DOI: http://dx.doi.org/10.26483/ijarcs.v16i6.7390

Volume 16, No. 6, November-December 2025

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

POST-QUANTUM IDENTITY MESH FOR AUTONOMOUS 5G, IOT, AND NATIONAL CONNECTIVITY SYSTEMS: IMPLICATIONS FOR FUTURE-RESILIENT DIGITAL INFRASTRUCTURE

Shiva Kumara
Independent Researcher
University of Washington, USA

***Abstract*—**Next-generation communication technologies such as fifth-generation (5G) wireless telecommunications systems enable the expansion of digital connectivity across commercial, industrial, and national infrastructure; as a result, an explosive increase in the use of the Internet of Things (IoT). In these highly distributed, autonomous environments, secure, scalable, and interoperable identity management systems are needed to provide authentication, authorization, and access control (AAA) for billions of devices and users. Centralized identity management frameworks have critical vulnerabilities due to their reliance on centralized architectures and traditional cryptographic algorithms. Vulnerabilities include susceptibility to quantum attacks, single points of failure, and cross-domain interoperability issues. Post-Quantum Cryptography (PQC) provides quantum-resilient security and Identity Mesh Architectures (IMAs) create decentralized and distributed identity management frameworks that support autonomous and cross-domain deployments. This paper presents a comprehensive analysis of PQC-IMAs through an examination of PQC, the IMA, security implications, deployment challenges, and future research directions. PQC-IMA integration allows for the creation of identity management systems that remain secure, resilient, and fault-tolerant when deployed in nationwide, large-scale 5G telecommunications networks and IoT systems. The solutions described in this paper can meet the challenges posed by the emerging Quantum Era and achieve operational efficiencies in connection ecosystems that are growing more and more complex and interconnected.**

***Keywords*—**Post-Quantum Cryptography, 5G Networks, Identity Mesh Architecture, Internet of Things (IoT), Secure Access Control, Autonomous Networks, National Digital Infrastructure.

I. INTRODUCTION

The emerging next-generations Communication technologies - including the 5G Network and Internet of Things (IoT) - have completely transformed not only the way people connect with the Digital World through commercial/Industrial avenues, but on a wider scale with their respective National Governments. As the use of Dynamic communication devices has increased on the world stage, so has the need for ultra-low latency communication capabilities through higher levels of interconnected device capability and autonomous control of such interconnected device capability supporting evolving Application Technologies (such as; Smart Cities, Intelligent Transportation Systems, Medical Networks, Critical Infrastructure) [1]. The Digital Identity is built on these emerging Connectivity Wizard technologies and it creates trusted relationships between the User, Devices, and Network by assuring that Users and devices have been properly authenticated, authorized and allowed access to Network Resources. As the connectivity ecosystem continues to evolve in terms of size and complexity, so too do the growing requirements for Mobile Service Providers to fulfil their customers' identities and build consumer Trust, through High-Level Interoperability between Service Providers, along with High-Operational Reliabilities, are not only a requirement of the service provider, but also of the consumer.

The independence and increasing number of 5G and IoT systems present additional cybersecurity challenges. The digital identity systems currently in place mainly utilize traditional (classical) cryptographic methods to determine the security of information. The traditional (classical) methods of cryptography do not provide sufficient protection against the computing capabilities of quantum computers being developed today because of the way that quantum algorithms impact existing public-key cryptosystems [2][3]. As quantum algorithms to be able to break existing popular cryptographic public-key schemes, long-term identity credentials and authentication schemes be compromised. The impact of these issues exacerbated in national connection areas where the compromise of an individual's identity could impact many sectors of the economy and society. In addition to quantum threats, current centralized identity management systems continue to have problems with identity spoofing, unauthorized access, large-scale device compromise, cross-domain trust management, etc.

In response to these challenges, there is growing recognition that PQC a major contributor to providing long-term security guarantees for digital identity systems. Secure long-term digital identity systems can be built on top of PQC's new generations of secure algorithms, which are impervious to conventional and quantum attack methods. However, PQC not solve all the problems associated with classical identity models, since PQC solutions not remedy the design vulnerabilities inherent in classical identity models. Thus, PQC solutions must be used in conjunction with decentralization to eliminate single points of failure and avoid scalability restrictions in large-scale and high-density systems (such as 5G or Internet of Things).

To deal with these types of problems, there has been an increase in interest in establishing a Post-Quantum Identity Mesh as a solid and scalable solution for managing identities in the digital age. An Identity Mesh is an approach that integrates Cryptographic Techniques, using Distributed and

Decentralized Identity Models and Systems to achieve secure, interoperable and self-managed identities within 5G Networks, IoT, and National Interconnectivity Infrastructures [4][5]. The architecture of a Post-Quantum Identity Mesh represents a potential building block for the creation of resilient Digital Infrastructure that meets the security and trust requirements of future generations of connectivity systems by reducing reliance on centralized trust models and increasing the susceptibility of these systems to quantum-based threats.

A. *Structure of the Paper*

The paper as organized: Section II outlines post-quantum cryptography for secure identity management. Section III explains the design and architecture of identity mesh systems. Section IV discusses their application in 5G, IoT, and national connectivity. Resilience in the future, security considerations, and obstacles are discussed in Section V. After a brief literature review in Section VI, the article finishes in Section VII with suggestions for further study.

II. Post-Quantum Cryptography for Identity Management

Data encryption algorithms like Post-Quantum Cryptography (PQC) attempt to ward off assaults from both quantum and traditional computers. Traditional cryptographic methods rely on number theory problems like discrete logarithm and split integer factorization; PQC substitutes these with methods that use a known mathematical structure that many researchers think can withstand the fastest known algorithm in quantum computing, such as Grover's algorithm for discrete logarithm computations and Shor's algorithm for split integer factorization [6]. Even though quantum computers can crack several popular cryptographic functions like RSA or ECC, PQC aims to create a new class of cryptographic procedures that impenetrable to these machines.

