Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 10, pp. 3777–3788
DOI : 10.47974/JIOS-2502

Post-quantum cryptographic policy frameworks for medical institutions

M. M. Thorat [§]
Department of Anatomy
Krishna Institute of Medical Sciences
Krishna Vishwa Vidyapeeth (Deemed to be University)
Karad 415539
Maharashtra
India

Mukesh Parashar [†]
School of Business Management
Noida International University
Greater Noida 201312
Uttar Pradesh
India

Mourya Murlidher *
Department of Computer Science and Engineering
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

V. B. Gawai [‡]
Department of Electronics & Telecommunication Engineering
AISSMS College of Engineering
Pune 411001
Maharashtra
India

[§] *E-mail:* mmthorat31@gmail.com
[†] *E-mail:* registrar@niu.edu.in
* *E-mail:* murli_cool9@vardhaman.org (Corresponding Author)
[‡] *E-mail:* vbgawai@aissmscoe.com

© Taru Publications

Pradnya Yuvraj Patil [@]
Department of Electronics and Telecommunication Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

J. Jayannan [#]
Department of General Medicine
Meenakshi Medical College Hospital and Research Institute
Meenakshi Academy of Higher Education and Research
Kanchipuram 631552
Tamil Nadu
India

Abstract

With the progress of quantum computing, medical institutions that use classical public-key cryptography to secure the confidentiality of long-lasting and delicate healthcare information are facing great security challenges. This research aims to suggest a policy framework for Post-Quantum Cryptographic Policy (PQCP) to facilitate systematic shift of healthcare infrastructures to quantum resistant infrastructure security. It seamlessly combines cryptographic asset discovery, quantum-risk assessment, asset prioritization, crypto-agility, hybrid cryptographic migration, secure key management, governance, compliance monitoring, and ongoing security evaluation. It covers electronic health records, healthcare platforms in the cloud, medical imaging, telemedicine applications and resource-limited Internet of Medical Things devices. A risk-oriented migration strategy gives institutions the ability to prioritize systems based on the amount of data in a system, the vulnerabilities of the cryptographic functions used, the clinical criticality of the system, and the length of time the information must be kept confidential. There are hybrid (classical and post-quantum) mechanisms for gradual migration and interoperability or clinical continuity. Finally, the suggested framework offers a structured approach to enhance the preparedness of healthcare institutions, adherence to regulations, resilience against cryptographic attacks, and long-term protection of healthcare information from the evolving quantum cybersecurity landscape.

Subject Classification: *68M25.*

Keywords: *Post-quantum cryptography, Healthcare cybersecurity, Medical institutions, Quantum security, Crypto-agility, Hybrid cryptography, Quantum risk assessment, Healthcare data protection.*

[@] *E-mail:* **pradnya.patil1@vit.edu**
[#] *E-mail:* **jayannan@maher.ac.in**

1. Introduction

The healthcare sector has undergone a dramatic digital transformation that has led to more reliance on electronic health records (EHRs), cloud computing, telemedicine, artificial intelligence, devices connected to the Internet of Medical Things (IoMT), and clinical information systems (CIS) that are interconnected [1]. The technologies enhance the accessibility of healthcare, diagnostics, operational efficiency and patient monitoring, but create and process sensitive medical data [2] at the same time. The preservation of these kinds of information over a long time is crucial as medical records contain personal, clinical, genomic, financial and demographic information that can be kept confidential for a long time [3]. The current healthcare security infrastructures are mainly based on a classical public-key cryptographic mechanism, including RSA and elliptic-curve cryptography (ECC). These mechanisms are a challenge in the development of large scale quantum computers [4].

