Received: 7 November 2023 | Revised: 30 December 2023 | Accepted: 18 January 2024

DOI: 10.1002/wics.1644

ADVANCED REVIEW

WIREs COMPUTATIONAL STATISTICS WILEY

A survey on post-quantum based approaches for edge computing security

Aykut Karakaya[1] | **Ahmet Ulu**[2]

[1]Department of Computer Technologies, Bulent Ecevit University, Zonguldak, Turkey

[2]Department of Computer Engineering, Artvin Coruh University, Artvin, Turkey

Correspondence
Aykut Karakaya, Department of Computer Technologies, Bulent Ecevit University, Zonguldak, Turkey.
Email: aykut.karakaya@bil.omu.edu.tr

Edited by: Emily Frieben, Commissioning Editor and David W. Scott, Co-Editor-in-Chief

Abstract

With the development of technology and its integration with scientific realities, computer systems continue to evolve as infrastructure. One of the most important obstacles in front of quantum computers with high-speed processing is that its existing systems cause security vulnerabilities. Therefore, in order to take advantage of quantum systems, existing systems that are already secure must also be secure in the post-quantum scenario. One of these systems is edge computing. There are challenges in terms of computational power for the implementation of pre- and post-quantum methods in structures with resource-constrained devices. This article reviews the post-quantum security threats of edge devices and systems and the secure methods developed for them. Although there is relatively little research in this field, it remains relevant. In the studies reviewed, lattice-based approaches are often highlighted for making edge systems quantum-resistant. Additionally, these studies indicate that there has been an increasing trend in this field in recent years.

This article is categorized under:

Applications of Computational Statistics > Defense and National Security

Algorithms and Computational Methods > Networks and Security

KEYWORDS

edge computing, internet of things, lightweight, post-quantum, security

1 | INTRODUCTION

With the development of technology and its integration with scientific facts, computer systems continue to evolve as the underlying infrastructure. One of the major obstacles facing high-speed quantum computers, which have the capability for rapid processing, is their potential to introduce security vulnerabilities into existing systems. Therefore, in order to harness the advantages of quantum systems, existing systems that are currently secure must also remain secure in a post-quantum scenario. One of these systems is edge computing systems. In structures that house resource-constrained devices, there are computational challenges in implementing both pre- and post-quantum methods. This situation must be taken into account when designing methods. This study examines the post-quantum security threats to edge devices and systems and the secure methods developed in response to these threats. Within this scope, methods,

tools, and models used for the security of quantum-resistant edge systems are explained and compared (Karakaya & Akleylek, 2022). Challenges, issues, and future trends in this field are examined, and directions for future research are provided.

Edge computing is a computational concept that is preferred in Internet of Things (IoT) systems and is used to process data generated by edge devices within the edge system. It is commonly used in applications where low latency is required. It is typically designed to be integrated with cloud systems. It is used in scenarios where data that needs to be persistently stored is sent to the cloud, while data that requires rapid processing is processed within the edge system (Arat & Akleylek, 2023b). Edge systems, despite their speed advantages, can introduce different vulnerabilities. Many attacks occur through traditional methods and can be prevented with established security measures. However, these measures cannot prevent attacks based on quantum computing. Therefore, quantum-based encryption methods should be used for protection in systems. IoT systems, due to their resource-constrained nature at the endpoints, make the implementation of encryption methods challenging. Hence, there is a tendency to design lightweight encryption algorithms, protocols, and frameworks.

In IoT systems, cloud computing, fog computing, and edge computing are used for storage and data processing. These systems can be used separately in models or applications, or they can be integrated with each other. Fog and edge computing provide local solutions for data processing and storage. Cloud computing, on the other hand, operates through a remote node accessed over the internet. Fog computing reduces service latency for end-users. Cloud computing extends storage, networking, and computing capabilities to the edge of the network, thus enhancing the system's performance and efficiency (Bader et al., 2016). Cloud computing optimizes data through remote servers, while fog and edge computing optimize and manage the local environment. Fog computing is characterized by low latency, the establishment of security measures, location awareness, and being local, among other features, while edge computing is characterized by being secure due to short distances, resource-constrained, low computing capacity, and local, among other features. Cloud computing, on the other hand, has high latency, undefined security measures, lacks location awareness, and is global in nature, among other characteristics.

In many of the security protocols proposed both pre- and post-quantum, there is an element of trust in an entity within or outside the system. However, the security of these entities cannot always be guaranteed. One of the major vulnerabilities in security protocols is the assumption of trust in third parties. When these systems are implemented, the presence of untrusted actors can jeopardize the entire system. Therefore, additional authentication mechanisms are being developed to account for the possibility of untrusted actors in both pre- and post-quantum systems. In recent years, research in this area has been rapidly increasing.

One of the primary methods that can be used to ensure post-quantum security in edge systems is the use of a security protocol based on post-quantum cryptography (PQC) for data exchange. These can be classified into code-based, lattice-based, and hash-based cryptographic systems. Since the methods used in public-key cryptography become obsolete in the post-quantum era, alternatives are being developed for these methods. Some of the existing symmetric encryption systems (especially AES-256) and hash systems (especially SHA-2 and SHA-3) are considered secure for post-quantum scenarios, even though their effectiveness may decrease (Mavroeidis et al., 2018). Therefore, the development of cryptographic algorithms that meet the requirements of public-key cryptographic systems is more prominent. These systems can also make current IoT structures secure for the post-quantum era. The fact that systems using traditional public-key cryptography are not quantum-resistant is the most significant threat to the security of these systems. IoT systems using edge devices often contain resource-constrained devices, making it challenging to integrate post-quantum approaches into them. However, there are lightweight post-quantum approaches in the literature to make systems quantum-resistant, albeit with some limitations.

1.1 | Contribution and organization

This article covers the vulnerabilities, threats, and general security aspects of cloud, fog, and edge computing systems. In addition, the paper specifically focuses on edge computing systems, which have become a common trend in recent years, and evaluates security issues in the context of the post-quantum era. There are relatively few studies and efforts dedicated to ensuring the security of edge computing mechanisms, especially those used in IoT systems, for the post-quantum era. Therefore, this article assesses the methods, schemas, and frameworks related to this topic. To the best of our knowledge, this is the first review study that examines only focusing edge computing post-quantum security.

In this article, Section 2 presents general security principles. Section 3 compares data processing and storage units, namely cloud, fog, and edge computing, and discusses the usage areas of edge computing. Section 4 covers the types and details of post-quantum security. Section 5 includes the analysis and results of post-quantum-based approaches to edge computing security, which is the primary contribution of this article. Sections 6 and 7 respectively discussion, future directions, and challenges in the field. The paper concludes in the final section.

2 | CYBERSECURITY

There are several reference models used to determine whether a system can be considered secure. One of the most widely accepted models is the Confidentiality–Integrity–Availability (CIA) model. The CIA model, as defined by NIST SP 800-95, describes measures that protect the availability, integrity, authentication, confidentiality, and nonrepudiation of information systems (Chowdhury et al., 2023). Systems that ensure these conditions are generally considered secure. The CIA model is illustrated in Figure 1.

Privacy is ensured by preventing unauthorized access to data or information (Nweke, 2017). Secure encryption algorithms are often used to guarantee the privacy of systems. Integrity ensures that data remains unchanged or uncorrupted from the source to the destination. Secure hash structures or Message Authentication Codes (MACs) are commonly used to achieve data integrity. Availability means that legitimate users can receive uninterrupted service from the system at any time, within the permitted timeframes and conditions. Therefore, the system should be resilient to attacks and should not disrupt users' access to services. In addition to these fundamental principles, systems need to incorporate principles of authentication and nonrepudiation to be secure. Authentication is the process of verifying that users are who they claim to be through methods like passwords, fingerprints, multi-factor authentication, or iris scanning. Nonrepudiation involves recording every action taken within the system, allowing for indisputable proof that a particular action was performed by a specific user (Nweke, 2017).

There are numerous encryption algorithms, security protocols, hash methods, blockchain structures, and more that provide the fundamental principles of security for systems. Presently, the security of the systems in use can be reasonably assured through traditional methods. However, the development of quantum computers and the significant increase in computing power they bring pose a risk to the security of traditional methods. Therefore, it appears inevitable that systems will need to be designed with quantum resilience in mind in the near future.

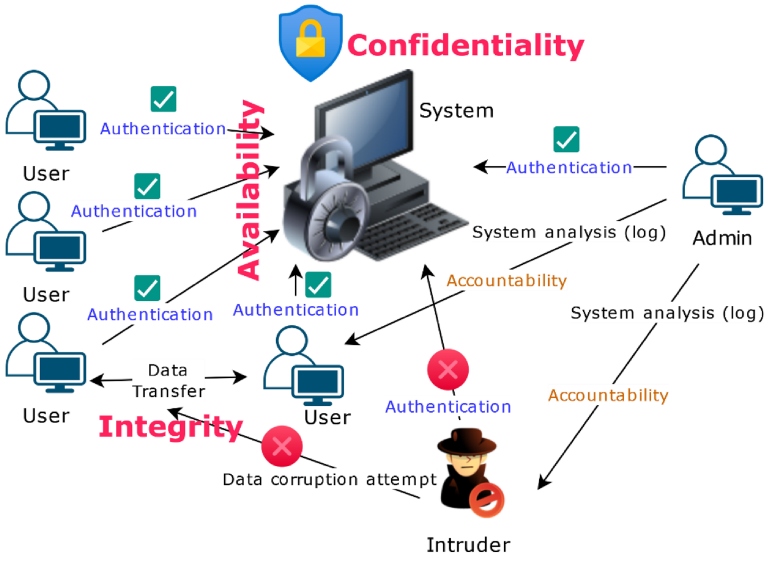

FIGURE 1 CIA model.

3 | CLOUD, FOG, AND EDGE COMPUTING

Cloud computing is a significant storage and data processing method in today's technological landscape. However, with the increasing prevalence of IoT applications, storing and processing data in cloud systems from IoT devices over the internet can introduce security threats and latency issues. In IoT systems that utilize cloud computing, data collected from sensor devices at the edge is typically sent directly to the cloud for storage and data processing. Transmitting data in its raw form over the internet to the cloud can create vulnerabilities in data security. Data security can be implemented at the edge devices, but in resource-constrained devices, the computational cost of encryption and protection can be high.

Fog computing, on the other hand, involves processing, storing, and transferring data in a local environment. It can address some of the unresolved issues posed by cloud computing due to its flexible resources and services. These issues include unknown security delays, lack of support for mobile nodes, high bandwidth requirements, and location awareness. In fog computing, services at the network's edge are provided by fog nodes (Karakaya et al., 2022).

Both fog and edge computing provide local solutions for data processing and storage, optimizing and managing the local environment. In contrast, cloud computing operates through remote servers accessed via the internet. Fog computing reduces service latency for end-users. Cloud computing extends storage, networking, and computing capabilities to the edge of the network, thereby enhancing system performance and efficiency. As a result, fog computing is a component that improves system performance and efficiency (Bader et al., 2016). It offers advantages such as low latency, security measures, location awareness, and being local. Edge computing, due to its proximity to the data source, is secure, resource-constrained, has low computing capacity, and is local. Cloud computing, however, has high latency, undefined security measures, lacks location awareness, and operates globally.

Edge and fog computing both provide local solutions for data management. The difference is that edge computing performs the work on edge devices, such as sensors and mobile devices (Varghese et al., 2016). Fog computing, on the other hand, performs the computation on fog nodes and sends the data to the cloud or edge devices in response. Edge is fully localized. Fog extends computing and communication resources to the edges of the network (Mukherjee et al., 2017). In other words, fog is a layer between edge devices and cloud systems that serve as long-term storage.

Edge computing does not directly support cloud services, so data is processed and sent to the cloud in a real-time data processing step. In IoT, cloud, fog, and edge can be used individually, or they can be used in combinations such as cloud-fog, cloud-edge, or cloud-fog-edge. Using edge or fog extends cloud capabilities to the edges of the network, which allows IoT systems to serve in a wide area. The locations of cloud, fog, and edge computing in a system are shown in Figure 2.

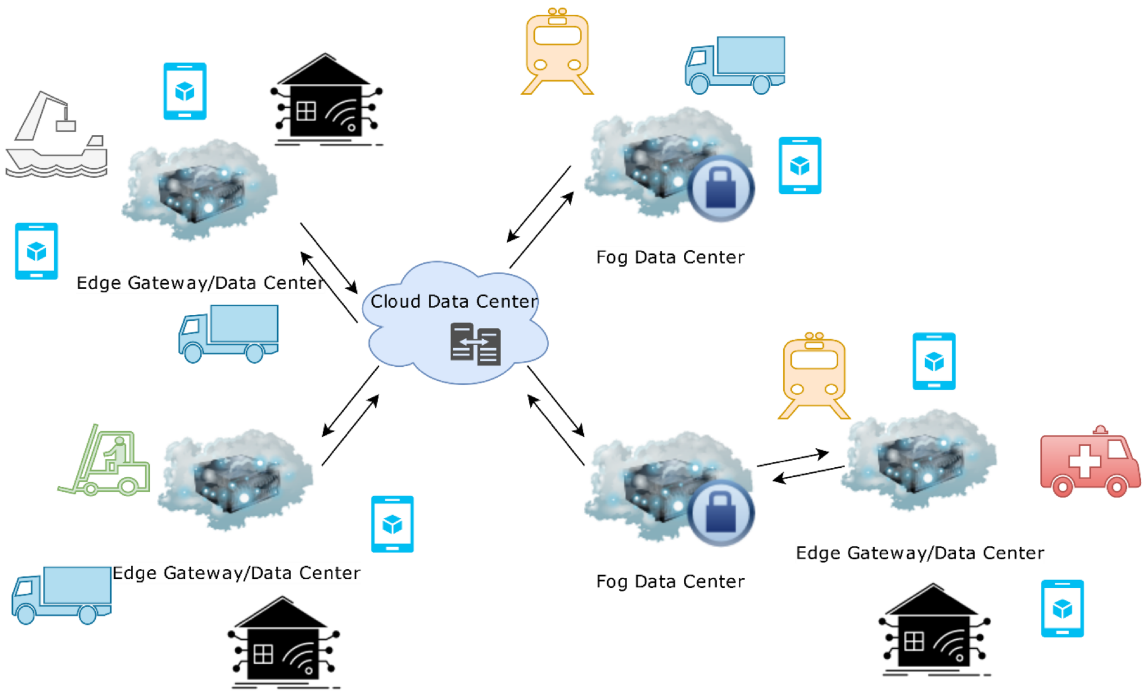

FIGURE 2 The locations of cloud, fog, and edge computing in a system.