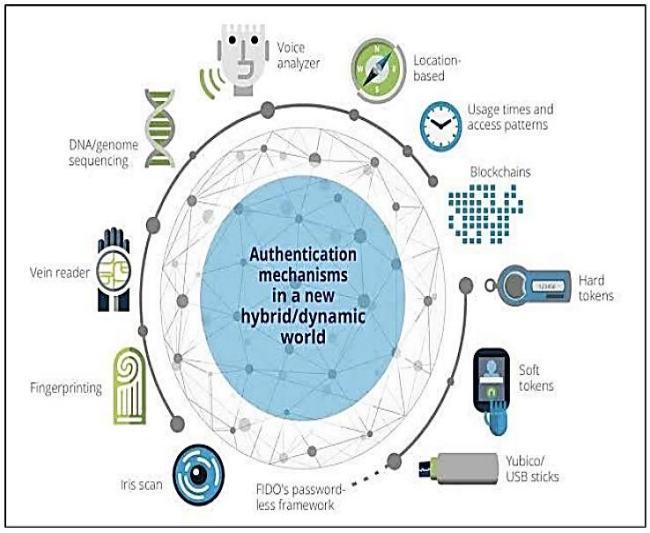

Fig. 1. The Race for Post-Quantum Cryptography.

The usage of quantum computers would not be an efficient solution to the complex mathematical problems used in PQC shown in Fig. 1 [7]. Utilizing the five mathematical principles of lattices, hashes, multivariate polynomials, codes, and isogenies, algorithms for secure public key encryption are constructed. Among these ideas, lattice-based cryptography (or just lattice-based encryption) stands out as a potential PQC contender due to its high level of purported resistance to quantum assaults, high efficiency, and dense implementation [8]. At this moment, no polynomial-time quantum algorithms exist to resolve the Shortest Vector Problem (SVP) or Learning with Errors (LWE), the two main categories of lattice issues. While PQC is designed to create a classical cryptosystem that is secure against potential attacks from quantum computing technology, it is not designed to use quantum encryption (e.g., quantum key distribution) methods.

A. *PQC For Identity Management*

The usage of quantum computers would not be an efficient solution to the complex mathematical problems used in PQC. Quantum secure public key encryption algorithms are built using the 5 mathematical concepts of lattices, hashes, multivariate polynomials, codes, and isogenies. Of these concepts, lattice-based (also known as lattice-based) cryptography is arguably the most likely candidate as PQC to provide excellent efficiency and density, combined with a high degree of claimed resistance to quantum attacks. Shortest Vector Problem (SVP) and Learning with Errors (LWE) are the two main categories of lattice problems for which no polynomial-time quantum algorithms are known to have solutions. The purpose of PQC is to build a classical cryptosystem that can withstand assaults from quantum computers, although it is not meant to employ quantum encryption techniques, such as quantum key distribution.

B. *Differences Between Classical and Post-Quantum Cryptography*

While classical cryptography and post-quantum cryptography are similar in that both algorithms have proven to be secure for exact solutions, they differ in their approaches to providing security against large-scale quantum attacks. Classical algorithms rely on computationally "hard" problems but also take advantage of an inherent "asynchronous" methodology to provide practical security against quantum computers. In contrast, existing asymmetric encryption methods like RSA, DSA, or ECC are super-dependent on computationally challenging problems that a quantum computer can easily solve using Shor's Algorithm. Therefore, this creates a vulnerability that could be exploited to decrypt any encrypted data previously stored on a digital device once high-capacity quantum computers become available.

Through the use of post-quantum cryptography, the information and communication technology industries can develop new methods of encryption to protect against the use of quantum computers to attack existing methods of encryption. For example, many of the proposed lattice-based encryption schemes consist of data stored in spaces called lattices that are not reversible, even using quantum computers. Lattice-based encryption utilizes the inefficiency of reversibility to efficiently provide security [9]. When comparing the resource requirements of a classical encryption scheme to those of post-quantum cryptography, and find that post-quantum encryption schemes tend to be much more resource-consuming than classical schemes. For example, a lattice-based encryption scheme may require a key size of several kilobytes, whereas RSA and ECC encryption schemes use a few hundred bytes for their keys.

Moreover, PQC is backward compatible with classical systems, making it the only differentiating feature of PQC from Quantum Cryptography, as Quantum Cryptography requires a quantum channel and quantum hardware. As a

result, PQC provides a more practical and extensible path toward Quantum Resistance.

C. Post-Quantum Cryptographic Techniques

New cryptographic techniques that can resist assaults from both classical and quantum computers are required in the future, as should be obvious to anyone keeping up with the latest news about quantum technology, including quantum computers and the possible dangers to existing cryptographic systems [10]. In Table I, shows the two primary methods for applying post-quantum cryptography:

1) Lattice-Based Cryptography

Advanced Structure-Related The foundation of cryptography lies on issues related to lattice structures, including Learning with Errors and Short Integer Solutions [11]. The leading post-quantum cryptographic schemes utilize lattice structure as their mathematical foundation because of the scalability and efficiency of creating digital signatures, performing key exchanges and encrypting data across a variety of industries using large networks (such as 5G/IOT).

2) Hash-Based Cryptography

Digital signatures can be generated using Hash-Based Cryptography by means of secure hash algorithms [12]. Security, simplicity, and low complexity are some of the advantages of hash-based signatures; however, there are certain limits, such as the size of the generated signatures and the management of keys for hash-based signatures.