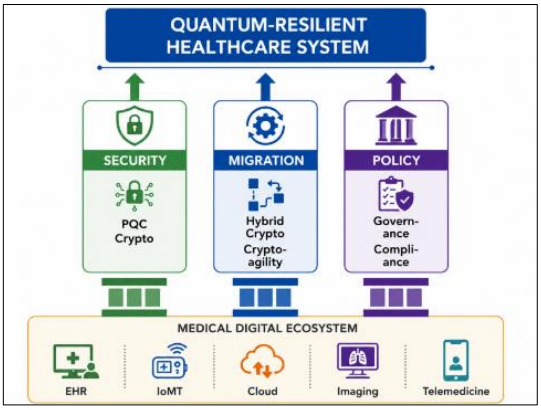

Figure 1

Three-pillar framework for quantum-resilient healthcare security

However, the algorithms by quantum computers could undermine the math behind public-key cryptography, which is used in many common applications, as illustrated in Figure 1. Furthermore, the "harvest-now, decrypt-later" attack makes it possible for attackers to gather healthcare data today that was encrypted and then wait until they are able to gain access to a more powerful quantum computer [5]. As a result, medical institutions need to start taking steps toward cryptographic migration early, in case the need arises for a quantum attack to occur in practice. Post-quantum cryptography (PQC) is cryptographic algorithms that are resistant to attacks from classical and quantum computers. However, introducing PQC in healthcare settings is not the end of the journey of introducing a new algorithm [6]. Medical institutions need to tackle interoperability, legacy health care devices, computational challenges, key administration, regulatory guidelines, vendor reliance, migration expenses, and

working continuity. Hence it is crucial to have a structured institutional policy for the journey towards quantum-safe transformation [7]. In this study, the authors have proposed a Post-Quantum Cryptographic Policy Framework for Medical Institutions which combines the following components: cryptographic asset discovery, quantum-risk assessment, algorithm selection, crypto-agility, hybrid migration, secure key management, compliance monitoring and continuous security evaluation [8]. The framework proposes a system of paths to secure and safeguard long-lived medical information while fostering secure, interoperable and resilient medical information infrastructures in the new post-quantum world.

2. Quantum Threat Landscape and Risk Assessment in Medical Institutions

Medical institutions have to deal with the interconnected environment that includes electronic health records (EHRs), cloud servers, diagnostic systems, IoMT devices, telemedicine platforms, and communication networks. Moving to the quantum era also makes some of the current cryptographic algorithms (such as RSA, ECC, and Diffie–Hellman) vulnerable to quantum attacks, posing a serious threat to security. One that is of particular concern is the "harvest-now, decrypt-later" (HNDL) approach; in which medical information is encrypted today, but decrypted when well-designed quantum computers will be available [9], [10]. A quantitative risk model is thus needed, which will rank the need for post-quantum migration. Suppose that the quantum risk of medical asset (i) is determined as

$$QR_i = P_i \times V_i \times I_i$$

The probability of a quantum enabled compromise (P_i), the cryptographic vulnerability (V_i) and impact of compromise success (I_i). The impact can also include confidentiality, integrity and availability:

$$I_i = w_C C_i + w_I I_i^{\{(g)\}} + w_A A_i$$

where (C_i), $(I_i^{\{(g)\}})$, and (A_i) denote confidentiality, integrity, and availability impacts, while

$$w_C + w_I + w_A = 1.$$

Due to the nature of healthcare records that often need to be maintained over long-term, an added data longevity factor is added. For asset (i)

$$L_i = \frac{\{T_{\{data,i\}}\}}{\{T_Q\}}$$

T_{data,i} is the desired value of the confidentiality period and T_Q is the estimated when quantum capability is needed. Values of 1 (L_i= 1) mean a specific level of exposure to the HNDL attacks. This gives rise to a risk score that is adjusted for the quantum, the resulting quantum adjusted risk score is

$$QARS_i = QR_{i(1+\alpha L_i)}$$

where (α) determines the effect of the sensitivity of long term data. Cryptographic dependency should also be taken into consideration in regard to migration priority. Consider a set of algorithms that depend on quantum technologies, (D_i), and a set of migration complexities, (E_i). Define (D_i) as the set of algorithms where quantum technologies are crucial, and (E_i) as the set of migration complexities. The Post-Quantum Migration Priority Score (PMPS) is in the form of

$$PMPS_i = \frac{\{QARS_i \times D_i\}}{\{1 + \beta E_i\}}$$

where (β) regulates the effect of implementation complexity.

