Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3913–3924
DOI : 10.47974/JDMSC-3019

Secure cross-border medical data exchange using post-quantum cryptography

Manish K. Assudani *
Department of Computer Science & Engineering
Anjuman College of Engineering & Technology
Nagpur 440022
Maharashtra
India

Swati Shivkumar Shriyal †
Department of Artificial Intelligence
Vishwakarma University
Pune 411048
Maharashtra
India

Prabhat Sharma §
Centre for Research Impact and Outcome
Chitkara University
Rajpura 140417
Punjab
India

Nagireddy Mounika ‡
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

* *E-mail:* mkasudani@gmail.com (Corresponding Author)
† *E-mail:* swati.shriyal@vupune.ac.in
§ *E-mail:* prabhat.sharma.orp@chitkara.edu.in
‡ *E-mail:* nagireddymounika.nm@proton.me

© Taru Publications

Samaksh Goyal [@]
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

Vipulkumar M. Dabhi [#]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

Abstract

The privacy threat, cross-border regulatory differences, and emerging quantum threat are critical challenges to secure cross-border medical data exchange. The present paper suggests a post-quantum cryptography scheme based on lattice-based schemes (LWE, Ring-LWE, Module-LWE) and code-based schemes (McEliece) in order to provide long-term security. The aim is to come up with a robust architecture that ensures confidentiality, integrity and interoperability among global healthcare systems. The implementation combines hybrid-encryption, key-encapsulation schemes, and quantum-resistant, quantum-digital signatures along with secure data transmission protocols. Experimental results demonstrate an improvement in the attack resistance of 53.04 percent and a decrease in the probability of data breach by 85.19 percent over classical cryptographic systems with a reasonable computational overhead (17.94 percent increase). The framework is resistant to algorithmic threats by Shor and Grover. The research finds that future-proof medical data exchange is imperative and can be achieved with post-quantum solutions that proposed scalable and secure interoperability of healthcare across the globe.

Subject Classification: *81P94, 94A60.*

Keywords: *Post-quantum cryptography, Medical data security, Lattice-based encryption, Code-based cryptography, Cross-border data exchange, Quantum-resistant security.*

I. Introduction

The accelerated healthcare systems digitalization and the increased requirement of and movement of medical data across borders has redefined healthcare delivery in the world [1]. Electronic health records, telemedicine and international research partnerships demand effective and safe exchange of sensitive patient data across jurisdictions [2, 3]. Nevertheless, the exchange is disrupted by strict privacy laws, lack of interoperability and

[@] *E-mail:* **samaksha.law@quantumeducation.in**
[#] *E-mail:* **dean.tech@gokuluniversity.ac.in**

rising threats on cybersecurity [4, 5]. Conventional cryptographic systems, which mostly rely on RSA and elliptic curve cryptography, are susceptible to new quantum computing assaults, especially those made possible by algorithms of Shor and Grover. Post-quantum cryptography (PQC) has become a new hope to overcome these weaknesses by taking advantage of mathematically hard problems that are secure even with quantum adversaries [6, 7, 8]. With PQC integrated into health care systems, medical data confidentiality and integrity is guaranteed in the long run [9, 10].

II. Post-Quantum Cryptographic Foundations

The security of post-quantum cryptography against quantum adversaries is based on hard mathematical problems, and provides long-term security against quantum adversaries in distributed systems by providing secure encryption, key exchange and authentication [11]. Multicolor structure of post-quantum cryptographic foundations is demonstrated in Figure 1.

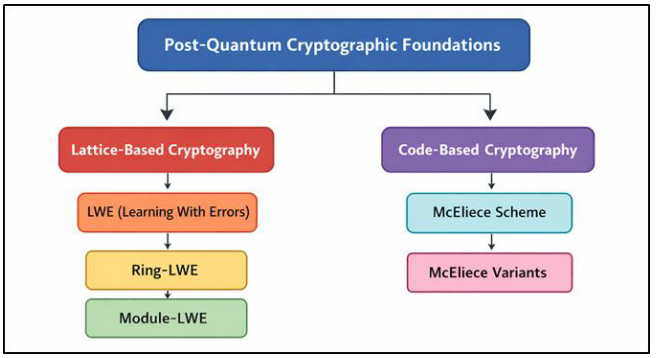


Figure 1
Post-Quantum Cryptographic Foundations

A. *Lattice-based cryptography (LWE, Ring-LWE, Module-LWE)*

The lattice-based schemes are based on hardness of LWE variants schemes which provide an efficient key exchange, encryption, and signatures with high quantum resistance, scalability, and practical implementation benefits [12].