3) Code-Based Cryptography

Cryptography that uses error-correcting codes—basically just random linear code—to decrypt messages is known as code-based cryptography [13]. These techniques have historically provided cryptographic security and have shown evidence of being resistant to quantum computing; however, these methods also tend to require large-sized public keys. As a result, storing and transmitting the keys can be difficult because of the size of these keys.

4) Multivariate Polynomial Cryptography

System solutions of multivariate quadratic equations formulated over finite fields are fundamental to these approaches. Since multivariate methods permit quick verification of signatures, they are mainly employed for digital signature production [14], making these systems a suitable option for identity verification, despite concerns of large key sizes and the ability to maintain long-term confidence in the underlying computational assumptions.

5) Isogeny-Based Cryptography

The basis of isogeny-based systems is the mathematical structure of elliptic curves isogenies. Isogeny-based systems typically result in shorter-sized keys than other schemes and provide strong cryptographic security assumptions; however, these systems generally still require substantially greater computational effort than the respective non-isogeny-based systems.

TABLE I. POST-QUANTUM CRYPTOGRAPHIC TECHNIQUES

Techniques	Security Basis	Key Strengths	Deployment Challenges
Lattice-Based Cryptography	LWE, SIS problems	Efficient, versatile, strong security	Parameter selection complexity, computational overhead
Hash-Based Cryptography	Secure hash functions	Simple design, strong security, provably secure	Large signature sizes, key management requirements
Code-Based Cryptography	Decoding random linear codes	Well-studied, robust against quantum attacks	Very large public keys, storage and transmission overhead
Multivariate Polynomial Cryptography	Solving multivariate quadratic equations	Fast verification, suitable for signatures	Large key sizes, limited practical adoption
Isogeny-Based Cryptography	Elliptic curve isogenies	Small key sizes, strong security assumptions	High computational cost, slow performance on low-power devices

D. Applicability of PQC in Large-Scale Connectivity Systems

The deployment of PQC is now being recommended to help provide security for large-scale connectivity systems such as 5G, IoT Ecosystems and National Communication Infrastructure which have a large number of users, devices and network functions that all require long-term secure authentication/key management. The use of PQC allows for a secure quantum-resistance mechanism for encryption, digital signatures and secure key exchanges so that identity credentials and communication channels remain confidential, even from potential future quantum-based attacks [15]. In addition, PQC also allow for secure device bootstrapping and machine-to-machine authentication, as well as cross-domain trust establishment, which aid in the operation of autonomous/distributed systems. Additionally, while some challenges exist with PQC, such as increased processing requirements and larger key size, continued improvements and hybrid approaches allow for continued, gradual utilization of PQC in existing systems, allowing for large-scale connector systems that are future-resilient to be developed.

III. IDENTITY MESH ARCHITECTURE AND DESIGN

The Identity Mesh Architecture is a Decentralized and Scalable identity-management system that is applied to distributed environments including 5G, IoT, and National connectivity [16]. This model supports secure Registration and Authentication of users through many different domains, i.e., it distributes the Identity service and Trust relationships among those that do not have a central Identity-Provider. This model increases the resilience, interoperability, and Autonomous cross-domain Interactions, and aligns with both a Zero-Trust and Post-Quantum security posture [17].

A. Overview of Identity Mesh

An identity mesh is an evolved form of IAM (Identity and Access Management) and it provides the ability for secure, scalable, and interoperable management of identity across disparate systems. In contrast to the traditional, centralized model of IAM, which makes all decisions about identities from one central point, an identity mesh uses decentralized and federated approaches for its IAM architecture. The architecture distributes identity services, policy enforcement, and the establishment of trust relationships among multiple domains [18]. This distributed architecture allows for a user, device, and application to perform authentication and authorization activities mutually, and independently of a

single identity provider. Thus, this architecture builds a more resilient, less reliance on a single point of failure.

The use of a mesh identity architecture allows for a more dynamic approach to identity verification, access control, and policy enforcement through interconnected identity services [19]. The services communicate using the same standardized protocols and share the same trusted frameworks, allowing for seamless interoperability of identity across 5G networks [20], IoT ecosystems, and large-scale connectivity infrastructures. Additionally, since identity is treated as a core security layer instead of as a centralized service, Mesh Identity Architectures enable autonomous operations, cross domain access and ongoing trust assessments, making them suitable for use in new distributed digital environments.

B. Distributed and Decentralized Identity Models

A safe, privacy-preserving, and user-centric identification system is necessary to manage an individual's identity due to the digital transformation of society. The storage, verification, and authentication of an individual's personal information is usually handled by a third-party organization in traditional, centralized identity management models [10]. Problems with data breaches, identity theft, individuals not having control over their data, and inefficient cross-platform interoperability of identity systems are all outcomes of these systems' centralized design. A new alternative for Identity Management is Distributed Ledger Technology (DLT) (Fig. 2) that allows individuals complete control of their data using a decentralized platform, such as blockchain technology [21].

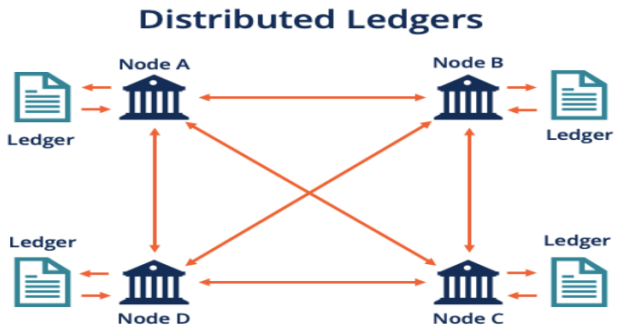

Fig. 2. Distributed Ledger Technology

A decentralized identity management system that is built on Distributed Ledger Technology (DLT) uses the fundamental components of SSI, DIDs, and VCs to create a system that is trustless, transparent, and resistant to tampering [22]. Digital ledger technology (DLT) has improved privacy, security, and user sovereignty by letting users safely communicate their own identity data with trusted parties of their choosing, without engaging or being manipulated by third parties. DLT also creates an immutable ledger for all transactions, ensuring the integrity of the data contained within it and allowing it to be certified.