Thus, systems with long lived patient records, genomic data, digital certificates, medical data in the cloud, and critical authentication data are given greater priority to be migrated [11]. The mathematical construct allows medical institutions to shift away from "guesstimates" of risk and to be able to identify cryptographic assets that need to be protected right away, via hybrid or post quantum means. It also provides a quantitative basis for the policy framework recommended and the decisions made for the PQC migration [12].

3. Proposed Post-Quantum Cryptographic Policy Framework

The proposed Post-Quantum Cryptographic Policy Framework (PQCPF) provides a structured mechanism for transitioning medical institutions from quantum-vulnerable cryptographic infrastructures toward secure and crypto-agile environments. The framework integrates five interconnected layers: governance and policy, cryptographic asset assessment, quantum-risk classification, cryptographic migration and implementation, and continuous compliance and monitoring. This layered structure enables hospitals to prioritize critical systems while maintaining interoperability and uninterrupted clinical operations.

A. *Governance and Policy Layer*

The governance layer sets up institutional accountability for the migration to post-quantum. The PQC Governance Committee should be multi-disciplinary and should consist of cybersecurity experts, healthcare IT administrators, clinical engineering, compliance officers and system owners. The score for Governance effectiveness can be stated as

$$G_E = w_{1P_C} + w_{2R_A} + w_{3T_R} + w_{4A_M}$$

P_C being policy completeness, R_A is the responsibility allocation, T_R is personnel training and A_M is audit maturity

$$\sum_{\{i=1\}_i^{\{4\}w}} T_R = 1.$$

B. *Cryptographic Asset Discovery and Classification*

The institution should have a centralised inventory of EHR databases, IoMT devices, medical imaging systems, cloud applications, digital certificates, VPN, API and authentication systems. A criticality score is given to each asset:

$$AC_i = w_{DD_i} + w_{CC_i} + w_{SS_i} + w_{OO_i}$$

The data sensitivity (D_i), clinical criticality (C_i), security dependency (S_i) and operational importance (O_i) of the data. Let's now define the cryptographic exposure of asset (i):

$$CE_i = AC_i \times QV_i,$$

where (QV_i) represents its dependence on quantum-vulnerable cryptography.

C. *Quantum-Risk Classification*

This framework is based on the risk of threats, the longevity of the data and asset exposure to determine how urgent the migration is:

$$QRI_i = CE_i \times P_{\{Q,i\}} \times (1 + \lambda L_i)$$

The quantum-threat probability is denoted as where (P_{Q,i}), the data longevity is denoted as (L_i) and the influence of long-term confidentiality is denoted as (λ).

Assets can subsequently be classified as

$$Risk\ i = \{\ Low, Moderate, High, Critical, QRIi < T1T1 \leq QRIi < T2T2 \leq QRIi < T3QRIi \geq T3\}$$

Critical and high-risk systems should receive priority during migration.

D. *PQC Migration and Algorithm Selection*

The framework calls for hybrid deployment of classical and PQC systems to enable gradual shift to PQC systems, not replacing all classical systems at once. It is checked whether algorithm (j) is suitable or not:

$$AS_j = \alpha S_j + \beta E_j + \gamma I_j + \delta CA_j - \eta O_j$$

Security strength, (S_j), efficiency, (E_j), interoperability, (I_j) and crypto-agility, (CA_j) and implementation overhead, (O_j). The best set up is

$$A^* = x_{\{A_j\}(AS_j)}$$

Subject to a set of pre-defined security and resource constraints. Migration may then continue along the lines of: Migration may then go on like the following:

$$Classical \rightarrow Hybrid\ Classical - PQC \rightarrow PQC - Dominant.$$

E. *Key Management and Access Control*

Secure procedures for generating, distributing, rotating, revoking, backing up and destroying post-quantum keys should be used for the management of post-quantum certificates. Making decisions about access can be summarized by:

$$Access(u,r) = \{1,0, Role(u) \in Permitted(r) otherwise,$$

Ensuring that only authorized healthcare personnel access protected resources.

F. *Continuous Monitoring and Compliance*

The last layer is constantly monitoring the security, regulatory compliance, cryptographic performance and migration status. It is suggested to create a Post-Quantum Readiness Index (PQRI) for.

$$PQRI = \frac{c\left\{w_{1G_E}+w_{2CAI}+w_{3MR}+w_{4CS}+w_{5MS}\right\}}{w_{1G_E}}\{\sum_{\{i=1\}_i^{\{5\}w}} w_{1G_E}]$$

Governance effectiveness (G_E), Crypto-agility (CAI), Migration readiness (MR), Compliance score (CS), Monitoring effectiveness (MS).