In recent times, multi-access edge computing (MEC) systems, which have become quite popular in the field of data centers, extend cloud services towards the edge of the network, providing resources for data storage and processing through base stations. In this respect, MEC architecture, which is similar to fog computing systems, enhances the performance of edge computing systems. Like fog computing, MEC architecture offers the ability to serve heterogeneous resources, virtualization, mobility, low latency, and scalability support (Roman et al., 2018). However, the key difference lies in the fact that MEC is typically utilized by telecommunications companies and is closer to the edge systems, making it faster. The most significant advantage of fog computing compared to MEC architecture is the ability to establish independent private networks, separate from telecommunications companies.

When designing IoT models that utilize fog or edge computing systems, cloud systems are often integrated into the design. The comparison between cloud, edge, and fog computing is shown in Table 1.

There are certain security threats associated with computing processes in cloud, fog, and edge computing. Some of these threats are common to all three, while others may affect one or two of them. The threats faced by cloud, fog, and edge computing systems are depicted in Table 2.

In IoT applications, as seen in Table 2, cloud, edge, and fog computing systems generally face similar threats. However, there are differences in how these attacks are executed due to the nature of cloud computing being internet-based while edge and fog computing are localized.

IoT systems' end devices can be models consisting of one or several sensors, and they can also utilize methods where a large number of sensors interact with each other, such as wireless sensor networks (WSN) and wireless body area networks (WBAN; Karakaya & Akleylek, 2018). These sensors often involve multi-hop connections, where data is transmitted between nodes after it is detected, until it reaches the data center.

TABLE 1 Comparison of cloud, fog, and edge computing.

Cloud computing	Fog computing	Edge computing
High latency	Low latency	Low latency
Long response time	Short response time	Short response time
Data processing and storage: On the device accessed via the Internet	Data processing and storage process: On devices in the fog layer	Data processing and storage: On-edge devices
Internet connected	Local	Local and internet connected
Storage and data processing capacity: High	Storage and data processing capacity: High	Storage and data processing capacity: Low
Central processing	Distributed processing	Distributed processing

TABLE 2 Security threats of cloud, fog, and edge computing.

Security threats	Affected computing system
Physical attacks	Cloud (to end devices), fog (to fog nodes and end devices), edge (to end devices)
Denial of service (DoS, XML-DoS, and HTTP-DoS)	Cloud, edge, fog (with malicious nodes)
Wormhole attack (creating shortcuts within sensor nodes)	Cloud, edge, fog (when used in IoT applications)
Sybil attack (copying sensor identities)	Cloud, edge, fog (when used in IoT applications)
Man-in-the-middle (MitM)	Cloud (over the internet—with IP, DNS, etc. breaches), edge, and fog (with local network intrusion)
Malware Injection	Cloud, edge, fog
Virtual Machine Attacks	Cloud, edge, fog (attacks on infrastructure)
Attacks on Encryption Systems	Edge (encryption with resource-constrained end devices), Fog (encryption with fog network nodes)
Attacks utilizing poorly designed infrastructure, insecure service providers, wireless network issues, etc.	Cloud, edge, fog

3.1 | Usage areas and security needs of edge systems

Edge computing brings data processing and storage needs closer to the point where data is generated or results are delivered. It offers several significant advantages, including (Bonomi et al., 2012):

- *Low latency*: One of its most important advantages is low latency. Data is processed and stored on nearby edge devices rather than distant cloud or local fog networks. Edge nodes deliver data to a closer point, where it is processed and displayed on the same device. This results in faster data processing and transmission with lower latency.
- *Wide geographical distribution*: Edge computing's ability to bring cloud capabilities closer to the local level significantly enhances the performance of IoT applications. It can serve a wide geographical area in applications like smart homes and smart cities.
- *Real-time applications*: Due to its low latency characteristics, edge computing provides robust data streaming capabilities, making it suitable for real-time applications. It improves the performance of applications that require instant data processing and response.
- *Security*: In an IoT application using cloud computing, edge nodes can perform computations and encryption tasks that resource-constrained end devices cannot. This helps protect data when it is transmitted over a potentially insecure internet environment.

Edge computing is widely used in various fields, including autonomous vehicles, smart grids, smart cities, smart homes, remote monitoring in hazardous areas, patient tracking, radio networks, 5G, and traffic management.

The security requirements for edge systems are primarily based on the general principles of the CIA model (confidentiality, integrity, and availability). To ensure these principles are met, the following methods are necessary for edge systems:

- *Secure encryption algorithm*: A secure encryption algorithm is essential to ensure data confidentiality. However, when selecting an encryption algorithm, the system's computational load should also be considered. Additionally, it is crucial to choose a quantum-resistant encryption system since some traditional encryption methods have vulnerabilities in post-quantum computation.
- *Mechanisms such as hash and session keys*: These mechanisms are used to ensure data integrity and to detect certain attacks like MitM and malware injection (Ranaweera et al., 2021). They provide methods to guarantee the immutability of messages, preventing data manipulation, or destruction.
- *Node capture and eavesdropping prevention*: Edge systems must prevent attacks like Relay, MitM, and Sybil. These attacks can occur by compromising end nodes, primarily because IoT devices often have lower levels of encryption and integrity checks, posing a higher risk when channels connecting to MEC edge systems are compromised (S. Wang et al., 2019).
- *Availability*: To address availability issues in edge systems, mechanisms to prevent common types of attacks like Jamming and Denial of Service (DoS) should be implemented. These attacks can lead to problems related to the radio resource control (RRC) connection status (Ranaweera et al., 2021). Additionally, continuous monitoring of storage and maintenance status is necessary for availability.
- *Malicious node prevention*: The diversity of end devices connected to base stations can lead to incompatibilities between communication protocols developed by different manufacturers. This can provide attackers with opportunities to integrate malicious nodes into the system and exploit security vulnerabilities (Ranaweera et al., 2021). Protection against these attacks includes measures such as device cloning, spyware, trojans, and other types of malicious software. Authentication approaches, as one of the principles of security, are essential; each end node must go through an authentication process when joining the system.

4 | POST-QUANTUM SECURITY

In this section, existing and post-quantum encryption systems, the requirements for achieving quantum-resistant security in IoT applications, and the types of PQC are discussed. Encryption algorithms play the most crucial role in ensuring the security of information systems. While theoretically, brute force attacks on encryption systems are not feasible

due to the absence of encryption keys, in practice, the security of encryption systems relies on the fact that brute force attacks do not yield results in real-time. However, with the development of quantum computers, certain encryption systems can be broken in real-time due to their high-speed computational capabilities (Karacan et al., 2022).

Today, the difficulty of solving NP-hard issues is used to assess the security of encryption systems. AES, one of the most powerful symmetric encryption systems, is secure due to the complexity of its operations, which include byte swapping, row and column shifting, and key XORing (Karakaya & Ulu, 2023). The difficulty of factorization makes RSA, one of the most well-known public key techniques, secure, whereas the difficulty of solving the discrete logarithm issue makes ECC secure. Quantum computing has the potential to solve NP-hard issues. The largest issue, however, is that today's encryption solutions based on public key cryptosystems are vulnerable to quantum attacks. After quantum, the effect of secure symmetric encryption systems like AES reduces (AES with 256-bit keys is as effective as AES with 128-bit keys), while the influence of secure public-key systems like RSA and ECC totally vanishes (Chen et al., 2016; Karacan et al., 2021). As a result, today's encryption techniques are unsuitable for the post-quantum future and create privacy issues. However, progress is being made on quantum computing-based encryption systems, quantum-resilient protocols, and security techniques. The methods of Shor and Grover can be used to determine if encryption systems can be cracked by quantum computers. As a result, robust encryption systems and protocols in PQC may be constructed.

To ensure that both existing and newly developed encryption systems are secure in the context of post-quantum computing, the following factors need to be assessed (Asif, 2021):

- *Key size*: The size of encryption keys plays a critical role in post-quantum security. As quantum computers are capable of more efficient factorization and searching algorithms, longer key sizes are often necessary to maintain security. Evaluating the appropriate key size for encryption systems is essential to resist quantum attacks.
- *Processing time for encryption*, *decryption*, *and signing*: The time it takes to perform encryption, decryption, and signing operations in a post-quantum context is crucial. Post-quantum encryption systems should aim to provide efficient and timely cryptographic operations to support real-world applications.
- *Traffic overhead for encryption*, *decryption*, *and signing on the transmission line*: The amount of additional data transmitted during encryption, decryption, and signing processes can impact network efficiency and bandwidth usage. Post-quantum encryption systems should minimize traffic overhead while still providing strong security.

For the development of quantum-resistant IoT systems, especially considering the resource-constrained nature of IoT devices, several key considerations and challenges must be taken into account (Asif, 2021):

- Latency caused by encryption and decryption at both ends of the communication connection, assuming a variety of devices from big and fast servers to sluggish and memory-restricted IoT devices.
- Limit the size of public keys and signatures for ultra-low latency.
- Clear network architecture that enables crypt-analysis and the discovery of vulnerabilities in a dense IoT network.
- Integration with current infrastructure is flawless.

Addressing these considerations will be essential in the development of quantum-resistant IoT systems that can effectively safeguard the security and privacy of IoT applications in a post-quantum.

PQC is typically categorized into four main sections, as shown in Figure 3. Since existing public key encryption (PKC) systems are not quantum-resistant, the systems developed in PQC often serve as replacements or alternatives to PKC counterparts.

4.1 | Code-based cryptography

Code-based cryptography is an approach that aims to address the vulnerability of today's public key systems to quantum attacks. It does so by embedding a series of codes into the message. The earliest of these systems is a PKC technique introduced in 1978 by Robert J. McEliece. The private key is a randomly generated binary irreducible Goppa code, and the public key is a randomly generated generator matrix of a randomly permuted version of that code. The ciphertext is a codeword with certain faults that can only be removed by the owner of the private key (the Goppa code; Overbeck & Sendrier, 2009).

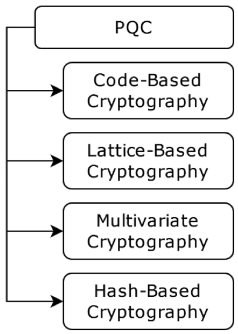

FIGURE 3 Types of post-quantum cryptography.

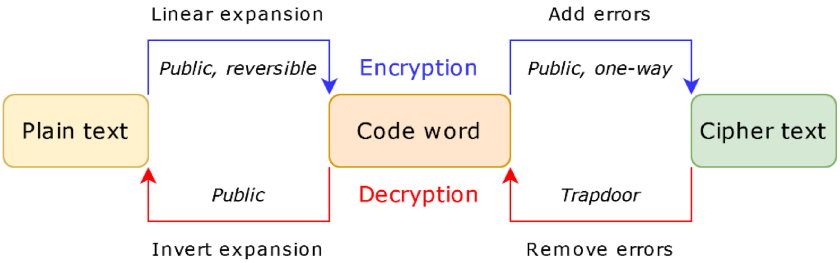

FIGURE 4 Code-based cryptography (McEliece; Bhattacharyya & Chakrabarti, 2022).

The public key serves as an arbitrary foundation for the code, allowing anybody to encrypt. Legitimate users who are aware of a hidden trapdoor can correct the faults and recover the cleartext. Adversaries are reduced to a general decoding task, which is thought to be difficult on average, even when faced with quantum adversaries (Sendrier, 2017). The general operation of code-based cryptography is depicted in Figure 4. McEliece is one of the most well-known methods within code-based cryptography.

4.2 | Lattice-based cryptography

The Ajtai–Dwork cryptosystem with proven security launched lattice-based cryptography (LBC) in 1997 (Ajtai & Dwork, 1997). The hidden hyperplane problem (HPP) underpins the cryptosystem.

In the LBC, the private key is defined as an n-dimensional secret vector for a positive integer n. The secret vector in n-dimensional space defines a periodic sequence of parallel equidistant hyperplanes: the secret vector is perpendicular to the hyperplanes, and its length is inversely proportional to the distance between subsequent hyperplanes. The public key is described as a collection of points that belong to one or more hyperplanes. Each plaintext bit is encrypted in an n-dimensional point. If the message bit is set to 0, the ciphertext is uniformly random. The ciphertext is the centroid of a uniform subset of the public key points if the message bit is 1. Decryption is accomplished by projecting the ciphertext point from the private key onto the secret vector (scalar product with a unit vector), with the message being 1 if the point is near to one of the hyperplanes and 0 otherwise (Mohsen et al., 2017).

In this cryptosystem, to extract the private key from the public key, a brute-force search of all possibilities is required, and even if quantum computers could speed up this search, it is still take a significant and unreasonable length of time. Even a quantum computer is assumed to be incapable of solving challenging lattice-based tasks in an acceptable amount of time.

LBC initially started as a theoretical concept and was not particularly efficient. However, subsequent research and developments have been aimed at making it both secure and efficient as a cryptographic system. Two well-known types of LBC are the Nth-degree truncated polynomial ring (NTRU) and the bimodal lattice signature scheme (BLISS). LBC has emerged as one of the most widely used types of PQC, offering robust security in the post-quantum era.

4.3 | Multivariate public key cryptography

Multivariate public key cryptography (MPKC) is secure because solving a random system of multivariate polynomial equations over a finite field is known to be an NP-hard task (Dey & Dutta, 2023). Therefore, it is a promising cryptosystem for the future.

Many public key multivariate quadratic equation systems are used in cryptography as both the public key and a portion of the private key. Although the issue can be defined in more general rings, it is believed that all such equations occur over finite fields. Due to two supposedly challenging difficulties, these systems are being explored. The multivariate quadratic (MQ) problem comes first. The IP problem, or isomorphism of polynomials problem, is the second. The security of MQ-based encryption techniques depends on how challenging it is to solve an apparently random instance of the MQ problem and the IP problem (Feldmann, 2005).

The private key must be challenging to decipher from the public key in order to be secure. Therefore, the IP issue must be challenging. The MQ problem must be maintained challenging for security reasons as well. If the MQ problem is quickly resolved, then the corresponding plaintext for every cipher text can be quickly determined by resolving one instance of the MQ problem.

4.4 | Hash-based cryptography

Merkle's hash-tree public-key signature system, developed in 1979 and based on Lamport and Diffie's one-message-signature concept, is a classic example (Bernstein, 2009). Like other digital signature techniques, hash-based schemes utilize a cryptographic hash function. The collision resistance of that hash function is essential for their security. You may think of collision-resistant hash functions as a necessary but not sufficient condition for a digital signature system that uses a single private key to sign several documents. A new hash-based signature technique is produced by every new cryptographic hash function. Therefore, difficult algorithmic difficulties in number theory or algebra are not necessary for the development of secure signature methods. The sole thing on which hash-based signature systems rely is symmetric cryptography (Balasubramanian, 2018).

Hash-based signatures are important due to their minimal security assumptions and flexibility. Hash-based signature schemes, such as the extended Merkle signature scheme (XMSS), require only a secure cryptographic hash function for their security. As long as a secure signature algorithm exists, it can be proven that a secure instance of XMSS exists. This demonstrates that hash-based signatures have low requirements for security.