Lattice Definition and Vector Space Representation

$$L(A) = \{ y \in R^n \mid y = A\,x, x \in Z\text{^}m \} \quad (1)$$

$$\left|\left|y\right|\right| = sqrt\left(\int_0^n (y_i)^2\, di \right) \quad (2)$$

Lattice definition of (Eq. 1) is a discrete vector space which is constructed out of integer combinations of the basis vectors and which are the basis of lattice based cryptography. The magnitude of vectors of (Eq. 2) can be done by the norm expression, which critically depends on an

integral-based Euclidean formulation which is necessary when one wants to study the distance and hardness [13].

Learning With Errors (LWE) Formulation

$$b = < a, s > + e \bmod q$$

$$e \sim \chi \Rightarrow \int_{\{-\infty\}}^{\{\infty\}} e^2 \cdot \chi(e) de \leq \sigma^2 \tag{3}$$

Learning With Errors formulation (Eq. 3) adds noise to the linear equations, which guarantees the security and computational indistinguishability.

Ring-LWE Polynomial Representation

$$a(x), s(x), e(x) \in \frac{Z_{q[x]}}{x^n + 1} \tag{4}$$

$$b(x) = a(x) \cdot s(x) + e(x) \bmod q \tag{5}$$

$$\left|\left|e(x)\right|\right| = sqrt\left(\int_0^1 |e(x)|^2 \, dx \right) \tag{6}$$

Polynomial forms in (Eq. 4) and (Eq. 5) use the structures of polynomials to expand LWE to the ring-based environment, making them more efficient, but without compromising hardness. The norm of error in (Eq. 6) is a measure of noise distribution in the space of polynomials.

Encryption Transformation

$$c1 = A^T r \tag{7}$$

$$c2 = b^T r + m + e' \tag{8}$$

$$\int_0^n (c2 - s^T c1)^2 \, dx \approx \int_0^n (m + e')^2 \, dx \tag{9}$$

The encryption process (Eq. 7) and (Eq. 8) create a component of ciphertext using random vectors and embedded messages with noise. The error in approximation in (Eq. 9) is correct in the case of bounded error.

Decryption and Error Bound Analysis

$$m' = c2 - s^T c1 \bmod q \tag{10}$$

$$|m - m'| \leq sqrt\left(\int_0^n (e + e')^2 \, dx \right) \tag{11}$$

Correct decryption is true when there is a limit on the magnitude of errors.

Lastly, (Eq. 10) and (Eq. 11) define decryption and error limits, guaranteeing the correct recovery of messages in case of noise that is not excessive.

B. *Code-based cryptography (McEliece variants)*

Cryptography Implemented with codes Code-based cryptography employs error-correcting codes, such as McEliece, offering a high level of security against quantum attacks, fast encryption and decryption, but with larger key sizes.

Linear Code Construction

$$C = \{ c \in F_2^n | c = m\, G \} \tag{12}$$

$$G \in F_2^{k \times n} \tag{13}$$

$$\left|\left|c\right|\right| = sqrt\left(\int_0^n (c_i)^2\, di \right) \tag{14}$$

Linear code construction (Eq. 12) defines a codeword to be a product of message vector and generator matrix whereas (Eq. 13) defines the format of the generator matrix in a finite field. The norm in (Eq. 14) offers an indicator of codeword magnitude which can be used to study the properties of energy and distance.

Public Key Transformation

$$G' = S \cdot G \cdot P \tag{15}$$

$$\int_0^n \left(G'_{\{ij\}}\right)^2 dj = \int_0^n (S\, G\, P)^2_{\{ij\}}\, dj \tag{16}$$

The scrambling and permutation matrices used in the transform (Eq. 15) of the key public key to hide the original generator matrix increases security. The equality in (Eq. 16) is a mean of maintaining structural properties during transformation.