4. Framework Architecture and Implementation Methodology

The proposed Post-Quantum Cryptographic Policy Framework consists of several layers that link together assets in healthcare, cryptographic discovery, quantum-risk assessment, policy decision-making, post-quantum security mechanisms, and continuous monitoring. The methodology will allow for step-by-step transition and not hold up critical healthcare functions. Can be deployed on EHR servers, cloud platforms, IoMT (Internet of Medical Things) device, medical imaging systems, telemedicine applications and hospital communication networks.

Step -1: Healthcare Asset and Data Acquisition Layer

The first layer identifies digital assets and their cryptographic dependencies. Let the institutional asset set be

$$\{H\} = \{H_1, H_2, \dots, H_n\}.$$

For each asset (H_i), a feature vector is constructed as

$$X_i = [D_i, C_i, A_i, L_i, R_i, Q_i],$$

where (D_i) represents data sensitivity, (C_i) clinical criticality, (A_i) algorithm dependency, (L_i) data longevity, (R_i) resource availability, and (Q_i) quantum vulnerability.

Step -2: Cryptographic Inventory and Vulnerability Analysis

The cryptographic discovery maps out various institutional systems that utilize RSA, ECC, Diffie–Hellman, certificates, key-exchange protocols, digital signatures and symmetric mechanisms. A Vulnerability Score is determined by the following:

$$CV_i = \sum_{\{j=1\}_{\{ij\}v_j}^{\{m\}d}} dijvj]$$

where d_{ij} is a variable that is 1 if the asset (i) requires the cryptographic mechanism (j) and 0 otherwise and (v_j) is a variable that represents the weight

of the quantum vulnerability of the cryptographic mechanism (j). As assets have higher (CV_i) they should have higher migration consideration.

Step -3: Quantum-Risk Assessment Engine

The structure is composed of the cryptographic weaknesses, the criticality of the assets and the long lasting confidentiality requirements:

$$QRA_i = CV_i \times AC_i \times P_{\{Q,i\}} \times (1 + \lambda L_i).$$

(AC_i) refers to the criticality of an asset, which is a vital asset to the company, and (P_{Q,i}) is the probability of quantum threat for the asset. The score obtained is used to quantitatively determine migration priority.

Step -4: Policy Decision and Migration Engine

According to the Risk calculation, the system automatically suggests an appropriate cryptographic policy:

$$Policy = \{P1, P2, P3, P4, QRAi < T1T1 \leq QRAi < T2T2 \leq QRAi < T3QRAi \geq T3\}.$$

In this context, (P1) signifies continued monitoring, (P2) is for the preparation of crypto-agility, (P3) is for hybrid classical–PQC migration, and (P4) is for priority deployment of quantum-resistant protection.

Step -5: Hybrid Cryptographic Implementation

In transition, both the classical and post-quantum mechanisms are in play. It is possible to derive a hybrid session key as

$$K_H = KDF\big(K_C \parallel K_{\{PQ\}}\big),$$

Here, (K_C) is the classical shared secret, (K_{PQ}) is the post-quantum shared secret and (KDF) is a secure key-derivation function. If the data is protected health data (M),

$$C = Enc_{\{K_H\}(M)},$$

and authorized reconstruction is performed as

$$M = Dec_{\{K_H\}(C)}.$$

The integrity and authenticity of the data are also checked prior to the release of clinical information to users with authorization. The implementation must meet security requirements and not be overly burdensome on the operations. The overall migration cost is:

$$MC_i = \alpha T_i + \beta M_i + \gamma B_i + \delta E_i,$$

Here (T_i), (M_i), (B_i) and (E_i) are time, memory, bandwidth and energy penalties for processing, respectively. Migration is allowed when

$$QRA_i^{\{post\}} < QRA_i^{\{pre\}},$$

while simultaneously satisfying

$$MC_i \leq MC_{\{\backslash max\}}$$

and

$$Compliance_i \geq C_{\{\backslash min\}}.$$

Step -6: Continuous Monitoring and Feedback

After deployment, the framework can constantly analyze the state of the algorithms, the validity of certificates, the rotation of keys, adherence to policies, quantum attack threat, and system performance. Where f is the product of the error, and d is the width of the confidence interval.