These schemes can be initialized with any hash function that meets simple criteria and can be modified without breaking the overall structure. This flexibility makes hash-based signature schemes versatile (Butin, 2017). XMSS, an example of such a scheme, is shown in Figure 5.

5 | POST-QUANTUM BASED APPROACHES FOR EDGE COMPUTING SECURITY

In this section, post-quantum based methods for edge computing security are examined, with a particular focus on their relevance to IoT systems. Edge computing brings cloud-like capabilities closer to the edge, which enhances the efficiency of data processing and storage systems such as cloud and fog computing. Being closer to the devices where data is generated or results are displayed reduces latency and enhances the relative security of data. However, edge systems in the IoT environment also require additional security.

Currently, many traditional security methods have been developed and used in edge computing systems. However, the advancement of quantum computing introduces a new dimension of security challenges. This necessitates the development of methods, schemes, and protocols for security in IoT systems that are quantum-resistant, considering the evolving landscape of quantum computing.

5.1 | Research methodology

Research on the security of quantum-resistant edge computing systems and devices is relatively limited. Therefore, this study aims to draw attention to the field of quantum-resistant IoT and edge computing. The research methodology

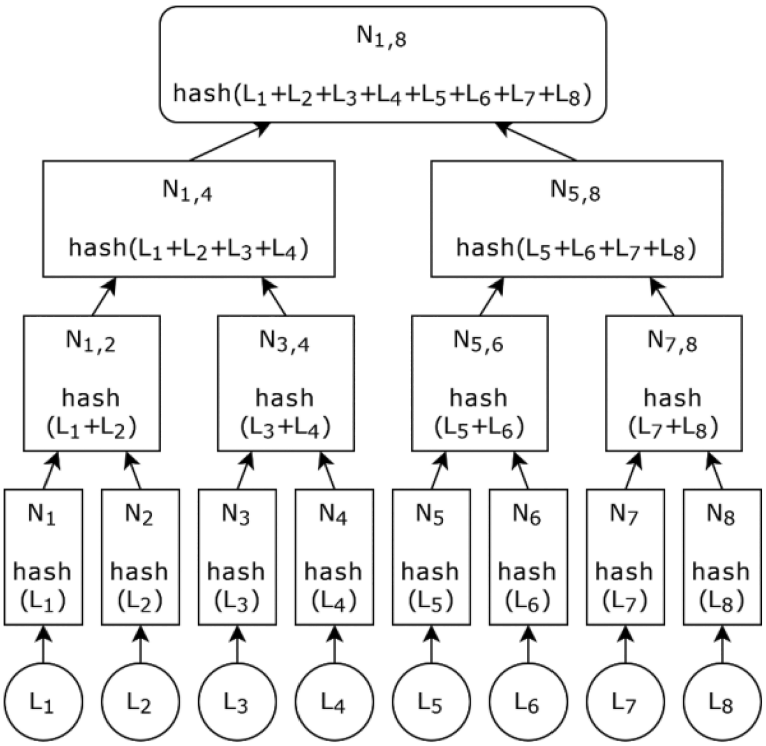

FIGURE 5 Extended Merkle signature scheme (XMSS).

involves conducting a literature review by gathering relevant studies and publications from several key databases using three types of queries: ["post-quantum" AND "edge" AND "security"] (RM1), ["quantum resistant" AND "edge computing" AND "security"] (RM2), and [("quantum" OR "post-quantum") AND ("edge" OR "MEC") AND "security"] (RM3). In this paper, the results obtained from three research methods named RM1, RM2, and RM3 are examined from the Web of Science Core Collection (WoS), Scopus, Institute of Electrical and Electronics Engineers (IEEE), Association for Computing Machinery (ACM), Elsevier, and Multidisciplinary Digital Publishing Institute (MDPI) databases. The graph containing the quantities of articles obtained from research methods is shown in Figure 6.

In Wos, Scopus, IEEE, ACM, Elsevier, and MDPI numbers of papers that have been searched are 37, 50, 25, 33, 6, and 84, respectively, for RM1, while for RM2 it is 3, 3, 2, 8, 0, and 26. Lastly, for RM3 numbers of papers that have been searched are 99, 253, 189, 762, 22, and 66. The number of publications per year for RM1, RM2, and RM3 are presented in Figure 7. Here, the total number of reviewed articles for RM1, RM2, and RM3 is presented based on years. As can be observed from the figure, the number of studies in this field has increased over the years.

The paper focuses only on the studies relevant to the area we are interested in and examines them in detail.

5.2 | Reviewed papers

In this section, as part of the research method, studies obtained from the literature are filtered to focus on those relevant to the area under investigation and are examined in detail. The bibliometric analysis of these studies is presented in Table 3.

In Zhao et al. (2022), a domain-specific processor based on a RISC-V matrix extension was suggested to enable a high-performance implementation of Module-LWE applications for the edge computing paradigm. The method has been compared to state-of-the-art crypto processors. It is reported to provide improvements in terms of the number of cycles, with a 3.5 times improvement over Kyber and a 3.3 times improvement over Dilithium. In Xu et al. (2023), a solution to the problem of increasing server processing time due to data encryption on edge devices before transferring them to the cloud was proposed. To address potential risks from quantum computers, a lattice-based protocol that achieves better performance in both time and storage for edge devices was presented. As a result, significant performance improvements have been achieved, with approximately 123 × −238× acceleration in the key derivation process,

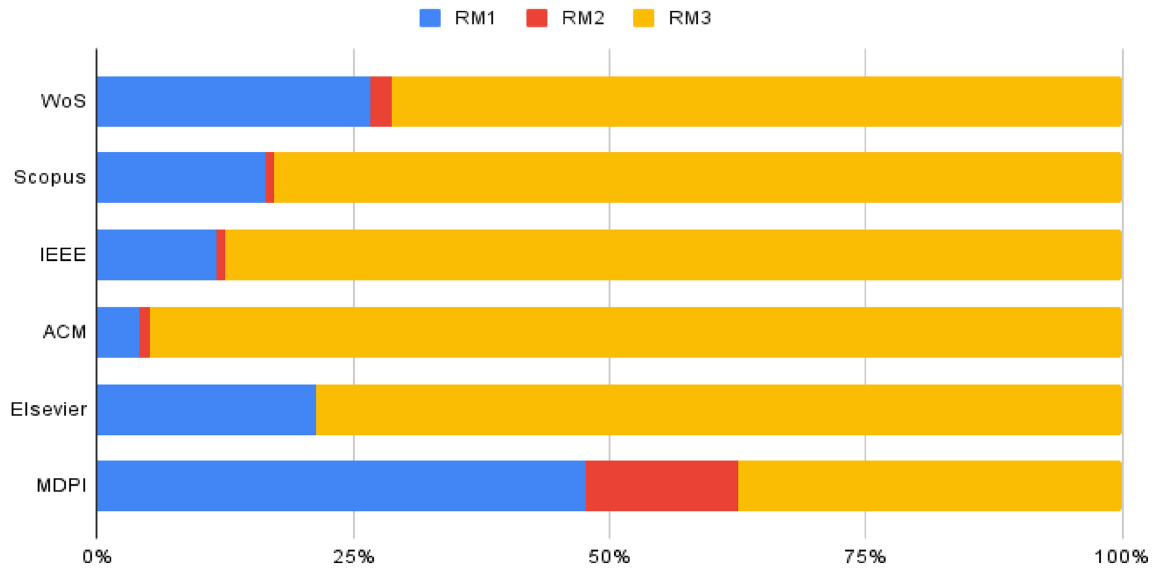

FIGURE 6 The chart displays the quantity of papers acquired from the databases.

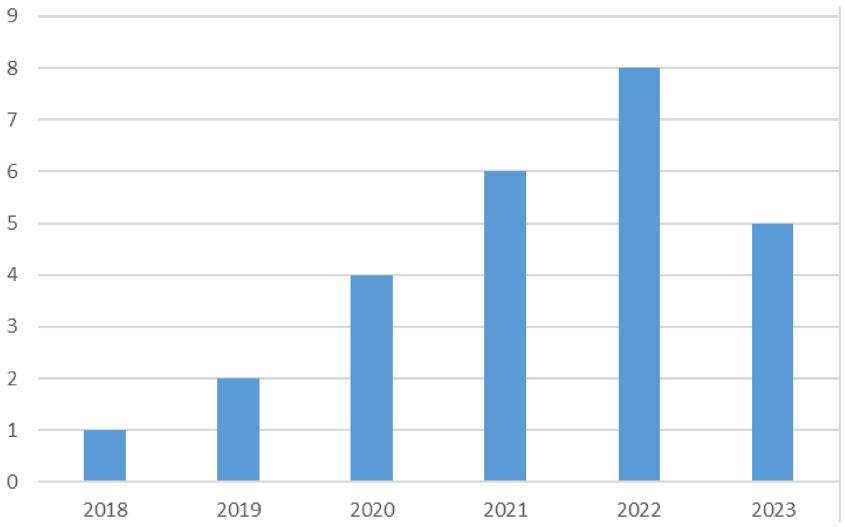

FIGURE 7 Total number of reviewed papers for RM1, RM2, and RM3.

and a reduction in the storage cost of the secret key from 547 to 1.7 MB. In El Kassem et al. (2019), due to the potential loss of efficiency of existing encryption and signing structures with the emergence of quantum computers, a quantum-resistant lattice-based direct anonymous attestation (DAA) scheme was proposed. It is claimed that as compared to the previous DAA technique with conjectured post-quantum security available, the TPM storage needs were cut in half, signature sizes were reduced five times, and signing and verification procedures were sped up by 1.1 and 2.0 times, respectively.

In Lizardo et al. (2021), Sharelock, a security protocol that guarantees end-to-end security and secrecy of communications exchanged by groups of communicating nodes, was suggested. It is mentioned that trials have been conducted with numerous post-quantum encryption systems, and any of them with suitable parameters can become quantum-resistant. In Kim, Song, Youn, and Seo (2022), when performing the Cristals–Dilithium application, ARMv8-based microcontrollers are used instead of the standard approach of RISC machines. To enhance the performance of Dilithium, the architectural features of ARMv8, including its large register sets and the NEON engine, are utilized to optimize number–theoretic–transform (NTT) based polynomial multiplication. These optimization methods are highlighted to have resulted in approximately 43.83% improvement in key pair generation, 113.25% improvement in

TABLE 3 Bibliometric analysis (all journal articles).

Author(s) & year	Title	Quartile	Impact factor	Number of citation
(El-Latif et al., 2018)	Secure quantum steganography protocol for fog cloud Internet of Things	Q2	3.476	72
(Ebrahimi et al., 2019)	Post-quantum cryptoprocessors optimized for edge and resource-constrained devices in IoT	Q1	11.1	39
(El Kassem et al., 2019)	More efficient, provably-secure direct anonymous attestation from lattices	Q1	7.4	4
(El-Latif et al., 2020)	Providing end-to-end security using quantum walks in IoT networks	Q2	3.476	41
(J. Wang et al., 2020)	Lattice-based incremental signature scheme for the authenticated data update in fog computing	Q2	4.1	1
(Nakkar et al., 2020)	Lightweight broadcast authentication protocol for edge-based applications	Q1	10.6	15
(Xin et al., 2020)	VPQC: A domain-specific vector processor for post-quantum cryptography based on RISC-V architecture	Q1	5.1	38
(Akleylek et al., 2021)	Novel post-quantum MQ-based signature scheme for internet of things with parallel implementation	Q1	10.6	5
(Dharminder et al., 2021)	Post-quantum secure conditional privacy preserving authentication for edge based vehicular communication	Q3	2.7	1
(Lizardo et al., 2021)	End-to-end secure group communication for the Internet of Things	Q2	5.1	4
(Shahbazi & Ko, 2021)	Area and power efficient post-quantum cryptosystem for IoT resource-constrained devices	Q2	2.2	12
(Wong et al., 2021)	High-speed RLWE-oriented polynomial multiplier utilizing Karatsuba algorithm	Q2	3.9	9
(Lu & Li, 2021)	Quantum-resistant lightweight authentication and key agreement protocol for fog-based microgrids	Q2	3.476	2
(Kim, Song, & Seo, 2022)	Accelerating Falcon on ARMv8	Q2	4.1	3
(Kim, Song, Youn, & Seo, 2022)	Crystals-Dilithium on ARMv8	Q3	2.079	2
(Kumari et al., 2022a)	Signature based Merkle Hash multiplication algorithm to secure the communication in IoT devices	Q1	8.6	2
(Kumari et al., 2022b)	To secure the communication in powerful Internet of Things Using Innovative Post-Quantum Cryptographic Method	Q2	2.7	3
(Li et al., 2022)	A novel privacy-preserving multi-level aggregate signcryption and query scheme for Smart Grid via mobile fog computing	Q1	5.6	2
(P. Wang et al., 2022)	Lattice-based public key searchable encryption with fine-grained access control for edge computing	Q1	7.4	5
(Señor et al., 2022)	Analysis of the NTRU post-quantum cryptographic scheme in constrained IoT edge devices	Q1	11.1	–
(Zhao et al., 2022)	A high-performance domain-specific processor with matrix extension of RISC-V for module-LWE applications	Q1	4.5	4
(Xu et al., 2023)	Towards efficient cryptographic data validation service in edge computing	Q1	7.6	3
(Lee et al., 2023)	Configurable encryption and decryption architectures for CKKS-based homomorphic encryption	Q2	3.9	–
(Shahidinejad & Abawajy, 2023)	Decentralized lattice-based device-to-device authentication for the edge-enabled IoT	Q2	4.3	–

TABLE 3 (Continued)

Author(s) & year	Title	Quartile	Impact factor	Number of citation
(Zhu et al., 2023)	Resource allocation in quantum-key-distribution-secured datacenter networks with cloud–edge collaboration	Q1	10.6	2
(Corrias et al., 2023)	Implementation of Italian industry 4.0 quantum testbed in Turin	–	–	–

signing, and 41.92% improvement in verification when compared to the reference implementation submitted for the final round of the NIST PQC competition for Dilithium 3.

In Wang et al. (2020), a lattice-based incremental digital signature system was presented to efficiently authenticate updated data in fog computing. It is stated that the shortest integer solution is based on the hardness of the standard model, its security can be proven, it is suitable for parallel computation, and when compared to other known lattice-based signatures, both the public key size and the signature size are shorter. In Kim, Song, and Seo (2022), the performance of the post-quantum signature algorithm Falcon is optimized using the NEON engine, which is the parallel processing unit in ARMv8 microprocessors. ARMv8 is widely used in various IoT applications, edge computing devices, and autonomous driving systems. They have developed both FFT (Fast Fourier Transformation) and NTT (Number Theoretic Transform) based multiplication methods. As a result, it is claimed that during FFT/NTT-based polynomial multiplication, the number of auxiliary memory accesses is minimized. Additionally, it is asserted that FFT provides a performance increase of 15.1% in key pair generation, 16.5% in signing, and 65.4% in verification, while NTT offers a performance increase of 18.1% in key pair generation, 17.1% in signing, and 69.4% in verification.