A decentralized model could change the way industries operate, including how do business, conduct healthcare, and manage governments. The decentralized model allows secure, permission-based identity management across multiple networks and eliminates the need for centralized databases through a DLT [23][24]. The development of innovative cryptographic methods such as ZKPs allows users to demonstrate their identity's attributes while also ensuring confidentiality of their private information.

New opportunities for building and sustaining digital trust arise as a result of the DLT-based approach to decentralized identity management, which offers a chance to address scalability, interoperability, and compliance issues within the present legal landscape. A more sustainable and safer alternative to the conventional approach of managing identification is emerging with the rising deployment of DLT based identity solutions. This provide individuals greater control over their digital life.

C. Comparison with Traditional Identity Management

Centralized or federated identity and access management (IAM) architectures are used by conventional IAM systems. In these IAM approaches, identity verification and access control are administered by a few reputable identity providers [18]. The reliance of these conventional IAM systems on centralized directories, certificate authorities, or federation protocols imposes barriers to scalability; introduces single points of failure; increases risk of large-scale attacks; and creates challenges for real-time autonomous decision-making in rapidly changing technology landscapes characterized by massive device connectivity and cross-domain interoperability that are features of 5G and IoT system environments Upon review of ISO standards that relate to IAM, many industry groups point to three significant weaknesses of existing IAM solutions.

A mesh of identities offers to decentralize authentication and authorisation using multiple domains spread across Identity Services and Trust Relationships that may spread out across multiple Domains. With this design methodology, identities could be verified dynamically as they would be residing in heterogeneous systems. Instead of using a central authority to manage the services, an Identity Mesh Architecture offers to use distributed systems of trust. Using these types of distributed trust relationships provides additional resilience, scalability, and flexibility capabilities compared to traditional models (i.e. a single point of service) while failing to provide autonomous/automated networks[25], machine-based systems for interaction, or address the challenges of continued security through the use of post-quantum Cryptographic Techniques.

IV. Identity Mesh in 5G, IoT, and National Connectivity Systems

Through decentralized identity management, Identity Mesh allows the development of large scale, interoperable and distributed infrastructure for 5G, Internet of Things (IoT), and Network Connectivity (NC) with multiple national borders [26]. The distributed infrastructure provides secure identity verification, secure interoperable identity exchange with other domains, and a high level of Trust with Resilience through Crypto-based security.

A. Identity Management in Autonomous 5G Networks

With the 5th generation (5G) technology enabling ultra-low latency, and high-bandwidth communications between different types of devices with limited resources on an unprecedented scale, it has resulted in a digital environment consisting of ultra-high-precision devices connected to each other. The emergence of this digital environment has led to the establishment of many application domains including autonomous vehicles and smart cities, robotic industrialization and remote medical treatment. In addition to increased deployment activities an inherent challenge in

developing, controlling and administering authenticated identities and entitlement to access for billions of digitally connected devices need to be addressed from a secure, efficient and scalable standpoint [27]. The concept of IAM play a key role in establishing MDP as a foundation for managing trust, privacy and security within IoT (on 5G) networks as it relates to selecting the appropriate authentication type, the potential of extending machine identities[28], device-to-device communication, and multi-tenancy services (to the MDP). The deployment dynamics of IoT devices and infrastructure and the way in which they may be dynamically authenticated, authorized and managed throughout their operational and lifecycle by utilizing the advances in technology (e.g., SDN, NFV and SBA) present new complexities not previously experienced.

The computing power, memory capacity, and connection availability of IoT devices are often limited, in contrast to more conventional mobile or IT devices. Such limitations make it harder to implement a centralized identity system and standard Public Key Infrastructure (PKI). Furthermore, most IoT devices need to be able to move freely and independently, which means they need to be able to securely switch between networks and edge nodes, oftentimes without any human involvement. This highlights the importance of having scalable, lightweight, distributed identity and access management tools that can understand context [29]. The design of the 5G network presents additional difficulties. With the advent of new capabilities such as network slicing and multi-access edge computing (MEC), trust boundaries are becoming more fragmented. As a result, identity and access management solutions must be able to support tasks such as credential management at the edge, and federation identity resolution. Interoperability and standardization in identity provisioning and access policy enforcement are necessary due to the large number of devices and domain participants in the 5G-IoT ecosystem, including mobile network operators, cloud providers, and third-party service vendors.

B. Post-Quantum Identity for IoT Ecosystems

Compared to traditional mobile and IT devices, IoT devices typically have limited resources, including a limited amount of processing power, memory, and availability of connection. The constraints of these resources make it impractical to use standard public key infrastructure (PKI) and centralized identity management systems. In addition, the requirement for IoT devices to be mobile and operate independently from humans means they must be securely transferred from one network to another and connected to edge nodes without human involvement [30]. Therefore, there is a need for IAM features that are distributed, lightweight, and able to understand context, to be scalable and to provide flexibility. The 5G Network Architecture poses even more difficulties. IAM solutions need to be able to handle credentials at the edge, provide federation for identity resolution, and enable cross-slice authentication due to the fragmentation of trust boundaries caused by new capabilities like MEC and network slicing [31]. Furthermore, due to the high volume of IoT devices and 5G-IoT ecosystem participants like cloud providers, mobile network operators, and third-party service vendors, there is a pressing need for standardized identity provisioning and access policy enforcement, as well as for interoperability between these systems.