$$RQR_i = QRA_{i(1-E_{\{PQC\}})},$$

where (E_{PQC}) is the effectiveness of the post quantum controls that are implemented. This architecture takes the proposed policy framework and turns it into a practical approach that can be used step-by-step as medical institutions work through the process of identifying vulnerabilities, ranking their most important assets, implementing quantum-resistant measures, and regularly reevaluating and updating their security measures as quantum technologies develop and evolve.

5. Regulatory and Ethical Considerations

Implementing post-quantum cryptography in healthcare goes beyond just the technical aspects and involves thoughtful considerations of regulation, ethics, and institutional roles. It is crucial for medical institutions to ensure quantum resistant security and keep patient information secure while maintaining privacy, appropriate access to patient records, clinical availability, and adherence to established healthcare regulations. The biggest regulatory and ethical issues are presented below:

1. **Patient Data Privacy and Confidentiality:** Health information, including patient records, medical images, genomic data, diagnostic reports and information that could identify the patient, should be shielded from security risks in the near future and long-term future with post-quantum security mechanisms.
2. **Regulatory Compliance:** PQC migration needs to be in line with relevant healthcare and data-protection policies and standards, including HIPAA, GDPR, national laws, cybersecurity policies, and institutional privacy laws.
3. **Clinical Accessibility and Continuity:** Efficient and secure protection of cryptographic data must not hinder the legitimate access of medical information. Healthcare professionals must have access to the medical data that has been collected and stored in a timely and secure manner, to include critical clinical situations and during emergencies.
4. **Data Minimization and Purpose Limitation:** Health care providers should only gather, use, share and keep patient information that is required for specific, legitimate and clearly outlined reasons. To protect medical and genomic data from future attacks, it is necessary to improve long-term medical and genomic records.

5. **Governance and Accountability:** Ensure that the roles and responsibilities of institutions around the PQC algorithm selection, key management, certificate replacement, vendor security, incident management and the monitoring of the cryptographic lifecycle are clearly defined.
6. **Ethical and Continuous Oversight:** Privacy, transparency, proportionality, security, accessibility and regulatory compliance should all be subject of regular audits. With continuous oversight, quantum-resistant technologies can enhance healthcare cybersecurity while remaining both patient rights-compliant and ethically sound, and ensuring that patients can still receive the medical care they need.

Achieving a successful post-quantum transition will depend on a combination of the security and security of technology, compliance with regulations, and the ethics of healthcare. Through integrating privacy protection, clinical accessibility, accountability, data minimization, transparent governance, and periodic auditing, medical facilities can build quantum-safe infrastructures for healthcare while safeguarding patient rights and vital medical assistance. Medical institutions can build quantum-safe healthcare infrastructures without infringing patient rights or vital healthcare services by integrating privacy protection, clinical accessibility, accountability, data minimization, transparent governance, and periodic auditing. All these factors will be relevant in the adoption of post-quantum cryptography in the modern healthcare environment, and will be important to consider, as well as trying to keep a balance between these factors.

6. Challenges and Future Directions

There are several challenges that medical institutions face in the shift towards post-quantum cryptography. Legacy healthcare systems, limited resources for IoMT devices, high migration costs, large size of cryptographic keys, interoperability constraints, and relying on third parties could hinder implementation. At the same time, hospitals need to continue to provide uninterrupted clinical services and upgrade their certificates, authentication systems, communication methods and security systems. Another added layer of complexity in migration is the fact that there are still limited technical expertise, and the standards for post-quantum are constantly changing.

The lightweight post-quantum algorithms for medical devices, automated quantum asset discovery, intelligent quantum risk assessment and efficient hybrid security methods are the areas that need to be explored in the future. Architectures should be designed to be crypto-agile, to ensure that quick algorithm changes as standards progress can be accommodated. Real-world hospital deployments, performance optimization, secure cloud integration, and regulatory harmonization are aspects of further studies that are needed. The advancements will contribute to the creation of global scalable, interoperable and sustainable quantum-resistant healthcare ecosystem.