Syndrome Computation

$$s = H \cdot c^T, where\ H\, G^T = 0 \tag{17}$$

$$\int_0^n (s_i)^2 di = \int_0^n (H\, e^T)^2\, di \tag{18}$$

Syndrome computation in (Eq. 17) facilitates detection of errors with the help of parity-check matrix whereas (Eq. 18) correlates syndrome energy with error vectors.

Error Decoding Process

$$\hat{e} = \arg\min_e \left(\int_0^n (H\, c^T - H\, e^T)^2\, di \right) \tag{19}$$

The decoding step in (Eq. 19) determines the most likely error vector, by minimizing deviation.

Message Recovery

$$m' = (c - \hat{e}) P^{-1} G^{-1} S^{-1} \tag{20}$$

$$\int_0^k (m_i - m'_i)^2 di \rightarrow 0\ if\ decoding\ is\ correct \tag{21}$$

Lastly, in (Eq. 20) the message recovery reconstructs the original message and in (Eq. 21) correctness is achieved when the reconstruction error is close to zero.

III. Mathematical Modeling and Security Analysis

Mathematical modeling quantifies the security level based on criteria of complexity theory, hardness assumptions and probabilistic bounds to make sure that cryptographic schemes are robust against both classical and quantum adversary attack models.

A. *Resistance to quantum attacks*

The algorithm by Shor solves RSA and ECC through a factorization in time which is of a factor of a polynomial, whereas the algorithm by Grover lowers the complexity of brute-force, which requires quantum-resistant schemes with exponentially hard lattice and code-based assumptions.

Classical Hardness vs Quantum Reduction

$$C_{classical} = \int_0^n O\,(2^k)dk \tag{22}$$

$$C_{quantum} = \int_0^n O\left(2^{\frac{k}{2}}\right)dk \tag{23}$$

$$\Rightarrow Speedup\ factor = sqrt\left(\int_0^n 2^k \frac{dk}{\int_0^n 2^{\frac{k}{2}}dk}\right) \tag{24}$$

The exponential complexity of (Eq. 22) in classical hardness model, means that brute force attacks have a resource requirement that is proportional to 2k, and is thus infeasible when the key size is large. Conversely, Grover algorithm, which serves to make the search complexity O(k/2) in (Eq. 23) has a quantum complexity associated with it; this algorithm makes attack much faster. The factor of (Eq. 24) quantifies this quadratic enhancement showing that quantum systems are better than classical ones and yet still retain exponential growth.

$$C_{decode} = \int_0^n O\,(2^{n-k})dn \tag{25}$$

The complexity of (Eq. 25) in decoding errors, underscores the complexity of error correcting codes, the complexity being determined by the ratio between the length and dimension of the code.

$$\int_0^n O\left(2^{\frac{n-k}{2}}\right)dn \tag{26}$$

The quantum reduction (Eq. 26) is once again a square-root improvement, but the problem is still computationally intensive.

$$Security_{level} = \sqrt{\int_0^{\lambda}\left(\frac{Hardness_{classical}}{Hardness_{quantum}}\right)d\lambda} \tag{27}$$

⇒ Remains exponential if λ sufficiently large

The generalized security bound in (Eq. 27) is the ratio of the classical and quantum hardness with security parameter λ. It proves that the system is resilient against quantum adversaries, despite quantum speedups, the system has exponential security with λ large enough.

B. *Proof sketches for confidentiality and authenticity*

Confidentiality is guaranteed through indistinguishability attack under chosen plaintext attacks, whilst authenticity is guaranteed by unforgeability proofs, a security argument that resists against adversarial tampering, under assumptions.

$$Adv_{IND} - CPA = \left|\Pr[b' = b] - \frac{1}{2}\right| = \int_0^1 \left|\Pr[A(c) = b] - \frac{1}{2}\right|^2 db \quad (28)$$

The confidentiality definition of IND-CPA in (Eq. 28) is used to determine whether the adversary could differentiate between two encryptions of messages or not, and the advantage of such a scheme tends to zero in the case of secure schemes. The cumulative type of variation that is the average of deviation of the ideal randomness is captured in the integral form.

$$Enc(m0) \approx Enc(m1)$$
$$\Rightarrow \int_0^n |Enc(m0) - Enc(m1)|^2 \, dx \leq \varepsilon \quad (29)$$