In (Kumari et al., 2022a), to secure communication in today's and tomorrow's IoT networks, the signature-based Merkle hash multiplication (SMHM) method was presented as an upgraded hash-based PQC architecture. To secure data storage and communication in IoT devices, the hash-based Merkle signature technique was augmented with the Bernoulli Karatsuba Multiplication algorithm. It is reported that the performance metrics were calculated using the hardware descriptive language (HDL) and high-level synthesis (HLS) technique, which improved 33% frequency, 22% area, power consumption up to 13%, 10% error, and 15% delay. In Wang et al. (2022), an effective lattice-based searchable PKC method with detailed access control for edge computing was proposed. It achieved quantum-resistant properties when transmitting data from edge systems to cloud systems. This approach used the LWE assumption and subset predicate encryption to achieve post-quantum security and extremely flexible access control rules for multi-user applications. According to the security proof, the proposed system was safe against selected plaintext and keyword attacks and was quicker than previous alternatives.

In Dharminder et al. (2021), a lattice-based quantum-resistant system was proposed for mobile nodes in a network system that includes smart devices to establish reliable communication with vehicles or usable roadside units (RSUs). Traditional methods were criticized for not being quantum-resistant and for having disadvantages such as the inability to verify previously transmitted messages repeatedly and failing during batch verification to search for messages that are no longer valid. An RSU may quickly check messages from adjacent genuine cars and disseminate them to all vehicles within its communication range, resulting in less duplicate message verification. As a result, an enhanced design based on the difficulty of a short integer solution in some random lattice was presented to assure security against quantum assaults. This system is said to ensure autonomous driving, regular vehicular traffic flow, and a revocation procedure in the advanced quantum future. In (Shahbazi & Ko, 2021), a novel multiplication approach dubbed in-place modular reduction and anti-circular rotation column-based multiplication (In-place Rot-Col-Mul) is presented, as well as a new Ring-BinLWE architecture. It is claimed that the implementation results indicate a 48.42% and 57.8% increase in power and area over the state-of-the-art design, respectively.

Señor et al. (2022) explored the post-quantum security of a custom wireless sensor node designed for IoT applications at the edge using NTRU. The cryptographic system was implemented within the processes of the Contiki-NG operating system. Additional experiments were carried out to see if commonly integrated hardware cryptographic peripherals inside modern microcontrollers can be used to improve NTRU performance at the single node and network levels, where the NTRU key encapsulation mechanism is tested in a real communication process. According to the findings, NTRU is appropriate for current microcontrollers targeting wireless sensor network architecture, however, older devices may not be able to pay the expense of its implementation. In Ebrahimi et al. (2019), InvRBLWE was offered as

an improved variation for binary learning with errors over the ring (Ring-LWE) technique that is safe against quantum attacks and very efficient for hardware implementations. Two designs were proposed: a high-speed architecture for edge and powerful IoT devices, and an ultra-lightweight architecture for resource-constrained IoT nodes. When compared to earlier classical and post-quantum applications, the best results were obtained, and two separate applications specific integrated circuit (ASIC) implementations demonstrated improvements in terms of speed, area, power, and/or energy.

In Wong et al. (2021), an improved SPMA-Karatsuba (schoolbook polynomial multiplication method) architecture was developed, along with a unique technique for implementing negacyclic convolution. It is claimed that the suggested design is more than 2.09 times quicker at the expense of 96.06% more hardware resources than the state-of-the-art SPMA architecture. This is especially handy for designing IoT edge nodes or gateway devices that demand a high level of performance. In Kumari et al. (2022b), it was introduced a revolutionary diffie supersingular multiplication (DSM) for safeguarding communication in powerful IoT devices. The developed approaches were validated by launching a Mirai botnet attack in the transmission channel and were implemented using the Xilinx ISE14.5 tool, which improved 30% frequency, 24% area, 10% confidentiality rate, and reduced power by up to 15%, error by 10%, and delay by 20%. It is claimed that the suggested strategy outperformed the other strategies tested.

Lu and Li (2021) presented a quantum-resistant authentication protocol designed for microgrids, establishing mutual authentication and a secure session key between a smart meter and a fog node. The protocol exhibited resilience against quantum attacks, leveraging the NP-complete LPN problem. Additionally, the suggested protocol boasted reduced computational and message costs. In El-Latif et al. (2020), the authors proposed a novel lightweight image encryption technique leveraging quantum walks (QW) to ensure secure data transfer within IoT platforms and wireless networks with edge computing capabilities. This innovative approach harnessed the nonlinear dynamic behavior of QW to create permutation boxes and generate pseudo-random numbers for encrypting individual blocks of the original image. By tapping into the nonlinear dynamics of QWs, the presented solution produced pseudo-random number sequences and constructed permutation boxes. Initially, the plain image was partitioned into blocks, which were then further subdivided into two segments. Each segment undergoes permutation and substitution processes with its respective permutation box and pseudo-random number sequence, derived from the probability distribution of active QW. Subsequently, the encrypted blocks were amalgamated and subjected to XOR operation with another pseudo-random number sequence to form the final encrypted image.

Li et al. (2022) introduced an innovative approach to privacy protection in Smart Grid systems incorporating mobile fog computing and a quantum key pool. First, it was devised a dynamic and multi-tiered privacy-preserving aggregate signcryption technique that operates without the need for a trusted authority. This included both space-based and time-based data aggregation. To bolster key management security, it was incorporated a quantum key pool for efficient key distribution. Second, it was deployed a data query and sharing method based on proxy re-encryption. This not only enabled users to inquire about historical data and bills, but also ensured secure data sharing with third-party entities. El-Latif et al. (2018) introduced a fresh framework designed for safeguarding information within the context of fog cloud IoT. Within this framework, a user at one location concealed their valuable data using the proposed quantum steganography protocol, and then uploaded the concealed data to the fog. Subsequently, the intended recipient at a different location retrieved the data from the fog and unveiled the intended content using the proposed extraction method. The paper also presented an original quantum steganography protocol founded on hash functions and quantum entangled states. Notably, no prior quantum steganography protocol has been identified to authenticate an embedded secret message. In this suggested protocol, a hash function was employed for this authentication process. The protocol outlined herein was resilient against recognized forms of attack, including message, MitM, and no-message attacks. Furthermore, it operated without the need for additional channels beyond the one proposed for sending a secret message or verifying security.

Xin et al. (2020) explored the process of vectorizing kernel algorithms for various candidates in LBC. They introduced a specialized vector processor named VPQC, designed within the extensible RISC-V architecture. VPQC incorporates a vector Number Theoretic Transform (NTT) unit to facilitate parallel computation across different dimensions (ranging from 64 to 2048). Additionally, a vector sampler capable of performing both uniform and binomial sampling was integrated. When assessed using TSMC 28 nm technology, the vector coprocessor of VPQC utilized 942 k equivalent logic gates and 12 KB of memory. Experimental results demonstrated that VPQC achieves a significant speedup, improving the performance of several common key encapsulation mechanisms (such as NewHope, Kyber, and LAC) by an order of magnitude compared to previous state-of-the-art hardware implementations. Lee et al. (2023) proposed efficient hardware architectures for CKKS-based ENC-DEC accelerators to facilitate computations on the client side. The proposed architectures are configurable to support a wide range of polynomial sizes with multiplicative depths (up to

30 levels) at a 128-bit security guarantee. They evaluated the hardware designs on the Xilinx XCU250 FPGA platform and achieved an average encryption time of 23.7 times faster than that of the well-known SEAL HE library. By reducing time complexity and improving the hardware utilization of cryptographic algorithms, their configurable CKKS-supported ENC-DEC hardware designs have the potential to greatly accelerate cryptographic processes on the client side in the post-quantum era.

A datacenter network secured through quantum key distribution (QKD-DCN) with collaborative cloud-edge capabilities can effectively address the communication, computation, caching, and cryptographic (4C) requisites of various services. Zhu et al. (2023) pioneered a solution for the novel 4C resource-allocation (4CRA) problem within the network, aiming to minimize cryptographic resource utilization. The authors devise an integer linear programming (ILP) model and put forth a heuristic cryptographic-dependent 4CRA algorithm to identify optimal solutions. This algorithm was benchmarked against two baseline 4CRA algorithms, one prioritizing minimized service delivery latency and the other focusing on first-fit resource availability. Analytical simulations demonstrated that the proposed algorithm achieves a reduction in the key-resource-consumption ratio and average key-resource consumption, under both static and dynamic traffic scenarios across diverse network topologies. Akleylek et al. (2021) introduced a novel signature scheme founded on multivariate polynomials, characterized by its efficient key and signature sizes. This scheme demonstrated resilience against quantum computer attacks and was designed for authenticating edge nodes in IoT. Moreover, the proposed scheme was highly amenable to parallel implementation, and allowed for the efficient deployment of edge node authentication with high throughput. When executed on a GPU device, the scheme achieved a signature generation rate of 113 signatures per second and a verification rate of 120 signatures per second. This represented a significant speedup, being 12.56 times faster for signature generation and 10.00 times faster for verification compared to a serial implementation on a CPU.

Nakkar et al. (2020) introduced a lightweight authentication protocol for forward secrecy in edge-based applications, reducing latency, minimizing cloud dependency, and efficiently utilizing cryptographic primitives on resource-constrained devices. The protocol involved secure session key derivation from a hash function and employed hash chains and authenticated encryption to withstand quantum attacks. It eliminated the need for permanent master keys and presented a smart emergency system use case. The protocol's computational complexity included three decryption operations, two HMAC, and five hash computations, with minimal storage and communication overhead (96 B and 56 B per session, respectively).

In Shahidinejad and Abawajy (2023), a decentralized authentication and key exchange protocol was proposed to reduce high storage costs, provide strong anonymity, and increase efficiency and privacy using LBC, edge computing, and blockchain technology. The protocol was claimed to be resilient against many known classical attacks, such as the ephemeral secret leakage attack and public-key quantum attack. The results obtained during the Italian Industry 4.0 Quantum Test Environment (II4QuTe) project, reported in Corrias et al. (2023), show that the authors implemented a QKD testbed that securely connects the Competence Industry Manufacturing 4.0 (CIM4.0) located in Turin to a TIM edge node located 10 km away. The edge node hosts the server that provides computing capabilities for managing real-time data generated by the machines on the CIM4.0 digital factory pilot line, thus elegantly integrating QKD with the MEC paradigm.

The summary of quantum-resistant approaches for edge computing security is shown in Table 4. Post-quantum security for edge systems is a current topic, which is why there are relatively fewer studies, and these studies are quite recent.

Post-quantum-based approaches for edge computing security are analyzed in detail in Table 5. The techniques used contributions, the specific focus of the study, as well as the method's testing environment and performance metrics, are evaluated. Furthermore, the strengths and weaknesses of the proposed methods or the entire article are also assessed. These sections aim to provide readers with preliminary information about the information contained in the articles and the limitations of the article, enabling them to assess whether the desired content is present in the paper.

6 | DISCUSSION AND FUTURE DIRECTIONS

This section includes insights and analyses about the examined quantum-resistant edge computing systems, as well as directions for future research in this area. Edge systems face certain challenges, especially in terms of security, due to their resource-constrained nature. After processing data on edge devices, the results are transferred to the relevant system. Edge devices, being deployed in close proximity to the application, offer certain advantages such as low latency

TABLE 4 Post-quantum based approaches for edge computing security.

Paper	Problem/method	PQC type	Keywords	Result
(El-Latif et al., 2018)	A novel quantum steganography framework for secure messages in fog cloud IoT was presented. Secure information in fog cloud IoT	Hash-based	Quantum steganography, authentication, Internet of Things, fog computing, cloud computing	The suggested protocol exclusively relies on the proposed method for transmitting or verifying the secret message, without necessitating any additional quantum communications or states. The protocol's security is confirmed through the use of a hash function.
(Ebrahimi et al., 2019)	InvRBLWE approach that improved variation for binary learning with errors over the Ring-LWE technique	Lattice-based	Error-based, computer architecture, IoT	Improvement in speed, area, power, and/or energy in ASIC implementation
(El Kassem et al., 2019)	A quantum resilient lattice-based direct anonymous attestation (DAA) scheme was proposed.	Lattice-based	Cloud, edge, Direct anonymous attestation	The TPM storage needs were cut in half, signature sizes were reduced five times, and signing and verification procedures were sped up by 1.1 and 2.0 times
(El-Latif et al., 2020)	Suggest a novel, lightweight image encryption scheme utilizing quantum walks (QW) for secure data transmission within Internet of Things platforms and wireless networks with edge computing capabilities. Secure data transfers in IoT platforms	Lattice-based	Quantum walks, lightweight cipher, data transfer in IoT, image encryption, edge computing, wireless communication	High efficiency in terms of randomness tests, correlation coefficients, NPCR, information entropy, and histogram analysis.
(J. Wang et al., 2020)	To efficiently authenticate updated data in fog computing, a lattice-based incremental digital signature system was described.	Lattice-based	Fog computing, incremental signature, authentication	Proven security, suitable for parallel computation, both public key size and signature size are shorter than other lattice-based signatures, efficient bandwidth
(Nakkar et al., 2020)	A lightweight broadcast authentication protocol designed to offer forward secrecy for applications operating at the edge. Message broadcast protocol that ensures confidentiality, forward secrecy, and message integrity for resource-constrained IoT devices	Hash-based	Authenticated broadcast messages, authentication, edge computing, fog computing, forward secrecy	It provided secure broadcast messaging with low computational and storage needs, with a minimal communication overhead of only 56 bytes per session.
(Xin et al., 2020)	A cryptographic processor based on RISC-V is proposed to fulfill high-throughput and low-latency vector processing for LBC (Lattice-based cryptography). High-throughput and low-latency vector processing for LBC	Lattice-based	Post-quantum cryptography, ring-LWE, lattice-based cryptography, vector architecture, processor, RISC-V	The VPQC processor enhanced Post-Quantum Cryptography with significant speed improvements, making it ideal for various security applications.
(Akleylek et al., 2021)	Propose a new signature scheme based on multivariate polynomials with efficient key and signature sizes, which is resistant to quantum computer attacks. Security for the authentication of edge nodes in Internet of Things	MPKC	GPU, IoT, multivariate quadratic polynomials, postquantum cryptography	It requires fewer rounds compared to leading schemes and is GPU-compatible, ideal for IoT security.

