable quantum systems. In Industry 5.0, with interconnected devices, smart automation, data-driven decision systems, and collaborative human–machine environments at the core, the imperative of secure communication underpins everything. Any vulnerability to encryption can compromise privacy but also the very core of operational stability, safety, and system resilience. It positions cybersecurity not just as a technological necessity but also as a strategic foundation for ensuring trust and continuity in modern socio-technical systems. The vulnerability introduced by quantum decryption is neither hypothetical nor distant. The Harvest Now, Decrypt Later risk illustrates that adversaries can already store encrypted data today and decrypt it in the future once sufficient quantum computing resources become available. Therefore, the timeline of action must be immediate. Any wait until quantum computers are fully capable will leave organizations with critical gaps and no time to remediate them.

This research underlines two complementary ways to prepare secure infrastructures:

1. **Post-Quantum Cryptography (PQC)** provides a practical and scalable solution suitable for wide deployment using existing hardware and network structures.
2. **Quantum key distribution (QKD)** ensures physically verifiable and tamper-evident key exchange for communication channels requiring high-assurance or sovereign-level security.

The strategic adoption roadmap put forward in this paper advocates for a phased migration approach that starts with creating awareness and risk assessment, then moves through a pilot integration of PQC, upgrades key management frameworks, and selectively deploys QKD where the security stakes are the highest. This allows organizations to make the transition smoothly without any disruption to business operations, while maintaining compliance, reducing long-term risk, and future-proofing their data ecosystems. Eventually, the move to quantum-safe security will be more than a technical imperative; it will also be a strategic enabler of economic resilience, national security, digital sovereignty, and societal trust. The ability of organizations to act now will secure long-term advantage, reduce long-term vulnerability, and allow them to help shape a quantum-enabled, secure technological ecosystem. Those who wait may find themselves reacting to systemic failure rather than preventing it. The reality is clear: The time to prepare for the post-quantum world is now.

REFRENCES:

[1] Arute, F., et al. “Quantum supremacy using a programmable superconducting processor.” *Nature*, vol. 574, no. 7779, 2019, pp. 505–510.

[2] Preskill, J. “Quantum Computing in the NISQ era and beyond.” *Quantum*, vol. 2, 2018, pp. 1–20.

[3] Chen, L., et al. “Report on Post-Quantum Cryptography.” *NIST Interagency/Internal Report (NISTIR)*, 2016.

[4] Boneh, D., and Shoup, V. *A Graduate Course in Applied Cryptography*. Stanford University, 2020.

[5] Shor, P. W. “Algorithms for quantum computation: Discrete logarithms and factoring.” *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, IEEE, 1994, pp. 124–134.

[6] Mosca, M. “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?” *IEEE Security & Privacy*, vol. 16, no. 5, 2018, pp. 38–41.

[7] Gidney, C. & Ekerå, M. “How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits.” *Quantum*, vol. 5, 2021, pp. 1–24.

[8] IBM Quantum Roadmap. IBM Research Report. 2022.

[9] Kutin, S. “Harvest Now, Decrypt Later: A Global Data Security Concern.” *Journal of Cyber Policy*, vol. 7, no. 3, 2022, pp. 244–260.

[10] Xu, X., et al. “Industry 5.0: Human-Centric Smart Manufacturing.” *Manufacturing Letters*, vol. 33, 2022, pp. 1–4.

[11] Sharma, R., & Kapoor, A. “Cybersecurity Challenges in Industry 5.0 Systems.” *International Journal of Information Security Research*, vol. 12, no. 2, 2023, pp. 45–59.

[12] NIST. “Post-Quantum Cryptography Standardization: Round 3 Results and Final Selections.” National Institute of Standards and Technology, 2022.

AUTHOR DETAILS:

Author 1 (Corresponding Author)

Name: Mr. Neelotpal Dey

Post: Head of Department, Computer Science

Affiliation: Computer Science, Microtek Groups of Institution, Varanasi, Uttar Pradesh, India

Email: dr.neelotpaldey@gmail.com

ORCID ID: 0009-0008-4759-7664

Contact Number: +91-9451123331

Corresponding Author: Yes

Author 2

Name: Mr. Madhup Srivastava

Post: Assistant Professor

Affiliation: Physics, Microtek Groups of Institution, Varanasi, Uttar Pradesh, India

Email: madhupvns.ms@gmail.com

Corresponding Author: No

Point of Contact: All correspondence regarding this manuscript should be addressed to Mr. Neelotpal Dey, Corresponding Author.

AUTHOR BIO:

Mr. Neelotpal Dey is an experienced Software Engineer, Educational Technology Specialist, and Research Scholar with over ten years of teaching experience and six years in industry training. He holds an MCA, an MSc in Counselling and Family Therapy, and is pursuing a PhD in Computer Science. His expertise spans programming, data science, artificial intelligence, and educational technology. He is also a counselor and mentor for children and adolescents and actively engages in motivational speaking, podcasting, and creative arts.