7. Conclusion

The current research suggests a Post-Quantum Cryptographic Policy Framework for Medical Institutions in order to tackle with the security challenges emerging with quantum computing. The framework incorporates crypto-agility, secure key management, governance, regulatory compliance, continuous monitoring, cryptographic asset discovery, quantum-risk evaluation, hybrid migration, and more. It offers a structured way to detect vulnerable health care systems and prioritize critical assets with long-term and sensitive patient data. The proposed layered architecture enables slow deployment of products and services using quantum-resistant security without impacting interoperability and clinical continuity. In a short time, the healthcare sector will be using a wide variety of security protocols to safeguard patient data.Soon, a healthcare organization may find itself using many different types of security protocols to protect patient information, especially with legacy systems and resource-poor medical devices. The framework provides a policy-based approach to improve cybersecurity in the long term healthcare industry and safeguard patient data from future quantum-based threats. It could be enhanced and scaled up in the future through implementation and validation in real-world settings.

References

[1] Y. Baseri, V. Chouhan, and A. Hafid, "Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols," *Comput. Secur.*, vol. 142, Art. no. 103883 (2024), doi: 10.1016/j.cose.2024.103883.

[2] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A survey on security threats and countermeasures in Internet of Medical Things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, Art. no. e4049 (2022), doi: 10.1002/ett.4049.

[3] K. Cherkaoui Dekkaki, I. Tasic, and M.-D. Cano, "Exploring post-quantum cryptography: Review and directions for the transition process," *Technologies*, vol. 12, no. 12, Art. no. 241 (2024), doi: 10.3390/technologies12120241.

[4] M. Uddin, M. Muzammal, M. K. Hameed, I. T. Javed, B. Alamri, and N. Crespi, "CBCIoT: A consensus algorithm for blockchain-based IoT applications," *Appl. Sci.*, vol. 11, no. 22, Art. no. 11011 (2021), doi: 10.3390/app112211011.

[5] N. Ahmed, L. Zhang, and A. Gangopadhyay, "A survey of post-quantum cryptography support in cryptographic libraries," in *Proc.*

IEEE Int. Conf. Quantum Comput. Eng. (QCE), pp. 906–917 (2025), doi: 10.1109/QCE65121.2025.00102.

[6] W. Yang, S. Wang, H. Cui, Z. Tang, and Y. Li, "A review of homomorphic encryption for privacy-preserving biometrics," *Sensors*, vol. 23, no. 7, Art. no. 3566 (2023), doi: 10.3390/s23073566.

[7] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. Dominguez Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243 (2022), doi: 10.1038/s41586-022-04623-2.

[8] S. K. Sahu and K. Mazumdar, "State-of-the-art analysis of quantum cryptography: Applications and future prospects," *Front. Phys.*, vol. 12, Art. no. 1456491 (2024), doi: 10.3389/fphy.2024.1456491.

[9] N. Babbar, A. K. Sharma, R. K. Saini, and N. K. Verma, "Mathematical foundations of secure AI: Homomorphic encryption for distributed learning systems," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 8, pp. 2967–2975 (2025), doi: 10.47974/JDMSC-2441.

[10] S. Li, Y. Chen, L. Chen, J. Liao, C. Kuang, K. Li, W. Liang, and N. Xiong, "Post-quantum security: Opportunities and challenges," *Sensors*, vol. 23, no. 21, Art. no. 8744 (2023), doi: 10.3390/s23218744.

[11] M. Ebrahim, A. Hafid, and E. Elie, "Blockchain as privacy and security solution for smart environments: A survey," *arXiv* preprint arXiv:2203.08901 (2022), doi: 10.48550/arXiv.2203.08901.

[12] H. Sebestyen, D. E. Popescu, and R. D. Zmaranda, "A literature review on security in the Internet of Things: Identifying and analysing critical categories," *Computers*, vol. 14, no. 2, Art. no. 61 (2025), doi: 10.3390/computers14020061.

Received March, 2026