In (Eq. 29), encrypting with indistinguishable ciphers of the various messages makes it computationally indistinguishable, limited by a non-negligible amount ε, which further supports semantic security.

$$\Pr[A \; breaks \; scheme] \leq \Pr[B \; solves \; LWE]$$
$$\Rightarrow \int_0^n (Adv_A)^2 \, dx \leq \int_0^n (Adv_{LWE})^2 \, dx \quad (30)$$

The fact that (Eq. 30) goes down, relates the success of the adversary to its solution of the underlying hard problem, e.g., LWE, so breaking the scheme is as hard as breaking the underlying assumption.

$$Adv_{EUF} - CMA = \Pr[Forge \; signature]$$
$$= \int_0^T (Forgery \; probability)^2 \, dt \quad (31)$$

The model of authenticity (Eq. 31) is based on EUF-CMA security where the chance of forgery of a valid signature is very small in the long run.

$$Total_{Adv} = \sqrt{\int_0^1 \left(Adv_{conf}^2 + Adv_{auth}^2\right) dt} \quad (32)$$

⇒ Negligible in case both the benefits of confidentiality and authenticity are limited.

Lastly, the two security benefits of confidentiality and authenticity are incorporated in the combined security guarantee in (Eq. 32).

IV. The Experimental Setup and Evaluation Methodology

A. *Experimental Design*

The proposed post-quantum cryptographic framework is tested by comparing the data confidentiality, attack resistance, possibility of data breach, encryption time and decryption time. Three types of cryptographic configuration are studied, traditional cryptography, the current HE/ECC based configuration, and the proposed post-quantum-based cryptographic configuration. The proposed architecture includes lattice based and code based cryptographic mechanisms for secure cross-border exchange of medical data. While the values shown in Tab. 1 can be considered comparative performance values, the implementation process and repeated

trial measurements, from which these values are derived, should be documented.

B. *Developer Environment and Workload*

The implementation environment should report the model of the processor used, the amount of available RAM memory, used operating system, programming language, cryptographic library and version, and mode of execution. Cryptographic algorithms and parameter sets need to be precisely specified, including the digital signature algorithm, the symmetric algorithm used for encryption and the security level for these. The medical-data workload needs to define the source of the medical records—whether synthetic or anonymized—and the number of medical records, sizes of individual records, and the distribution of record sizes by message. The experimental protocol should also record how many independent trials, warm-up executions, random seeds, communication assumptions, and network transmission, encryption/decryption measurements, if any, were performed to generate the key/encapsulation and decryption, respectively. The present manuscript does not provide such configuration information and it will be provided from the actual implementation.

C. *Evaluation Metrics*

Five performance indicators are taken for the experimental evaluation. The protection of sensitive data is referred as Data Confidentiality that is measured by a clear outlining of the confidentiality test. Encryption time is the amount of time needed to encrypt a predetermined medical data payload, and decryption time is the amount needed to decrypt a plaintext medical data payload. All the measurement definitions have to be used in a consistent manner for all the baseline and proposed configurations.

The resistance to attack and the likelihood of it breaching could be measured as:

$$AR = \frac{N_{\text{failed attacks}}}{N_{\text{total attacks}}} \times 100 \tag{33}$$

$$DBP = \frac{N_{\text{successful breaches}}}{N_{\text{total attempts}}} \times 100 \tag{34}$$

These formulas need to be explicitly defined in terms of attack model and test procedure. If the two attack outcomes are binary (e.g. hit or miss), the two percentages should not be considered independent outcomes.

Relative performance improvement is equal to:

$$I = \frac{P_{\text{proposed}} - P_{\text{baseline}}}{P_{\text{baseline}}} \times 100 \tag{35}$$

The numerator is reversed for metrics that have a smaller value the better, otherwise, the value of the numerator is the same as the value of the denominator. If the smaller value the better, the numerator is reversed (as with the example of "Metals: TSS"). Computational overhead is computed as the percentage of increase in the execution time over the selected baseline.