TABLE 4 (Continued)

Paper	Problem/method	PQC type	Keywords	Result
(Dharminder et al., 2021)	An enhanced design based on the difficulty of a short integer solution in some random lattice was proposed to assure security against quantum assaults.	Lattice-based	Vehicle, edge, IoT, ad hoc network	Ensure autonomous driving, regular vehicular traffic flow, a revocation procedure, and post-quantum resistant
(Lizardo et al., 2021)	Sharelock, a security protocol that guarantees end-to-end security and secrecy of communications exchanged by groups of communicating nodes	Any with suitable parameters	End to end, group communication	It is stated that it was a flexible and low-cost protocol that secures database transactions regardless of encryption systems.
(Shahbazi & Ko, 2021)	A multiplication approach dubbed In-place modular Reduction and anti-circular rotation column-based multiplication (In-place Rot-Col-Mul), and a new Ring-BinLWE architecture.	Lattice-based	Hardware implementation, lightweight, Ring-BinLWE	48.42% and 57.8% increase in power and area, respectively
(Wong et al., 2021)	An optimized SPMA-Karatsuba (schoolbook polynomial multiplication algorithm) architecture	Lattice-based	Karasutba, hardware, memory management	More than 2.09 times quicker at the expense of 96.06% more hardware resources than the SPMA architecture.
(Lu & Li, 2021)	Introduces a quantum-resistant authentication protocol that establishes mutual authentication and generates a secure session key between a smart meter and a fog node. Privacy between main grid and microgrid	Any with suitable parameters	Quantum-resistant, LPN, microgrid, lightweight, fog, mutual authentication, key agreement	Quantum attack resistant, less message cost, and computational cost
(Kim, Song, & Seo, 2022)	Performance optimization of Falcon, one of the post-quantum signature algorithms, with the NEON engine in the ARMv8 microprocessor, which is also widely used as an edge computing device.	Lattice-based	Falcon, edge computing, FFT, NTT	FFT (15.1%) and NTT (18.1%) in key pair generation, FFT (16.5%) and NTT (17.1%) in signing, FFT (65.4%), and NTT (69.4%) in verification provide performance increase
(Kim, Song, Youn, & Seo, 2022)	Number theoretical transform-based polynomial multiplication optimization by taking advantage of ARMv8's large register sets and NEON engine's architectural features	Lattice-based	Optimization, polynomial multiplication	Compared to others, it achieves a performance increase of approximately 43.83% in key pair generation, 113.25% in signing, and 41.92% in verification.
(Kumari et al., 2022a)	Signature-based Merkle hash multiplication algorithm, an enhanced hash-based post-quantum cryptography architecture	Hash-based	Edge, IoT, Bernoulli Karatsuba	The performance measures increased by 33% frequency, 22% area, 13% power consumption, 10% error, and 15% delay
(Kumari et al., 2022b)	A novel Diffie supersingular multiplication (DSM) model	Any with suitable parameters	Supersingular multiplication, IoT, Mirai	The method outperformed the other methods tested.
(Li et al., 2022)	Introduces an innovative privacy-preserving multi-level aggregate signcryption and query scheme designed for Smart Grid systems. This	Any with suitable parameters	Smart grid, mobile fog computing, privacy-preserving, aggregate	Ensuring robust key management security, facilitating user queries for historical data and bills, and enabling statistical inquiries by third

(Continues)

TABLE 4 (Continued)

Paper	Problem/method	PQC type	Keywords	Result
	scheme incorporates mobile fog computing and utilizes a quantum key pool for enhanced security. The key management problem in smart grid		signcryption, quantum key pool	parties. Noteworthy for its high efficiency, lightweight design, and robustness
(P. Wang et al., 2022)	An effective lattice-based public key searchable encryption method with fine-grained access control for edge computing	Lattice-based	Edge, cloud, fine-grained access control	Proven in terms of security, secure against selected plaintext and keyword attacks, faster than previous alternatives
(Señor et al., 2022)	Post-quantum security testing of a custom wireless sensor node designed for applications at the edge of IoT using NTRU	Lattice-based	Wireless sensor network, edge, NTRU	NTRU is appropriate for current microcontrollers targeting wireless sensor network architecture
(Zhao et al., 2022)	A high-performance implementation of Module-LWE applications for the edge computing	Lattice-based	RISC-V, edge, module-LWE	3.5 times better than Kyber and 3.3 times better than Dilithium in cycle count
(Xu et al., 2023)	Due to the potential threats posed by quantum computers, a lattice-based protocol that achieves superior performance in both time and storage for edge devices has been developed.	Lattice-based	Edge, data validation	Approximately 123–238 times faster than similar studies in key derivation and the storage cost of the secret key decreased from 547 MB to 1.7 MB.
(Lee et al., 2023)	Efficient hardware architectures for CKKS-based ENC-DEC accelerators to facilitate computations on the client side. Optimizing encryption and decryption (ENC-DEC) operations on the edge side	Lattice-based	Homomorphic encryption, ring-LWE, NTT, hardware architecture	It considerably boosted homomorphic computations, with a 23.7× faster encryption time and 10.9× faster decryption time for end-users.
(Shahidinejad & Abawajy, 2023)	A decentralized authentication and key exchange protocol to reduce high storage cost, provide strong anonymity, increase efficiency and privacy	Lattice-based	Security protocol, edge, lattice	The method addresses major security challenges without burdening resource-constrained devices, paving the way for safer and more efficient smart homes, factories, healthcare systems, and even vehicle-to-vehicle communication.
(Zhu et al., 2023)	Proposed the cryptoD-4CRA heuristic for resource allocation in large networks, considering various constraints like communication, computation, caching, and cryptography, and an ILP model to optimize service resource consumption. Resource allocation in QKD-DCN	Any with suitable parameters	Caching, cloud–edge collaboration, datacenter networks, quantum key distribution (QKD), resource allocation	The algorithm considered node selection (CCNS) and path calculation (CQPC) while aiming for the lowest resource consumption.
(Corrias et al., 2023)	Integration using QKD-based method to connect the center and edge node in Industry 4.0	Any with suitable parameters	MEC, industry 4.0, QKD	In Industry 4.0, a QKD system successfully was used to encrypt sensitive data from sensors in real time. Thus, it paves the way for wider adoption of quantum technology in factories.

TABLE 5 Post-quantum-based approaches for edge computing security (more detailed).

Paper	Contribution	Used techniques	Focused area	Strength	Weakness	Test environment	Performance metrics
(El-Latif et al., 2018)	First quantum hiding protocol proposed to authenticate embedded secret data	Steganography, gray code, SDBM hash function	General (fog/edge/cloud computing performance improvement)	Embedding capacity, imperceptibility, man-in-the-middle attack, message attack, measurement attack, no-message attack	There is no simulation results	–	It was stated that the quantum steganography scheme is secure against common attacks.
(Ebrahimi et al., 2019)	Introduced InvRBLWE, a hardware-optimized Ring-BinLWE variant, with no reduction operations, providing superior speed on FPGA and ASIC platforms.	Ring-BinLWE	General (Security enhancement)	The method was elaborately explained, optimized, subjected to a side-channel analysis, implemented, and tested, and compared using numerous parameters.	More details could have been given about the test environment or scenarios.	ASIC using two different 65 nm TSMC and 45 nm Nangate standard cell libraries, FPGA with Xilinx Spartan-6	Time and AT were improved by at least 68% and 52%, respectively. Compared to best ECC practices, AT was improved by at least 92%.
(El Kassem et al., 2019)	A novel Direct Anonymous Attestation (DAA) approach based on lattices was offered. The scheme's security was demonstrated using the universally composable model. Storage and signature size decreased, and signing and verification became faster.	DAA, The Ring Short Integer Solution Problem, Ring-LWE, Discrete Gaussian Distributions	General (Performance improvement)	A new DAA approach was devised, and detailed mathematical proofs were supplied. Cost estimations were supplied, as well as comparisons of signature, verification, and key sizes.	Experiments were not detailed; only the results of the experiments were shared.	The encryption parameters used were $n = 256$, $q = 8{,}380{,}417$, $l = 32$, $m = 24$, and $\beta = 256$. The experiments were conducted on a machine with CentOS 7.5 operating system, equipped with a 3.3 GHz Intel i9 7900X CPU, 64 GB of RAM, and compiled using gcc 4.8.5.	Storage size is reduced by a factor of two when compared to the prior system, and signature size is reduced by a factor of five. The signing and verification procedures are both 1.1 and 2 times quicker.

(Continues)

TABLE 5 (Continued)

Paper	Contribution	Used techniques	Focused area	Strength	Weakness	Test environment	Performance metrics
(El-Latif et al., 2020)	A new lightweight cipher scheme using QWs. This system ensures secure IoT data transfers with lightweight design using Quantum Walks for confusion and PRNGs for diffusion.	Quantum walks (QW)	General (security enhancement)	High efficiency in terms of randomness tests, correlation coefficients, NPCR, information entropy, and histogram analysis.	–	6-GB RAM and Intel CoreTM i5 CPU 2.50-GHz with preinstalled MATLAB R2016b	The entropy value is close to 8, the number of the pixel change rate (NPCR) is greater than 99.61%, NIST SP 800-22 (randomness tests)
(J. Wang et al., 2020)	An incremental lattice-based signature scheme was presented with unforgeable security based on the shortest integer solution problem. Security (shorter signatures, smaller public keys, and faster algorithms) by concealing the message coding structure was improved.	Discrete Gaussian Distribution, Incremental Signature	General (fog/edge/cloud computing performance improvement)	The mathematical models of the scheme were provided, and it was simulated using Java. Accuracy, security, and efficiency analyses were conducted.	It was only compared with one similar study.	The scheme was simulated using Java on a PC with an Intel Core i7-8700K (3.7GHz) processor and 32GB of RAM.	Both public key size and signature length were shorter, run time better than 40.5% similar.
(Nakkar et al., 2020)	Introduce a lightweight message broadcast protocol for IoT devices with limited resources, ensuring confidentiality, forward secrecy, and message integrity. Showcase its application in a smart medical emergency scenario.	FEC-IoT Protocol, one-time-signature (OTS)	General (fog/edge/cloud computing performance improvement)	Less computational, less communication and storage overheads and message authenticity, confidentially, integrity	–	Two different benchmarks, a high-end Intel Core 2 Duo CPU 2.4 GHz, and a low-end microcontroller ARM Cortex-M0 48-MHz ATECC508A HW accelerated	Required storage for each node is only 96 B, communication overhead is only 56 B per session

TABLE 5 (Continued)

Paper	Contribution	Used techniques	Focused area	Strength	Weakness	Test environment	Performance metrics
(Xin et al., 2020)	Researched vectorization in NTT and sampling processes for NIST PQC candidates. Introduced VPQC, a high-throughput processor. Achieved tenfold speed increase using TSMC 28 nm CMOS technology.	Keccak-f[1600] for PRNG, Barrett reduction method for vectorized rejection sampler, constant-time binomial sampler	General (Security enhancement)	VPQC is able to support all Ring-LWE and Module-LWE key encapsulation schemes, low latency, high speed, energy efficient	The area cost of the proposed design is large	The complete processor, including the vector coprocessor and SCR1 core, was implemented and assessed using TSMC 28 nm HPC+ technology at 0.9 V supply voltage with Synopsys Design Compiler 2013.12-SP4 and PTPX 2013.12-SP3.	Architecture which in the cost of 942 k logic gates and 12 KB SRAM at 300 MHz frequency. The execution time of binomial sampling on VPQC can be 1.37 μs, complete the NTT computation with $q = 3329$ (used by the latest version of Kyber) in 0.137 μs which is 2349 times faster
(Akleylek et al., 2021)	A novel signature scheme based on quantum secure MQ hard problem was proposed. The first study that explore the implementation challenges of MQ-based cryptography on massively parallel platforms like GPUs.	Fiat–Shamir (FS) transform, commitment functions	General (fog/edge/cloud computing performance improvement)	EUF-CMA secure signature scheme, low impersonation probability (1/2), can be implemented in parallel architecture	–	Intel i9-7900X CPU at 3.30 GHz and RTX2060 GPU, embedded platform (Jetson Nano)	Impersonation probability 1/2, signature size 12.096 byte for 128-bit and 26.208 byte for 192-bit
(Dharminder et al., 2021)	The proposed design was focused on advanced conditional privacy-preserving signatures in the quantum era, ensuring security and efficient	Cuckoo filter, lattice-based cryptography	Vehicular communication	A mathematical model was presented, along with a detailed security analysis based on mathematical proofs. Performance was	The experimental study only covered timing information and did not encompass security conditions.	1000 trials were conducted on a Windows 7 computer with a 3.20 GHz Pentium processor and 2 GB of RAM.	It reduced the number of signature verifications, reducing the load on roadside units (RSUs) with limited resources. The time for 40

(Continues)

TABLE 5 (Continued)

Paper	Contribution	Used techniques	Focused area	Strength	Weakness	Test environment	Performance metrics
	authentication in advanced VANET systems through centralized processes and the utilization of Cuckoo filters.			evaluated, and a comparison was made with various parameters using similar methods.			messages was reduced to less than 25 ms.
(Lizardo et al., 2021)	An innovative IoT security approach was introduced, emphasizing privacy, performance, and quantum-resistant key management, while ensuring compatibility with resource-constrained devices.	Sharelock protocol	General (Security enhancement)	Node group communication received end-to-end security, complete with performance and quantum attack analysis.	The study had limited IoT attack coverage, lacked detailed experiments and comprehensive result evaluation.	MICAz wireless sensor node was used. The MICAz consists of an 8-bit ATmega128L MCU running at 7.37 MHz, featuring 4 KB of SRAM and 512 KB of flash memory, alongside a ZigBee CC2420 transceiver.	Adequate storage and computing power for resource-constrained nodes, flexible, low-cost, secure communications.
(Shahbazi & Ko, 2021)	A novel column-based multiplication technique was introduced for efficient modular reduction. Shift registers were utilized, leading to a 57.8% area reduction and a 48.42% power consumption decrease in ASIC implementation compared to the state-of-the-art design.	Ring-BinLWE, NTT-based polynomial multiplication	General (Security enhancement)	The method was described in detail, simulated, compared, and the results were thoroughly analyzed.	Possible attacks on the system have not been evaluated.	For simulation, ISE 14.7 and ISim 14.7 were used, and the simulation was performed in Python, ASIC, and FPGA using different test vectors. VHDL was used for ASIC, while Virtex was used for FPGA.	The maximum frequency of 500 MHz was reached and 48.42% and 57.8% power and area improvements were achieved compared to the state-of-the-art design.