Post-Quantum Identity Models utilise Quantum-Resistant Cryptographic Primitives to secure the life cycle of IoT identities, from Device Registration through to Device Authentication, Authorisation and Secure Communication. This approach requires a lightweight and scalable model to support the limited resources available to IoT Devices [32][33], while allowing for decentralised and autonomous operation. Through the integration of Post-Quantum Integrity into Identity Models, IoT ecosystems able to create Future-Resilient Trust and allow for Secure M2M communication and ongoing Protection of Digital Identity in the Quantum Era.

C. Cross-Domain Identity in National Connectivity Infrastructure

Many different types of Infrastructures Connect to the Nation's Telecommunications Systems, Shipping and Public Sector through Cloud Services and Critical Infrastructure. In this context, the ability for organizations operating under different government authorities to verify and authenticate Users and Devices is necessary for Secure Seamless Interoperability [34][35]. Unfortunately, for many organizations their current identity Management approaches still function within Silos, creating barriers to Success and Limitations on growth within the Global Market.

By establishing a Federated/Decentralized Model of Trust, Cross-Domain Identity Management Frameworks can overcome the Obstacles to Successful Cross-Domain Identity Management [36]. This Method also provide an additional layer of security by implementing Post post-quantum cryptography and facilitating continued Support for Secure Services, Policy Enforcement and Interoperability across National Connectivity Infrastructures.

V. Security, Challenges, and Future-Resilient Infrastructure

The security benefits, installation issues and future areas of study for identity Mesh Architecture in 5G, IoT and National Connected Systems have been discussed within this section [37]. Decentralized/post-quantum identity Frameworks provide benefits to increase resiliency of identity mesh, identify practical constraints to those benefits and formulate ways to develop secure, scalable and future-ready digital infrastructure.

A. Security and Resilience Implications

Identity Mesh Architecture and post-quantum cryptography create stronger levels of security and resiliency within 5G and IoT systems as well as national systems for connectivity [38]. By providing decentralized methods for verifying an individual’s identity, these systems eliminate the potential for a single point of failure and support continuous authentication and dynamic enforcement of policies that strengthen operational resilience. Additionally, through the use of quantum resistant methodologies, these systems can protect users against the upcoming threats posed by cyber and quantum attacks and facilitate secure autonomous communications between users, devices and network resources.

B. Deployment Challenges and Limitations

Although Identity mesh technology provides many benefits, implementing the systems presents many challenges. Interoperability with legacy IAM solutions (such as RSA token solutions), multiple individual networks

(heterogeneous) and differing cross-domain administration policies make integration difficult [39]. Furthermore, IoT devices and edge nodes with limited resources may be impacted by the increased computational and communication demands caused by post-quantum cryptography. Finally, because there is still no robust set of standards, no clear regulatory direction or no operational experience available, it difficult to deploy Id-Mesh at a large scale.

C. *Future Research Directions.*

To be competitive in the emerging and rapidly-maturing field of IoT cryptography, future research should address new cryptographic approaches and concepts that are lightweight and energy efficient enough for use on low-powered IoT devices. Additionally, future research need to build upon existing initiatives to create adaptive identity mesh frameworks, automate trust management processes, and facilitate cross-domain orchestration [40]. Finally, as the commercial marketplace matures, there increased opportunities for stakeholders to pursue standardized approaches for building interoperable, scalable identity infrastructures that can resist both classical and quantum threats.

VI. LITERATIRE REVIEW

The purpose of this section is to present a summary of recent findings in 5G and IoT security and identify gaps that led to the need for post-quantum identity solutions as illustrated in Table II.

Sebestyen, Popescu and Zmaranda (2025) Recent studies published from 2021–2025 have provided a thorough examination of current security issues for the IoT arena, highlighting how the IoT security landscape continues to evolve. This review identifies the primary areas of focus, associated challenges, and suggested solutions, based on recent research. Additional classification of IoT security studies yielded six priority areas: Among these areas, 35.2% are new technologies, 19.3% are secure identity management, 17.9% are attack detection, 8.3% are data management and protection, 13.8% are communication and networking, and 5.5% are risk management. This percentage breakdown of research indicates where the research community has been directing its attention and signifies areas that warrant additional attention in future research. The review indicates that there is a strong emphasis on integrating advanced technologies in order to improve Security for IoT Systems, while also recognizing that there continues to be challenges associated with integrating these technologies into the respective application domains [41].

Hoque et al. (2025) provides an in-depth analysis of how UE (User Equipment) to UE communication in a 5G network uses PQC algorithms chosen by NIST. This study investigates the different digital signature techniques and Key Encapsulation Mechanisms (KEMs) used by PQC algorithms in real-world network scenarios utilizing a Complete 5G Emulation Stack (Open5GS and UERANSIM) and TLS (PQCE-Enabled Version 1.3) (using BoringSSL and the liboqs library). Performance is evaluated in terms of handshake latency, usage of CPU and memory, amount of data transferred, and the number of retransmissions that occur, with changes in configuration or client loads. As a result of testing, and found that ML-KEM and ML-DSA perform the most efficiently in terms of using the best configuration for application usage, while SPHINCS+ and HQC combinations produce the highest amount of calculation and transmission overhead and, as a result, may not be appropriate for security critical but time-sensitive applications in a 5G environment [42].