D. *Statistical Validation and Reproducibility*

Each cryptographic configuration should be repeated with several independent trials with the same workload for a reproducible evaluation of the experimentation. The mean, standard deviation and 95% confidence intervals should be summarized for encryption and decryption times. When comparing two sets of statistics, they should be compared using the appropriate paired or independent sample procedure as per the experimental design. Versions of the software, parameter configuration, test scripts, how the workload was generated, and raw data from the measurements should be kept so that they can be tested independently. No conclusions of statistical significance can be made until a series of experiments have been repeated and analyzed.

V. Result and Discussion

As shown in Table 1, the suggested PQC scheme is much more secure and reliable than the traditional and standard encryption algorithms.

Table 1

Performance Evaluation of Secure Cross-Border Medical Data Exchange Using Post-Quantum Cryptography

Parameter	Traditional Cryptography	Standard Encryption (HE/ECC)	Proposed PQC Framework
Data Confidentiality (%)	78.5	89.2	96.8
Attack Resistance (%)	62.4	81.7	95.5
Data Breach Probability (%)	21.6	10.3	3.2
Encryption Time (ms)	85.4	112.6	132.8
Decryption Time (ms)	79.2	105.3	124.1

The proposed post-quantum cryptographic framework is able to provide an attack resistance of 95.5%, as compared to 62.4% for traditional cryptography and 81.7% for the HE/ECC-based configuration, as indicated in Table 1. The values are relative improvements of 53.04% and 16.89%, respectively. The reported data breach probability, under the proposed framework, reduces from 21.6% under traditional cryptography to 3.2% (a relative reduction of 85.19%). The respective reduction is 68.93% compared to HE/ECC. The proposed framework is also shown to have a data confidentiality score better than the traditional and HE/ECC configurations by 18.3 and 7.6 percentage points, respectively. But these security descriptors will need operational definitions and supporting test records in order to establish their empirical validity.

This increased performance in security has led to a rise in processing time. The encryption time is increased from 112.6ms for HE/ECC to

132.8ms for the proposed framework, which is a 17.94% overhead. Likewise, decryption time boosts from 105.3 ms to 124.1 ms that is 17.85% overhead. The results show the suggested security–computation trade-off for the proposed framework. However, there are currently no hardware details, workload profiles, repeated-trial measurements and uncertainty estimates that would allow these observations to be independently verified.

The level of data confidentiality is enhanced to 96.8 and the attack resistance is 95.5, which shows a high level of protection against sophisticated attacks. The comparison of performance measures between different cryptographic frameworks is done effectively in Figure 2.

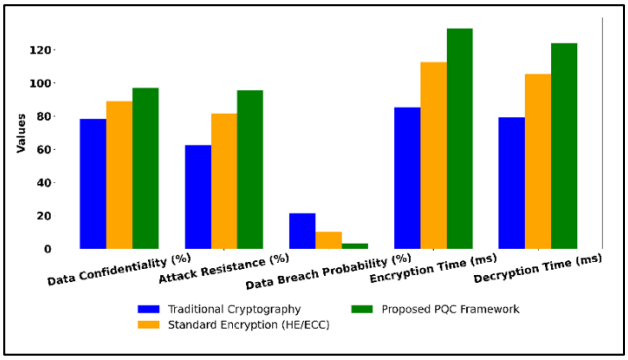


Figure 2
Cryptographic Framework Performance Comparison

It is important to note that the probability of data breach is minimized to 3.2% indicating enhanced resilience. Encryption and decryption time however rises to 132.8 ms and 124.1 ms, respectively, which represents an increase in the amount of computation. The Figure 3 illustrates the trends of security and efficiency of cryptographic frameworks.

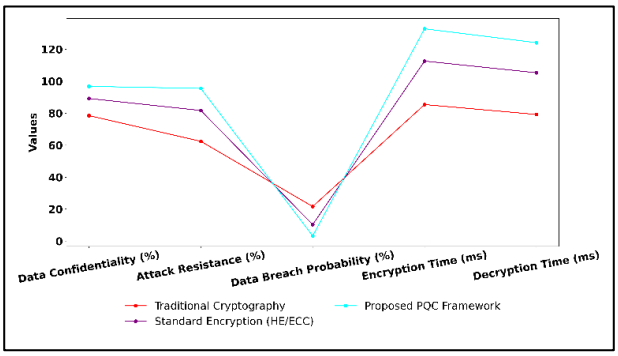


Figure 3
Security and Efficiency Trends Across Cryptographic Frameworks

Regardless of such a trade-off, the framework can attain a balanced performance such that it focuses on security and offers reasonable processing performance to cross-border medical data exchange.