TABLE 5 (Continued)

Paper	Contribution	Used techniques	Focused area	Strength	Weakness	Test environment	Performance metrics
(Wong et al., 2021)	A novel algorithm was proposed to reduce memory consumption and simplify nega-cyclic operations, achieving higher throughput than the state-of-the-art SPMA implementation.	Negacyclic convolution in R-LWE, Karatsuba algorithm, schoolbook polynomial multiplication algorithm (SPMA)	General (Performance improvement)	The method was explained in detail, algorithms were presented, implementation results were provided, and comparisons were made with previous studies.	A detailed security analysis has not been provided.	Implemented on a Xilinx Kintex 7 FPGA (KC705) using Vivado 2019.2 ISE.	Reduced the time and hardware needed by 66.15% and 100% respectively. 2.09 times faster than state-of-the-art SPMA architecture.
(Lu & Li, 2021)	A quantum-resistant lightweight authentication and key agreement (AKA). Three-layer network based on fog computing. A lightweight implementation of the smart meter in microgrid.	Random-HB# protocol to design AKA protocol and a three-layer network design based on fog computing	Smart grid	User anonymity, untraceability, perfect forward secrecy, resistance of man-in-the-middle attack, resistance of replay attack, resistance of impersonation attack, resistance of desynchronization attack	Storage overhead of the proposed protocol is larger than others	MacBook Pro personal computer as the server with a 4-core Inter Core i7 2.30GHz processor, 8GB main memory. To simulate a smart meter, we use a Raspberry Pi 4 Model B, built on the Broadcom BCM2835, ARMv7 Processor 1.5GHz and 2GB RAM. ProVerif tool	Message cost in largerly less than others. Total: 1647 bits, computational cost of proposed protocol is considerably less than others.
(Kim, Song, & Seo, 2022)	The initial effort to optimize Falcon software for ARMv8, including optimizing polynomial multiplication based on FFT/NTT for ARMv8-A devices,	Falcon, FFT/NTT-based polynomial multiplication, point-wise multiplication, butterfly method on ARM and NEON	General (Performance improvement)	All methods employed were extensively explained, algorithms were provided, results were evaluated, and a thorough comparison with	It was only compared with one similar study.	It was executed in an ARM Cortex-M4 environment using the AArch64-gnu-gcc 7.5.0 compiler on the Ubuntu 20.04 operating system.	A performance improvement of 15.1% in KeyGen, 16.5% in Sign, and 65.4% in Verify was attained when compared to Falcon Round 3 Submission

(Continues)

TABLE 5 (Continued)

Paper	Contribution	Used techniques	Focused area	Strength	Weakness	Test environment	Performance metrics
	and providing optimized Falcon software for all security parameters.			similar methods was presented.			based on Falcon-512.
(Kim, Song, Youn, & Seo, 2022)	The paper introduced the initial ARMv8-based Crystals Dilithium structure, emphasizing memory and NTT optimizations, which notably reduced memory access in NTT.	Crystals-Dilithium, NTT core operation, butterfly method on ARM and NEON, Point-Wise Multiplication on ARMv8	General (Performance improvement)	All methods employed were extensively explained, algorithms were provided, results were evaluated, and a thorough comparison with similar methods was presented.	No experimental work was included.	–	A 43.83% enhancement in KeyGen, 113.25% in Sign, and 41.92% in Verify processes was attained compared to the reference Crystals-Dilithium security level 3 implementation on ARMv8.
(Kumari et al., 2022a)	It was combined Hash-based Merkle and Bernoulli Karatsuba methods, was FPGA-evaluated, and was tested against Mirai botnet and side-channel attacks. Performance metrics were compared with existing approaches using Xilinx ISE 14.5.	Signature based Merkle hash multiplication (SMHM) algorithm, Bernoulli Karatsuba multiplication algorithm	General (Security enhancement)	Algorithms were provided, and analyses against botnet and side-channel attacks were conducted. Experimental results were presented in detail and compared with several known methods.	–	Simulated using the Xilinx ISE 14.5 simulator on a computer with an Intel i5 processor and Windows 10 operating system. The simulation was conducted in Verilog-HDL. A registry was created for 25 IoT devices.	Enhanced frequency by 33%, reduced area by 22%, lowered power consumption by up to 13%, minimized errors by 10%, and decreased delay by 15%.
(Kumari et al., 2022b)	A new PQC method called DSM has been proposed to ensure the security of IoT channels on	DSM algorithm, Mirai	General (Security enhancement)	The method's details, algorithms, implementation, analysis against Mirai botnet	A detailed security analysis has not been provided.	Xilinx ISE14.5 tool on Windows 10 Operating System with Intel	Improved 30% frequency, 24% area, 10% confidential rate and reduced the

TABLE 5 (Continued)

Paper	Contribution	Used techniques	Focused area	Strength	Weakness	Test environment	Performance metrics
	powerful devices using Xilinx Software. It was tested against the Mirai botnet attack.			attacks, performance evaluation, and comparisons with similar methods have been presented.		i5 processor was used.	power up to 15%, error 10% and 20% delay.
(Li et al., 2022)	Designed a versatile signcryption technique for multi-level aggregation, eliminating the need for a trusted authority. Enabled both space-based and time-based data aggregation, along with secure data queries and sharing.	Key distribution algorithm based on quantum key pool, signcryption with AES, Multi-level data aggregation, group-based data query scheme, blockchain technology for revocation and dynamic updating	Smart grid	Low computational complexity, fast key distribution, revocation and dynamic updating, and general security requirements	High communication cost	Hyperledger Fabric (v2.3.3) platform on VMs Ubuntu 20.04. The simulation environment is Intel(R) Core (TM) i5-10,400 CPU @ 2.90 GHz * 2.90 GHz, 16.0 GB RAM, Windows 10, VMware(R) Workstation 15 Pro, Ubuntu 20.04, Pairing-Based Cryptography (PBC) library.	Computational complexity, communication cost, and general security (false message inject attack, message tampering attack, replay attack, robustness)
(P. Wang et al., 2022)	The paper presented a lattice-based public key searchable encryption scheme with fine-grained access control. It offers post-quantum security and has formal security proofs. Extensive experiments confirmed its practicality for edge	Lattice-based cryptography, LWE problem	General (fog/edge/cloud computing performance improvement)	Mathematical models were presented, proofs were discussed in detail, complexity was calculated, a detailed experimental result was provided, and performance was compared with many similar studies.	–	The experiments were performed on a Windows 10 PC with an Intel Core i5-9600KF processor and 8GB of RAM, as well as a Raspberry Pi 4B running Raspbian GNU/Linux 10 (Buster) with an	3630 KB private key size, 180.688 KB ciphertext size, 300 KB trapdoor size

(Continues)

TABLE 5 (Continued)

Paper	Contribution	Used techniques	Focused area	Strength	Weakness	Test environment	Performance metrics
	computing by assessing time and memory costs.					ARM Cortex A72 processor and 2 GB of RAM.	
(Señor et al., 2022)	The goals were to test NTRU's performance on an IoT node, measure energy consumption for cryptographic components, assess NTRU within Contiki-NG, enhance performance with IoT microcontroller hardware, and evaluate its impact on network-level key distribution.	NTRU with Contiki-NG	General (Security enhancement)	NTRU's performance on an IoT node, including encryption, decryption, key encapsulation, and network-level performance, was detailed with presented experimental results and analyses.	More details could have been given about the test environment or scenarios.	Sky Motes utilize MSP430F1611 microcontrollers with 48-KB of flash memory and 10-KB of RAM to run their software.	KEM-NH-HW was improved by 11.06% in terms of code size optimization and 8.27% in terms of speed optimization compared to KEM on average.
(Zhao et al., 2022)	A domain-specific architecture (DSA) for constructing PQC protocols for Module-LWE-based LBC aimed at high-performance security services on 5G edge computing systems. The TSMC 28 nm version surpassed earlier crypto-processors, with significant cycle count advantages for both Kyber and Dilithium.	Module-LWE, Matrix-Based NTT, PQC, Dilithium	General (Performance improvement)	A detailed experimental study was conducted, and Module LWE-based schemes were implemented and compared. Analyses were provided for high performance.	General security analysis was not provided, and security against side-channel attacks was not tested.	Rocket core, RISC-V core, RV64IMC, Chisel language, Synopsys Design Compiler 2017.12-SP4, FPGA, Arithmetic/NTT Core on Xilinx Artix-7 AC701 Platform with Xilinx Vivado 2018.3	The findings reveal that the NTT Core beats existing implementations in NTT and polynomial multiplication by at least 2.16 and 2 cycles, respectively. The design is better than from state-of-the-art crypto-processor equivalents in terms of both speed and energy efficiency.

TABLE 5 (Continued)

Paper	Contribution	Used techniques	Focused area	Strength	Weakness	Test environment	Performance metrics
(Xu et al., 2023)	Based on ideal lattice structures, an effective identity-based public-key data validation communication technique that simplified key management and lowered was devised. The technique was shown to provide semantic security against quantum-enabled attackers.	Ideal lattice and sampling algorithm, ring-LWE problem, and hardness assumption	General (Performance improvement)	Algorithms for the proposed method were shared, detailed experimental results were presented, and accuracy, security, and complexity analysis was conducted.	Security analysis only mathematical proofs were provided, and was not demonstrated in the simulator.	Implemented in MATLAB on a MacOS system with an Intel Core i9 2.4GHz processor and 64GB of RAM.	Taking 19.4 and 18.9 ms to encrypt and filter one keyword when $n = 256$. Compared to prior work, the key derivation technique was roughly 123–238 faster, and the storage cost of the secret key was lowered from 547 to 1.7 MB.
(Lee et al., 2023)	Designed specialized pipelined architectures for NTT and INTT in homomorphic encryption (HE) systems. Created efficient hardware accelerators (ENC-DEC) for CKKS-based HE schemes, accommodating various parameter sets and polynomial sizes	Barrett-based MM algorithm, pipelined NTT architecture	General (fog/edge/cloud computing performance improvement)	Larger throughput and greater hardware efficiency, less encryption and decryption time	Design consumes more DSP slices	Xilinx VivadoTM (v2020.2) tool and Xilinx Alveo UltraScale+ XCU250 FPGA platform	The throughput rate per equivalent slice, latency (μs)
(Shahidinejad & Abawajy, 2023)	Blockchain and lattices join forces to safeguard IoT device communications, easing their workload and offering robust	Blockchain, lattice-based cryptography	General (Performance improvement)	The method's details, algorithms, implementation, analysis, performance evaluation, and comparisons with	Resistance to attacks has not been evaluated in detail.	ESP32-DevKitC as the IoT device, and an HP Proliant DL380 G9 Server with 10 CPU cores and 16 GB of	Reduced the device-side computation by 58% and the communication overhead by 2%

(Continues)

TABLE 5 (Continued)

Paper	Contribution	Used techniques	Focused area	Strength	Weakness	Test environment	Performance metrics
	security features. Rigorously tested, this approach was proven superior to classical, blockchain-based, and even post-quantum methods in real-world trials.			similar methods have been presented.		RAM, running on a virtual Ubuntu machine for the blockchain, were used.	
(Zhu et al., 2023)	Created QKD-DCNs with cloud-edge collaboration for 4C services. Introduced QKD-generated cryptographic resources. Defined the 4CRA problem and proposed a resource-efficient algorithm, CryptoD-4CRA. Compared to latency-focused algorithms, CryptoD-4CRA demonstrated better performance in key consumption and service success ratio	Dense wavelength division multiplexing (DWDM), network is based on IP offloading, transponders with fixed bit rates, Secret keys are generated using QKD and stored in the QKP (quantum key pool), formulate an ILP (integer linear programming) model	General (Performance improvement)	Algorithm reduces the key resource consumption ratio and average key resource consumption	Large-scale topology drops the effectiveness of proposed algorithms in terms of SR(the ratio of the number of successful services over the total arrived services), WU(wavelength utilization), and AL(average latency)	ILP formulations are programmed based on the IBM CPLEX 12.6 software, and the heuristic algorithms are implemented based on Java. The simulation is run on a PC with Intel Core i7-10510U CPU 1.80 GHz 2.30 GHz and 16-GB memory.	It significantly reduced key resource consumption and evaluated the performance of 4CRA algorithms in terms of SR, AL, and WU.
(Corrias et al., 2023)	A QKD-based method was implemented for secure communication between the center and a remote edge structure. This made it possible to use hardware encryptors that provide real-time encryption.	QKD	General (Security enhancement)	The method's details, algorithms, implementation, analysis, have been presented.	A detailed security analysis, performance evaluation, and comparisons with similar methods have not been provided.	SENTRON PAC4200 power monitor, SIMATIC Industrial Edge (SIE) IPC227E, Quell-X QKD, and layer-3 Encryptor system (HypnosX) were used.	An average key exchange speed of 1.3 kbit/s, average quantum bit error rate of 1.5% over 10.8 dB of channel loss

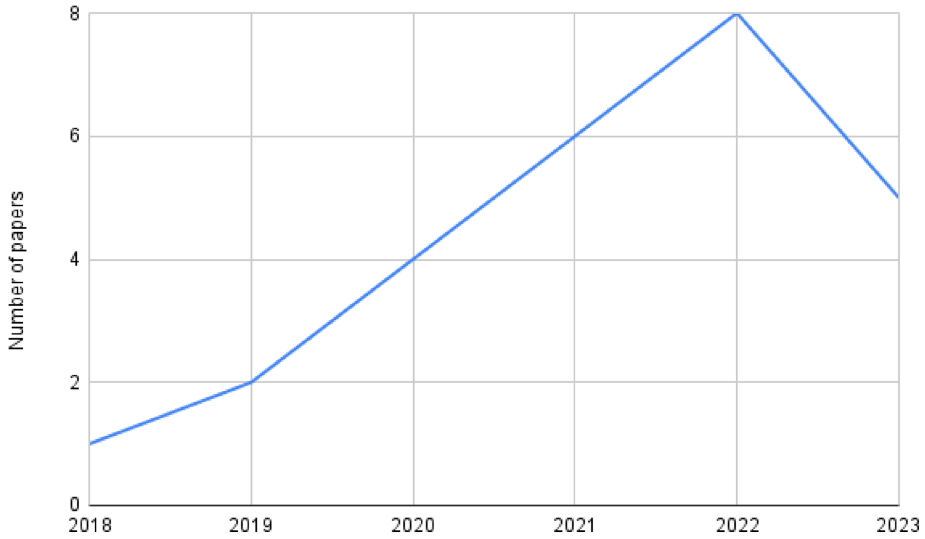

FIGURE 8 The distribution of reviewed papers by years (until the end of December 2023).