Zhang et al. (2024) A lattice-based approach is the one that has been suggested for PQ-IDS. This formulation of the Difficult Problem of Lattice Assumptions is based on the discrete Gaussian sampling technique and Bimodal Gaussian distributions. These guarantee that the proposed scheme is able to withstand quantum attacks to keep IoT devices safe during communications. In addition, the use of IoT device identity in the signature process guarantees that the information proving ownership cannot later be denied, thus proving ownership and guaranteeing that the information is not transferred without the original owner's permission. A thorough security proof proves that the proposed PQ-IDS possesses the security properties of being unforgeable, non-repudiable, and non-transferable. Efficiency and performance comparisons show that the suggested PQ-IDS scheme is well-suited to Internet of Things (IoT) applications [43].

Wazid, Das and Park (2024) presented a few examples of the possible uses of the new quantum cryptography-based framework are mentioned. The article also provides an overview of why quantum cryptography provides better security than conventional means of securing information over a public channel. Examples of how a typical blockchain works, its various applications, categorization of a blockchain by types, a depiction of the layout of a traditional blockchain are noted. Quantum computing's characteristics are further detailed, along with their possible detrimental effects on blockchain-based systems' security. Lastly, different quantum key distribution schemes, digital signatures, and hashing methods are compared with regard to cryptocurrency security [44].

Mehic et al. (2023) provides a comprehensive overview of the Network Protocols, Interfaces, and Management organizations' (NPIs) security concerns in 5G networks, as well as formal approaches to address these concerns. Primary focus is on the design, implementation, and practical use of Quantum Key Distribution (QKD) Networks after provide an overview of the fundamental concepts of QKD. Next, describe the overall structure of QKD Network Architectures and QKD Network Components, including the various standards associated with each component; finally, present a summary comparison of QKD Techniques and Current Solutions to Quantum Key Distribution that are applicable to existing Security Frameworks such as VPN's (e.g., IPsec and MACsec) and describe the key features of each. Additionally, examine the Requirements, Architecture and Approach to Building an FPGA-based Encryptor for use in executing Cryptographic Algorithms using Security Keys [45].

Pons et al. (2023) this manuscript provides an overall picture and explanation of interference in general wireless applications, as well as interference types specific to high-speed broadband networks (e.g. 5G) and IoT devices, and may also provide some techniques and methods for mitigating the impact of interference on high-speed wireless broadband networks (5G) and IoT device performance, thereby increasing the efficiency of IoT devices, thus providing more productive solutions for businesses that use them. In addition to providing methods for improving network efficiency, businesses that utilize the capabilities offered by both 5G and IoT technologies may be able to take advantage of the

convergence of multiple networks and services that can provide a greater level of access to the internet faster and with greater reliability, unlocking the potential for new innovative products and services. Overall, the results of this research indicate that business processes depend on effective and efficient use of technologies such as 5G and the IoT, therefore the future growth potential for businesses from these technologies is dependent on ensuring optimal connectivity and flexible access to the internet for multiple devices and multiple types of businesses [46].

TABLE II. COMPARATIVE ANALYSIS OF RELATED WORKS ON IOT, 5G, AND POST-QUANTUM SECURITY

Reference	Focus Domain	Security Technique / Approach	Key Contributions	Limitations / Research Gaps	Future Directions
Sebestyen et al. (2025)	IoT Security	Survey-based analysis	Reviews IoT security studies (2021–2025); categorizes research into six major areas with quantitative insights	Does not consider post-quantum cryptography or identity mesh frameworks	Integration of post-quantum and identity-centric security mechanisms for IoT
Hoque et al. (2025)	5G Networks	NIST-selected PQC (ML-KEM, ML-DSA, SPHINCS+)	Evaluates PQC performance in UE-to-UE 5G communication using TLS 1.3	Focuses on cryptographic performance; identity management not addressed	PQC-enabled identity authentication for autonomous 5G networks
Zhang et al. (2024)	IoT Networks	Lattice-based PQC (PQ-IDS)	Proposes quantum-resistant identity-based signature scheme with strong security properties	Limited to IoT networks; scalability across domains not discussed	Extension to large-scale IoT and integration with identity mesh architectures
Wazid et al. (2024)	Blockchain & Quantum Security	Quantum cryptography, QKD, quantum signatures	Analyses quantum threats to blockchain and reviews quantum-based security mechanisms	No integration with 5G, IoT, or identity management systems	Convergence of quantum-secure blockchain with identity mesh systems
Mehic et al. (2023)	5G Security	QKD and post-quantum key distribution	Surveys QKD integration into 5G security frameworks and hardware encryptors	Emphasis on key distribution rather than identity-centric security	Identity-centric PQC integration in 5G architectures
Pons et al. (2023)	5G & IoT Networks	Network optimization techniques	Discusses interference challenges and optimization for reliable IoT connectivity	Cryptographic security and identity aspects are not considered	Secure and quantum-resilient identity-aware network optimization

VII. CONCLUSION AND FUTURE DIRECTIONS

The integration of 5G networks, IoT systems and national connectivity systems has emphasized the importance of secure, scalable, and resilient identity management systems. The classical cryptographic schemes and traditional centralized schemas on identity are becoming too limited by their susceptibility to quantum attacks, scale issues and cross-domain energy-efficient PQC algorithms on constrained IoT devices, adaptive identity mesh structures, automated trust management, and standardized cross-domain energy-efficient PQC algorithms on constrained IoT devices, adaptive identity mesh structures, automated trust management, and standardized cross-domain governance frameworks. Also, to get scaled, security-aware and quantum-resistant identity infrastructures that can support next-generation connectivity systems, experimental validations, pilot deployments and optimization studies are needed.

REFERENCES

[1] M. Almutairi and F. T. Sheldon, "Resilience of Post-Quantum Cryptography in Lightweight IoT Protocols: A Systematic Review," Eng, vol. 6, no. 12, p. 346, Dec. 2025, doi: 10.3390/eng6120346.