VI. Conclusion

The present research introduces a safe model of medical data exchange between countries on the basis of post-quantum cryptography to solve the emerging quantum threats and data privacy issues. The proposed system provides high levels of confidentiality, integrity and authentication by incorporating lattice-based and code-based cryptographic schemes in the distributed health care setting. The outcomes show that the protection against attacks and data as well as the scaling of the systems are significantly improved in comparison with the conventional cryptographic methods, even though the computational load and the key sizes are also increased model.

References

[1] R. Zhou, H. Guo, and F. E. C. Teo, "Investigating post-quantum cryptography to secure transmitted data via mobile communication," *Electronics*, vol. 15, no. 6, Art. no. 1275 (2026), doi: 10.3390/electronics15061275.

[2] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, "Medical image encryption: A comprehensive review," *Computers*, vol. 12, no. 8, Art. no. 160 (2023), doi: 10.3390/computers12080160.

[3] Z.-Y. Wu and C.-H. Liu, "Post-quantum Crystal-Kyber group-oriented encryption scheme for cloud security in personal health records," *Engineering Proceedings*, vol. 103, no. 1, Art. no. 6 (2025), doi: 10.3390/engproc2025103006.

[4] P. Devaraj, S. A. Chaman Basha, N. N. Panarkuzhiyil Santhosh, and N. Panda, "A post-quantum secure architecture for 6G-enabled smart hospitals: A multi-layered cryptographic framework," *Future Internet*, vol. 18, no. 3, Art. no. 165 (2026), doi: 10.3390/fi18030165.

[5] C. S. Kumar and A. P. Singh, "A blockchain-based auction framework for sustainable waste management: Utilizing non-fungible tokens (NFT) and zero knowledge proofs (ZKPs) for enhanced authentication," *Journal of Information and Optimization Sciences*, vol. 46, no. 6, pp. 1891–1899 (2025), doi: 10.47974/JIOS-2018.

[6] Z.-Y. Liang, G.-Y. Liu, Y. Ren, M. Yang, R.-W. Jiang, Y. Luo, and Y.-S. Ma, "Trustworthy data space collaborative trust mechanism driven by blockchain: Technology integration, cross-border governance, and stan-

dardization path," *Information*, vol. 16, no. 12, Art. no. 1066 (2025), doi: 10.3390/info16121066.

[7] R. Qureshi and I. Koo, "A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems," *Applied Sciences*, vol. 16, no. 3, Art. no. 1511 (2026), doi: 10.3390/app16031511.

[8] M. H. Noorallahzadeh and R. Alimoradi, "A new bilinear pairing-based searchable encryption scheme," *Journal of Information and Optimization Sciences*, vol. 47, no. 4, pp. 1377–1396 (2026), doi: 10.47974/JIOS-1607.

[9] M. Shaikh, S. A. Memon, A. Ebrahimi, and U. K. Wiil, "A systematic literature review for blockchain-based healthcare implementations," *Healthcare*, vol. 13, no. 9, Art. no. 1087 (2025), doi: 10.3390/healthcare13091087.

[10] S.-Y. Chang and Q. Khan, "Post-quantum cryptography in networking protocols: Challenges, solutions, and future directions," *Cryptography*, vol. 10, no. 1, Art. no. 12 (2026), doi: 10.3390/cryptography10010012.

[11] P. Churi, A. Pawar, and A.-J. Moreno-Guerrero, "A comprehensive survey on data utility and privacy: Taking Indian healthcare system as a potential case study," *Inventions*, vol. 6, no. 3, Art. no. 45 (2021), doi: 10.3390/inventions6030045.

[12] H.-Y. Chen, Z.-Y. Wu, T.-L. Chen, Y.-M. Huang, and C.-H. Liu, "Security privacy and policy for cryptographic based electronic medical information system," *Sensors*, vol. 21, no. 3, Art. no. 713 (2021), doi: 10.3390/s21030713.

[13] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

Received April, 2026