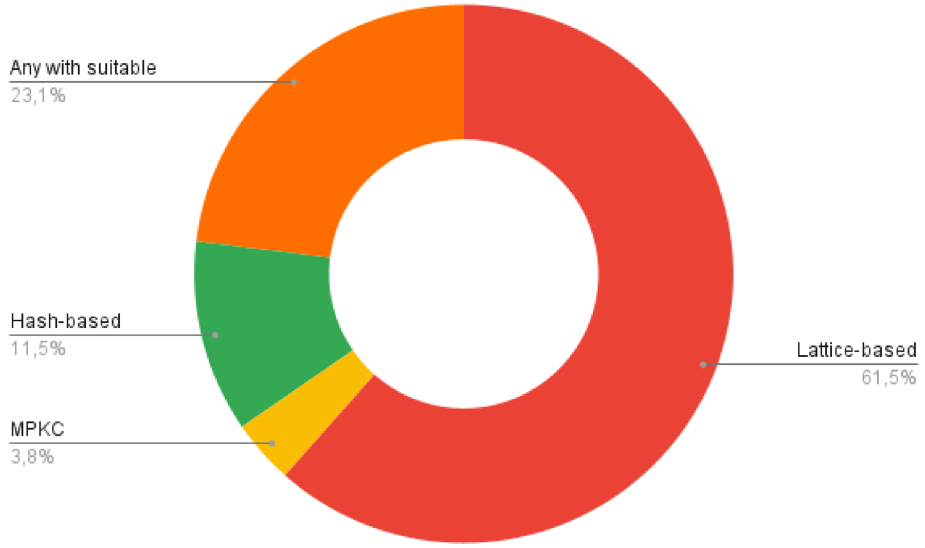

FIGURE 9 The distribution of reviewed papers by PQC types.

and resistance to MitM attacks. However, in some cases, edge systems may need to transmit processed data to the cloud for persistent storage. In such cases, data on edge devices needs to be encrypted. The resource constraints necessitate that these operations be performed in a lightweight manner.

Quantum computing is significantly faster than classical computing, rendering today's PKC systems vulnerable to quantum attacks. Therefore, under the umbrella of PQC, various approaches like lattice-based, code-based, hash-based, and multivariate-based cryptography are being developed. This article focuses on quantum-resistant structures for edge computing security. The limited number of studies and their relatively recent emergence indicates the nascent state of this research area. In these studies, lattice-based encryption systems are often used to make edge systems quantum-resistant. LBC is considered more established compared to other post-quantum approaches. There are also approaches developed using code-based and hash-based techniques. Hash-based systems are typically used for signature purposes. Multivariate-based systems are relatively new but hold promise as an NP-hard problem (Dey & Dutta, 2023). For this reason, we found only one study on edge computing security using these methods. The distribution of reviewed papers by years is illustrated in the graph in Figure 8. According to this, it can be observed that the trend in this field has increased in recent years.

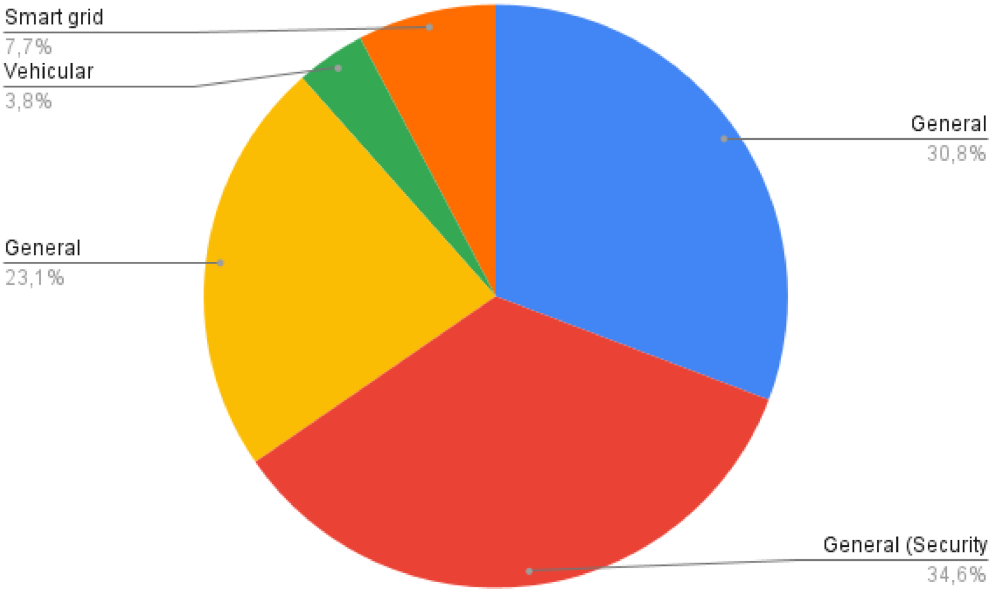

FIGURE 10 The distribution of reviewed papers by focused area.

The intensity of research on post-quantum-based methods for the security of edge systems, with the majority of it conducted in the last 4 years, demonstrates the relevance of this research area. While quantum computer systems may not be widely used yet, the existence of quantum computers in the proposed systems should not be ignored. When evaluating PQC types within quantum-based encryption or signature approaches, the types with fewer studies are relatively more recent developments compared to others. Furthermore, since this article focuses on the security of IoT and edge systems, methods are designed with the presence of resource-constrained devices in mind. This situation often directs security improvement efforts toward the development of lightweight protocols. The distribution of reviewed papers by PQC types is shown in Figure 9. Values are obtained from 26 articles examined in detail.

Edge computing structures are generally used in IoT systems. There are many areas where IoT systems, such as smart cities, healthcare, vehicle communication, and smart grids, are frequently used. The graph depicting which area of IoT-based applications the reviewed articles are focused on can be found in Figure 10.

The development of methods based on quantum-resistant and lightweight structures is crucial for the security of IoT applications. Here are some potential research directions that could be pursued in the future:

- *Adaptation of quantum-resistant symmetric encryption systems*: There are lightweight approaches available for resource-constrained systems using quantum-resistant existing symmetric encryption systems. Similarly, adaptations can be made for different domains where needed.
- *Security for industry 4.0 and IoT communication*: Industry 4.0 describes changes in traditional production systems, especially IT-oriented (Lasi et al., 2014). Industry 4.0, characterized by the fusion of technologies like IoT, AI, and big data, marks the transformative fourth industrial revolution. Driven by cyber-physical systems and interconnectivity, it promises to revolutionize production with enhanced efficiency, flexibility, and customization. Automation, powered by machine learning and AI, optimizes processes and facilitates real-time decision-making, paving the way for a dynamic and responsive industrial landscape. Industry 4.0 connects and empowers smart devices to autonomously manage tasks like production, logistics, and self-maintenance. In Industry 4.0, there is a need for security approaches in machine-to-machine communication and autonomous vehicles (Karakaya & Arat, 2021). Security schemes or models based on PQC can be developed to prepare these systems for the quantum era.
- *New techniques to counter emerging threats*: Evaluate existing attack methods and those based on post-quantum approaches to devise new techniques for protecting systems against these threats. Staying ahead of potential attackers is crucial in the evolving landscape of cybersecurity (Arat & Akleylek, 2023a).
- *AI-enhanced anomaly detection*: Leverage artificial intelligence to enhance anomaly detection techniques for edge computing systems. Develop intrusion detection systems (IDS) and intrusion prevention systems (IPS) with AI and Decision Support Systems to proactively identify and mitigate attacks on edge systems (Sahmutoglu et al., 2023).

TABLE 6 Acronyms and meanings.

Acronym	Meaning
4C	Communication, computation, caching, and cryptographic
4CRA	4C resource-allocation
4CRA	4th generation of centralized radio access
AES	Advanced encryption standard
AI	Artificial intelligence
AKA	Authentication and key agreement
AL	Average latency
ARMv8	Advanced RISC machine (version 8)
ASIC	Applications specific integrated circuit
BLISS	Bimodal lattice signature scheme
CCNS	Context-aware considered node selection
CIA	Confidentiality–integrity–availability
CKKS	Cheon–Kim–Kim–Song
CMOS	Complementary metal oxide semiconductor
CPLEX	IBM ILOG CPLEX optimization studio
CPU	Central processing unit
CQPC	Continuous-time quantum walk path calculation
DAA	Direct anonymous attestation
DoS	Denial of service
DSA	Domain-specific architecture
DSM	Diffie supersingular multiplication
DSM	Diffie supersingular multiplication
DSP	Digital signal processing
DWDM	Dense wavelength division multiplexing
ECC	Elliptic curve cryptography
ENC-DEC	Encryption–decryption
ESP	Espressif system's platform
EUF-CMA	Existential unforgeable under adaptive chosen message attack
FEC-IoT	Fog/edge computing IoT
FFT	Fast Fourier transformation
FPGA	Field programmable gate array
GPU	Graphics processing unit
HDL	Hardware descriptive language
HLS	High-level synthesis
HMAC	Hash-based message authentication code
ILP	Integer linear programming
IoT	Internet of things
IPC	Industrial personal computer
IPS	Intrusion prevention system
ISE	Integrated synthesis environment
Kb, KB, GB, kbit/s	Kilobit, kilobyte, gigabyte, kilobit per second
KEM-NH-HW	Key encapsulation mechanism-noninteractive-hardware oriented
LAC	Low-density parity-check

(Continues)

TABLE 6 (Continued)

Acronym	Meaning
LBC	Lattice-based cryptography
LPN	Learning parity with noise
MAC	Message authentication code
MCU	Micro controller unit
MEC	Multi-access edge computing
MHz, GHz	Megahertz, gigahertz
MICAz	Multi-access, intelligent, convergent, and autonomous network
MitM	Man-in-the-middle
MPKC	Multivariate public key cryptography
MQ	Multivariate quadratic
NIST	National institute of standards and technology
NPCR	Number of the pixel change rate
NTRU	*N*-th degree truncated polynomial ring
NTT	Number theoretic transform
OTS	One-time-signature
PAC	Power automation controller
PBC	Pairing-based cryptography
PKC	Public key encryption
PQC	Post-quantum cryptography
PRNG	Pseudo random number generator
PTPX	Precision time protocol over ethernet extensions
QKD-DCN	Datacenter network secured through quantum key distribution
QW	Quantum walks
RAM	Random access memory
RISC-V	Reduced instruction set computer fifth generation
RLWE	Ring learning with error
RM	Research methodology
RRC	Radio resource control
RSA	Rivest Shamir Adleman
RSUs	Roadside units
RV64IMC	RISC-V 64-bit integer, compressed instructions, multiply-accumulate, single-precision floating-point
SCR1	Syntacore core RISC-V (version 1)
SDBM	Simple database manager
SHA	Secure hash algorithm
SIE	SIMATIC industrial edge
SMHM	Signature-based Merkle Hash multiplication
SP4	Secure platform 4
SPMA	Schoolbook polynomial multiplication method
SR	Success rate
TPM	Trusted platform module
TSMC	Taiwan semiconductor manufacturing company
VANET	Vehicular ad hoc network
VHDL	Very high speed integrated circuit hardware description language

TABLE 6 (Continued)

Acronym	Meaning
VPQC	Vector processor for post-quantum cryptography
WBAN	Wireless body area networks
WSN	Wireless sensor networks
WU	Wavelength utilization
XMSS	Extended Merkle signature scheme

- *Parameters optimization*: Ways to optimize the transmission of data among edge systems for minimal latency can be explored.

These research directions aim to address the pressing need for secure IoT systems, especially in the context of edge computing, while considering the challenges posed by quantum computing advancements.

7 | CHALLENGES IN THIS AREA

This section discusses the challenges and issues related to post-quantum edge systems. Edge computing is a concept often used in IoT applications, bringing cloud capabilities closer to the endpoints of data processing and storage. It offers advantages such as low latency, mobility, and enhanced security. However, alongside these benefits, there are also disadvantages and challenges to consider.

Connecting numerous low-power IoT devices can pose challenges related to access control and authentication (Zeyu et al., 2020). High mobility in such systems can also introduce general security difficulties. Ensuring privacy protection, reducing the risk of attacks, and implementing security measures like anomaly detection are crucial. However, these tasks are complicated by the resource constraints of IoT devices, which often lack the computational power required for these operations. This is why lightweight methods are being developed.

Edge devices are vulnerable to risks like node theft or physical manipulation since they are located in close proximity to applications. Therefore, ensuring the physical security of edge systems can be considered one of the challenges. Additionally, securing the data collection process, sharing protocols, and storage management systems for the increasing volume of data is also crucial (Kwon et al., 2023).

The development of quantum computers poses a serious security risk due to the increase in computational speed, which threatens the security of existing encryption systems. IoT and other applications that use cloud, fog, and edge computing structures need to be made quantum-resistant. The biggest challenge in these systems is the development of highly secure and lightweight mechanisms. Research in this area is growing, and promising developments are being made.

The meanings of the acronyms that we use in our paper are located in Table 6.

8 | CONCLUSION

This article examines quantum-resistant approaches, schemes, and infrastructure for IoT and other systems using edge computing. To the best of our knowledge, this study constitutes the initial comprehensive review focused solely on post-quantum security within the domain of edge computing. As a preliminary overview, it covers general security methods, the differences and security needs between cloud, fog, and edge computing, as well as the types and details of post-quantum systems. While no historical filtering was applied in the research methodology, it is observed that the two oldest studies date back to 2018, with the majority being from 2022 and 2023. This suggests that the research area is current and that an insufficient number of studies have been conducted so far. To make edge systems quantum-resistant, more lattice-based models are being established. There are fewer instances of code-based and hash-based methods. During our research, we found only one study on multivariate models. However, the developments in this field show promise. The crucial point to consider is that every security measure adds an additional load to the system,

and since edge systems are generally resource-constrained, there is a need for lightweight models. We believe that in the future, there will be an increasing focus on research in this direction.

AUTHOR CONTRIBUTIONS

Aykut Karakaya: Investigation (equal); methodology (equal); writing – review and editing (equal). **Ahmet Ulu:** Investigation (equal); methodology (equal); writing – review and editing (equal).

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their suggestions to improve the quality of this article.