[2] Y. Wang and E. Shahril Ismail, "A Review on the Advances, Applications, and Future Prospects of Post-Quantum Cryptography in Blockchain and IoT," IEEE Access, vol. 13, pp. 112962–112977, 2025, doi: 10.1109/ACCESS.2025.3584473.

[3] B. Senapati et al., "Quantum Computing and Its Potential Disruption to Data Centers and Edge Computing in Battery Cell Manufacturing Sites," in 2025 IEEE International Conference on Electro Information Technology (eIT), 2025, pp. 126–131.

[4] M. T. Damir and V. Niemi, "On Post-Quantum Identification in 5G," in Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, New York, NY, USA: ACM, May 2022, pp. 292–294. doi: 10.1145/3507657.3529657.

[5] R. P. Mahajan, "Transfer Learning for MRI image reconstruction: Enhancing model performance with pretrained networks," Int. J. Sci. Res. Arch., vol. 15, no. 1, pp. 298–309, Apr. 2025, doi: 10.30574/ijsra.2025.15.1.0939.

[6] Tim Abdiukov, "Quantum-resilient cybersecurity: Evaluating the impact of post-quantum cryptography on identity, asset and network security models," World J. Adv. Eng. Technol. Sci., vol. 13, no. 2, pp. 986–997, Dec. 2024, doi: 10.30574/wjaets.2024.13.2.0593.

[7] R. Patel, "Security Challenges in Industrial Communication Networks: A Survey on Ethernet/IP, Controlnet, and Devicenet," Int. J. Recent Technol. Sci. Manag., vol. 7, no. 8, pp. 54–63, 2022.

[8] T. Liu, G. Ramachandran, and R. Jurdak, "Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization," arXiv, Jan. 2024.

[9] A. Choudhary, Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions, vol. 4, no. 1. Springer International Publishing, 2024. doi: 10.1007/s43926-024-00084-3.

[10] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," Sensors, vol. 23, no. 8, p. 4117, Apr. 2023, doi: 10.3390/s23084117.

[11] D. Patel and R. Tandon, "Cryptographic Trust Models and Zero-Knowledge Proofs for Secure Cloud Access Control and Authentication," Int. J. Adv. Res. Sci.

Commun. Technol., pp. 749–758, Dec. 2022, doi: 10.48175/IJARSCT-7744D.

[12] Islam Ahmad Ibrahim Ahmad, Femi Osasona, Samuel Onimisi Dawodu, Ogugua Chimezie Obi, Anthony Chigozie Anyanwu, and Shedrack Onwusinkwue, "Emerging 5G technology: A review of its far-reaching implications for communication and security," World J. Adv. Res. Rev., vol. 21, no. 1, pp. 2474–2486, Jan. 2024, doi: 10.30574/wjarr.2024.21.1.0346.

[13] Vibhor Pal, "Hybrid Quantum-Classical Machine Learning Architectures for Accelerated Drug Discover," Int. J. Adv. Res. Sci. Commun. Technol., vol. 6, no. 2, pp. 1641–1653, Jun. 2021, doi: 10.48175/IJARSCT-6582M.

[14] H. Shekhawat and D. S. Gupta, "A survey on lattice-based security and authentication schemes for smart-grid networks in the post-quantum era," Concurr. Comput. Pract. Exp., vol. 36, no. 14, Jun. 2024, doi: 10.1002/cpe.8080.

[15] Ramat Yusuf and Ibrahim Abdul Abdulrahman, "Towards Quantum-Resilient Log Integrity in 5G/6G Mobile Network Protocol Analysis," Glob. J. Eng. Technol. Adv., vol. 24, no. 3, pp. 391–405, Sep. 2025, doi: 10.30574/gjeta.2025.24.3.0280.

[16] N. Minhas, "Post-Quantum Authentication Scheme for IoT Security in Smart Cities," Jul. 30, 2024. doi: 10.20944/preprints202407.2309.v1.

[17] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," Int. J. Sci. Res. Mod. Technol., vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[18] B. Choudhury, A. Hota, M. Karmakar, S. Saha, A. Nag, and S. Nandi, "A Comprehensive Survey on Pre Versus Post Quantum Security Schemes for 5G-Enabled IoT Applications," IEEE Access, vol. 13, pp. 159305–159333, 2025, doi: 10.1109/ACCESS.2025.3608623.

[19] V. Chamola, M. Shall Peelam, M. Guizani, and D. Niyato, "Future of Connectivity: A Comprehensive Review of Innovations and Challenges in 7G Smart Networks," IEEE Open J. Commun. Soc., vol. 6, pp. 3555–3613, 2025, doi: 10.1109/OJCOMS.2025.3560035.

[20] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large- Scale Cybersecurity Networks Data Analysis : A Comparative Study," TIJER – Int. Res. J., vol. 11, no. 12, pp. 922–928, 2024.

[21] R. Soltani, U. T. Nguyen, and A. An, "Practical Key Recovery Model for Self-Sovereign Identity Based Digital Wallets," in 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), IEEE, Aug. 2019, pp. 320–325. doi: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066.

[22] Z. A. Lux, F. Beierle, S. Zickau, and S. Gondor, "Full-text Search for Verifiable Credential Metadata on Distributed Ledgers," in 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), IEEE, Oct. 2019, pp. 519–528. doi: 10.1109/IOTSMS48152.2019.8939249.

[23] N. Naik and P. Jenkins, "uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain," in 2020 IEEE International Symposium on Systems Engineering (ISSE), IEEE, Oct. 2020, pp. 1–7. doi: 10.1109/ISSE49799.2020.9272223.

[24] S. Singh, "Open Radio Access Networks in Multi - Vendor Environments : A Survey of Interoperability Solutions and Best Practices," Int. J. Innov. Sci. Res. Technol., vol. 10, no. 2, 2025, doi: 10.5281/zenodo.14881343.

[25] P. Nutalapati, J. R. Vummadi, S. Dodda, and N. Kamuni, "Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data," in 2025 International Conference on Data Science and Its Applications (ICoDSA), IEEE, Jul. 2025, pp. 880–885. doi: 10.1109/ICoDSA67155.2025.11157595.

[26] N. Prajapati, "Review of Quantum Computing Advances and their Impact on Modern Cryptographic Security," Int. J. Innov. Sci. Res. Technol., vol. 10, no. 5, pp. 2023–2035, May 2025, doi: 10.38124/ijisrt/25may501.

[27] P. Varga et al., "5G support for Industrial IoT Applications— Challenges, Solutions, and Research gaps," Sensors, vol. 20, no. 3, p. 828, Feb. 2020, doi: 10.3390/s20030828.

[28] G. Sarraf and V. Pal, "Adaptive Deep Learning for Identification of Real-Time Anomaly in Zero-Trust Cloud Networks," ESP J. Eng. Technol. Adv., vol. 4, no. 3, 2024, doi: 10.56472/25832646/JETA-V4I3P122.

[29] A. Panwar and P. Peddi, "A Study to Explore the Aptitude and Attitude of Educators Towards Emerging Technologies in Computer Science in Higher Education in Shekhawati: Bridging the Digital Divide," SSRN Electron. J., 2025, doi: 10.2139/ssrn.5362850.

[30] F. Samiullah, M.-L. Gan, S. Akleylek, and Y. Aun, "Post-Quantum Group Key Management in IoTs," in 2023 25th International Multitopic Conference (INMIC), IEEE, Nov. 2023, pp. 1–6. doi: 10.1109/INMIC60434.2023.10466001.

[31] S. Amrale, "Anomaly Identification in Real-Time for Predictive Analytics in IoT Sensor Networks using Deep," Int. J. Curr. Eng. Technol., vol. 14, no. 6, pp. 526–532, 2024.

[32] P. Scalise, R. Garcia, M. Boeding, M. Hempel, and H. Sharif, "An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods," Electronics, vol. 13, no. 21, p. 4258, Oct. 2024, doi: 10.3390/electronics13214258.

[33] V. Prajapati, "Role of Identity and Access Management in Zero Trust Architecture for Cloud Security:

Challenges and Solutions," Int. J. Adv. Res. Sci. Commun. Technol., vol. 5, no. 3, pp. 6–18, Mar. 2025, doi: 10.48175/IJARSCT-23902.

[34] D. Chawla and P. S. Mehra, "A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions," Internet of Things, vol. 24, p. 100950, Dec. 2023, doi: 10.1016/j.iot.2023.100950.

[35] P. Chandrashekar and M. Kari, "Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing System," vol. 11, no. 4, pp. 901–907, 2024.

[36] R. Asif, "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms," IoT, vol. 2, no. 1, pp. 71–91, Feb. 2021, doi: 10.3390/iot2010005.

[37] J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," Microprocess. Microsyst., vol. 77, p. 103201, Sep. 2020, doi: 10.1016/j.micpro.2020.103201.

[38] G. R. Figlarz and F. P. Hessel, "Applied Post-Quantum Secure Method for IoT Devices: A Case Study for Autonomous Vehicles Communication," in 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), IEEE, Oct. 2022, pp. 1–6. doi: 10.1109/WF-IoT54382.2022.10152075.

[39] J.-A. Septien-Hernandez, M. Arellano-Vazquez, M. A. Contreras-Cruz, and J.-P. Ramirez-Paredes, "A Comparative Study of Post-Quantum Cryptosystems for Internet-of-Things Applications," Sensors, vol. 22, no. 2, p. 489, Jan. 2022, doi: 10.3390/s22020489.

[40] M. Menghnani, "Advancing PWA Accessibility: The Impact of Modern Frameworks and Development Tools," Int. Res. J., vol. 12, no. 3, 2025.

[41] H. Sebestyen, D. E. Popescu, and R. D. Zmaranda, "A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories," Computers, vol. 14, no. 2, p. 61, Feb. 2025, doi: 10.3390/computers14020061.

[42] S. Hoque, A. Aydeger, E. Zeydan, and M. Liyanage, "Analysis of Post-Quantum Cryptography in User Equipment in 5G and Beyond," in 2025 IEEE 50th Conference on Local Computer Networks (LCN), IEEE, Oct. 2025, pp. 1–9. doi: 10.1109/LCN65610.2025.11146323.

[43] Y. Zhang, Y. Tang, C. Li, H. Zhang, and H. Ahmad, "Post-Quantum Secure Identity-Based Signature Scheme with Lattice Assumption for Internet of Things Networks," Sensors, vol. 24, no. 13, p. 4188, Jun. 2024, doi: 10.3390/s24134188.

[44] 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.

[45] M. Mehic et al., "Quantum Cryptography in 5G Networks: A Comprehensive Overview," IEEE Commun. Surv. Tutorials, vol. 26, no. 1, pp. 302–346, 2023, doi: 10.1109/COMST.2023.3309051.

[46] M. Pons, E. Valenzuela, B. Rodríguez, J. A. Nolazco-Flores, and C. Del-Valle-Soto, "Utilization of 5G Technologies in IoT Applications: Current Limitations by Interference and Network Optimization Difficulties—A Review," Sensors, vol. 23, no. 8, p. 3876, Apr. 2023, doi: 10.3390/s23083876.