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no conflict of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Aykut Karakaya https://orcid.org/0000-0001-6970-3239
Ahmet Ulu https://orcid.org/0000-0002-4618-5712

RELATED WIREs ARTICLE

Internet of Things and data mining: From applications to techniques and systems

REFERENCES

Ajtai, M., & Dwork, C. (1997). Public-key cryptosystem with worst-case/average-case equivalence. In: Proceedings of the Annual ACM Symposium on Theory of Computing, pp. 284–293. https://doi.org/10.1145/258533.258604

Akleylek, S., Soysaldı, M., Lee, W.-K., Hwang, S. O., & Wong, D. C.-K. (2021). Novel postquantum MQ-based signature scheme for internet of things with parallel implementation. *IEEE Internet of Things Journal*, *8*(8), 6983–6994. https://doi.org/10.1109/JIOT.2020.3038388

Arat, F., & Akleylek, S. (2023a). A new method for vulnerability and risk assessment of IoT. *Computer Networks*, *237*, 110046. https://doi.org/10.1016/j.comnet.2023.110046

Arat, F., & Akleylek, S. (2023b). Attack path detection for IIoT enabled cyber physical systems: Revisited. *Computers & Security*, *128*, 103174. https://doi.org/10.1016/j.cose.2023.103174

Asif, R. (2021). Post-quantum cryptosystems for internet-of-things: A survey on lattice-based algorithms. *Internet of Things*, *2*(1), 71–91. https://doi.org/10.3390/iot2010005

Bader, A., Ghazzai, H., Kadri, A., & Alouini, M. S. (2016). Front-end intelligence for large-scale application-oriented internet-of-things. *IEEE Access*, *4*, 3257–3272. https://doi.org/10.1109/ACCESS.2016.2580623

Balasubramanian, K. (2018). Recent developments in cryptography: A survey. In K. Balasubramanian & M. Rajakani (Eds.), *Algorithmic strategies for solving complex problems in cryptography* (pp. 1–22). IGI Global. https://doi.org/10.4018/978-1-5225-2915-6.ch001

Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), *Post-quantum cryptography* (pp. 1–14). Springer. https://doi.org/10.1007/978-3-540-88702-7_1

Bhattacharyya, S., & Chakrabarti, A. (2022). Data management, analytics and innovation. In N. Sharma, A. Chakrabarti, V. E. Balas, & A. M. Bruckstein (Eds.), *Post-quantum cryptography* (pp. 375–405). Springer Singapore.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In *Proceedings of the 1st ACM Mobile Cloud Computing Workshop* (MCC'12), pp. 13–15. https://doi.org/10.1145/2342509.2342513

Butin, D. (2017). Hash-based signatures: State of play. *IEEE Security and Privacy*, *15*(4), 37–43. https://doi.org/10.1109/MSP.2017.3151334

Chen, L., Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R. A., & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (Vol. 12). US Department of Commerce, National Institute of Standards and Technology.

Chowdhury, M. M., Rifat, N., Ahsan, M., Latif, S., Gomes, R., & Rahman, M. S. (2023). ChatGPT: A threat against the CIA triad of cyber security. In: *Proceedings of the 2023 IEEE International Conference on Electro Information Technology* (EIT), pp. 1–6. https://doi.org/10.1109/eIT57321.2023.10187355

Corrias, N., Vagniluca, I., Francesconi, S., de Lazzari, C., Biagi, N., Menchetti, M., Lombardi, G., Scordato, A., Gionco, V., Mercinelli, R., Pagano, A., Valvo, M., Tovar, O., Giacalone, G., Brizzi, P., Occhipinti, T., Zavatta, A., & Bacco, D. (2023). Implementation of Italian industry 4.0 quantum testbed in Turin. *IET Quantum Communication*, 1–6. https://doi.org/10.1049/qtc2.12074

Dey, J., & Dutta, R. (2023). Progress in multivariate cryptography: Systematic review, challenges, and research directions. *ACM Computing Surveys*, *55*(12), 1–34. https://doi.org/10.1145/3571071

Dharminder, D., Kumari, S., & Kumar, U. (2021). Post quantum secure conditional privacy preserving authentication for edge based vehicular communication. *Transactions on Emerging Telecommunications Technologies*, *32*(11), 1–15. https://doi.org/10.1002/ett.4346

Ebrahimi, S., Bayat-Sarmadi, S., & Mosanaei-Boorani, H. (2019). Post-quantum Cryptoprocessors optimized for edge and resource-constrained devices in IoT. *IEEE Internet of Things Journal*, *6*(3), 5500–5507. https://doi.org/10.1109/JIOT.2019.2903082

el Kassem, N., Chen, L., el Bansarkhani, R., el Kaafarani, A., Camenisch, J., Hough, P., Martins, P., & Sousa, L. (2019). More efficient, provably-secure direct anonymous attestation from lattices. *Future Generation Computer Systems*, *99*, 425–458. https://doi.org/10.1016/j.future.2019.04.036

El-Latif, A. A. A., Abd-El-Atty, B., Hossain, M. S., Elmougy, S., & Ghoneim, A. (2018). Secure quantum steganography protocol for fog cloud internet of things. *IEEE Access*, *6*, 10332–10340. https://doi.org/10.1109/ACCESS.2018.2799879

El-Latif, A. A. A., Abd-El-Atty, B., Venegas-Andraca, S. E., Elwahsh, H., Piran, M. J., Bashir, A. K., Song, O.-Y., & Mazurczyk, W. (2020). Providing end-to-end security using quantum walks in IoT networks. *IEEE Access*, *8*, 92687–92696. https://doi.org/10.1109/ACCESS.2020.2992820

Feldmann, A. (2005). A Survey of Attacks on Multivariate Cryptosystems [UWSpace]. http://hdl.handle.net/10012/1032

Karacan, E., Akleylek, S., & Karakaya, A. (2021). PQ-FLAT: A new quantum-resistant and lightweight authentication approach for M2M devices. In *Proceedings of the 2021 9th International Symposium on Digital Forensics and Security* (*ISDFS*), pp. 1–5. https://doi.org/10.1109/ISDFS52919.2021.9486341

Karacan, E., Karakaya, A., & Akleylek, S. (2022). Quantum secure communication between service provider and Sim. *IEEE Access*, *10*, 69135–69146. https://doi.org/10.1109/ACCESS.2022.3186306

Karakaya, A., & Akleylek, S. (2018). A survey on security threats and authentication approaches in wireless sensor networks. In *Proceedings of the 2018 6th International Symposium on Digital Forensic and Security* (*ISDFS*), pp. 1–4. https://doi.org/10.1109/ISDFS.2018.8355381

Karakaya, A., & Akleylek, S. (2022). A fusion of artificial intelligence and internet of things for emerging cyber systems. In P. Kumar, A. J. Obaid, K. Cengiz, A. Khanna, & V. E. Balas (Eds.), *A review of resource allocation and management methods in IoT* (pp. 409–429). Springer International Publishing. https://doi.org/10.1007/978-3-030-76653-5_22

Karakaya, A., & Arat, F. (2021). A survey on security requirements, threats and protocols in industrial internet of things. *International Journal of Information Security Science*, *10*(4), 138–152.

Karakaya, A., & Ulu, A. (2023). A review on latest developments in post-quantum based secure Blockchain systems. In *Proceedings of the 2023 11th International Symposium on Digital Forensics and Security* (*ISDFS*), pp. 1–6. https://doi.org/10.1109/ISDFS58141.2023.10131840

Karakaya, A., Ulu, A., & Akleylek, S. (2022). GOALALERT: A novel real-time technical team alert approach using machine learning on an IoT-based system in sports. *Microprocessors and Microsystems*, *93*, 104606. https://doi.org/10.1016/j.micpro.2022.104606

Kim, Y., Song, J., & Seo, S. C. (2022). Accelerating falcon on ARMv8. *IEEE Access*, *10*, 44446–44460. https://doi.org/10.1109/ACCESS.2022.3169784

Kim, Y., Song, J., Youn, T. Y., & Seo, S. C. (2022). Crystals-Dilithium on ARMv8. *Security and Communication Networks*, *2022*, 1–12. https://doi.org/10.1155/2022/5226390

Kumari, S., Singh, M., Singh, R., & Tewari, H. (2022a). Signature based Merkle hash multiplication algorithm to secure the communication in IoT devices. *Knowledge-Based Systems*, *253*, 109543. https://doi.org/10.1016/j.knosys.2022.109543

Kumari, S., Singh, M., Singh, R., & Tewari, H. (2022b). To secure the communication in powerful internet of things using innovative post-quantum cryptographic method. *Arabian Journal for Science and Engineering*, *47*(2), 2419–2434. https://doi.org/10.1007/s13369-021-06166-6

Kwon, H. J., Salim, M. M., & Park, J. H. (2023). Recent trends on Smart City security: A comprehensive overview. *Journal of Information Processing Systems*, *19*(1), 118–129. https://doi.org/10.3745/JIPS.03.0182

Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, *6*(4), 239–242. https://doi.org/10.1007/s12599-014-0334-4

Lee, J., Duong, P. N., & Lee, H. (2023). Configurable encryption and decryption architectures for CKKS-based homomorphic encryption. *Sensors*, *23*(17), 7389. https://doi.org/10.3390/s23177389

Li, K., Shi, R., Wu, M., Li, Y., & Zhang, X. (2022). A novel privacy-preserving multi-level aggregate signcryption and query scheme for smart grid via mobile fog computing. *Journal of Information Security and Applications*, *67*, 103214. https://doi.org/10.1016/j.jisa.2022.103214

Lizardo, A., Barbosa, R., Neves, S., Correia, J., & Araujo, F. (2021). End-to-end secure group communication for the internet of things. *Journal of Information Security and Applications*, *58*, 102772. https://doi.org/10.1016/j.jisa.2021.102772

Lu, S., & Li, X. (2021). Quantum-resistant lightweight authentication and key agreement protocol for fog-based microgrids. *IEEE Access*, *9*, 27588–27600. https://doi.org/10.1109/ACCESS.2021.3058180

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications*, *9*(3), 405–414. https://doi.org/10.14569/IJACSA.2018.090354

Mohsen, A. W., Bahaa-Eldin, A. M., & Sobh, M. A. (2017). Lattice-based cryptography. In *Proceedings of the 2017 12th International Conference on Computer Engineering and Systems* (*ICCES*), pp. 462–467. https://doi.org/10.1109/ICCES.2017.8275352

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and privacy in fog computing: Challenges. *IEEE Access*, *5*, 19293–19304. https://doi.org/10.1109/ACCESS.2017.2749422

Nakkar, M., Altawy, R., & Youssef, A. (2020). Lightweight broadcast authentication protocol for edge-based applications. *IEEE Internet of Things Journal*, *7*(12), 11766–11777. https://doi.org/10.1109/JIOT.2020.3002221

Nweke, L. O. (2017). Using the CIA and AAA models to explain cybersecurity activities. *PM World Journal*, *VI*(Xii), 1–3. https://pmworldlibrary.net/wp-content/uploads/2017/05/171126-Nweke-Using-CIA-and-AAA-Models-to-explain-Cybersecurity.pdf

Overbeck, R., & Sendrier, N. (2009). *Code-based cryptography*. In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), *Post-quantum cryptography* (pp. 95–145). Springer. https://doi.org/10.1007/978-3-540-88702-7_4

Ranaweera, P., Jurcut, A. D., & Liyanage, M. (2021). Survey on multi-access edge computing security and privacy. *IEEE Communication Surveys and Tutorials*, *23*(2), 1078–1124. https://doi.org/10.1109/COMST.2021.3062546

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, *78*, 680–698. https://doi.org/10.1016/j.future.2016.11.009

Sahmutoglu, I., Taskin, A., & Ayyildiz, E. (2023). Assembly area risk assessment methodology for post-flood evacuation by integrated neutrosophic AHP-CODAS. *Natural Hazards*, *116*(1), 1071–1103. https://doi.org/10.1007/s11069-022-05712-1

Sendrier, N. (2017). Code-based cryptography: State of the art and perspectives. *IEEE Security and Privacy*, *15*(4), 44–50. https://doi.org/10.1109/MSP.2017.3151345

Señor, J., Portilla, J., & Mujica, G. (2022). Analysis of the NTRU post-quantum cryptographic scheme in constrained IoT edge devices. *IEEE Internet of Things Journal*, *9*(19), 18778–18790. https://doi.org/10.1109/JIOT.2022.3162254

Shahbazi, K., & Ko, S.-B. (2021). Area and power efficient post-quantum cryptosystem for IoT resource-constrained devices. *Microprocessors and Microsystems*, *84*, 104280. https://doi.org/10.1016/j.micpro.2021.104280

Shahidinejad, A., & Abawajy, J. (2023). Decentralized lattice-based device-to-device authentication for the edge-enabled IoT. *IEEE Systems Journal*, *17*(4), 6623–6633. https://doi.org/10.1109/JSYST.2023.3319280

Varghese, B., Wang, N., Barbhuiya, S., Kilpatrick, P., & Nikolopoulos, D. S. (2016). Challenges and opportunities in edge computing. In *Proceedings of the 2016 IEEE International Conference on Smart Cloud* (*SmartCloud*), pp. 20–26. https://doi.org/10.1109/SmartCloud.2016.18

Wang, J., Wang, F., Shi, S., & Yang, W. (2020). Lattice-based incremental signature scheme for the authenticated data update in fog computing. *IEEE Access*, *8*, 89595–89602. https://doi.org/10.1109/ACCESS.2020.2994007

Wang, P., Chen, B., Xiang, T., & Wang, Z. (2022). Lattice-based public key searchable encryption with fine-grained access control for edge computing. *Future Generation Computer Systems*, *127*, 373–383. https://doi.org/10.1016/j.future.2021.09.012

Wang, S., Zhao, Y., Xu, J., Yuan, J., & Hsu, C.-H. (2019). Edge server placement in mobile edge computing. *Journal of Parallel and Distributed Computing*, *127*, 160–168. https://doi.org/10.1016/j.jpdc.2018.06.008

Wong, Z.-Y., Wong, D. C.-K., Lee, W.-K., & Mok, K.-M. (2021). High-speed RLWE-oriented polynomial multiplier utilizing Karatsuba algorithm. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *68*(6), 2157–2161. https://doi.org/10.1109/TCSII.2020.3049002

Xin, G., Han, J., Yin, T., Zhou, Y., Yang, J., Cheng, X., & Zeng, X. (2020). VPQC: A domain-specific vector processor for post-quantum cryptography based on RISC-V architecture. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *67*(8), 2672–2684. https://doi.org/10.1109/TCSI.2020.2983185

Xu, L., Yuan, X., Zhou, Z., Wang, C., & Xu, C. (2023). Towards efficient cryptographic data validation Service in Edge Computing. *IEEE Transactions on Services Computing*, *16*(1), 656–669. https://doi.org/10.1109/TSC.2021.3111208

Zeyu, H., Geming, X., Zhaohang, W., & Sen, Y. (2020). Survey on edge computing security. *2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, 96–105. https://doi.org/10.1109/ICBAIE49996.2020.00027

Zhao, Y., Xie, R., Xin, G., & Han, J. (2022). A high-performance domain-specific processor with matrix extension of RISC-V for module-LWE applications. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *69*(7), 2871–2884. https://doi.org/10.1109/TCSI.2022.3162593

Zhu, Q., Yu, X., Zhao, Y., Nag, A., & Zhang, J. (2023). Resource allocation in quantum-key-distribution-secured datacenter networks with cloud–edge collaboration. *IEEE Internet of Things Journal*, *10*(12), 10916–10932. https://doi.org/10.1109/JIOT.2023.3242725

How to cite this article: Karakaya, A., & Ulu, A. (2024). A survey on post-quantum based approaches for edge computing security. *WIREs Computational Statistics*, *16*(1), e1644. https://doi.org/10.1002/wics.1644