Received: 2026-02-26
Accepted: 2026-03-27
Published Online: 2026-04-06
DOI: 10.70454/JRICST.2026.30202

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

Cryptographic Techniques for IoT: A Survey of Symmetric, Asymmetric, and Post Quantum Algorithms

Bhupender Singh Rawat*[1], Mohan Vishal Gupta[2], Navneet Vishnoi[3], Ranjana Sharma[4]

[1]Professor, College of Smart Computing , COER University, Roorkee, India.
[2]Associate Professor, CCSIT, Teerthanker Mahaveer University, Moradabad , India.
[3]Associate professor, Department of Cyber Security and IOT, greater Noida Institute of Technology, Greater Noida, India.
[4]Associate professor, Department of computer science and engineering SRM Institute of Science and Technology, Delhi NCR Campus, Ghaziabad, India

***Corresponding Author Email**: rawat.bhupender@gmail.com

Abstract

In this paper, we investigated the most widely utilized group key management approaches, which enabled and best-effort perspective within a trusted domain, for the Internet of Things (IoT) devices. The protection of such data is extremely challenging, as a majority of IoT devices have limited computation capabilities, small memory size, and constrained battery life. Traditional security techniques are usually excessively resource-intensive in such scenarios. This review quantitatively discusses three types of cryptographic primitives that can be executed on IoT devices, Symmetric Cryptography, Asymmetric Cryptography, and Post-Quantum Cryptography. Symmetric cryptographic algorithms are widely used in IoT, as they have the highest throughput among other cryptographic primitives and they are energy efficient, due to their applicability for fast and low-energy data protection on devices. Asymmetric Cryptography plays an important role in secure key exchange and device authentication, especially in large scale and distributed IoT networks. Strong security is needed, but at the same time, devices must be able to communicate even if they have never met. Post-Quantum Cryptography is a new research area that aims to protect systems against powerful quantum computers in the future that are potentially capable of breaking most of the existing algorithms. However, while post-quantum algorithms are more secure, they can also be more resource-intensive, posing a challenge for small IoT devices. This paper emphasizes the importance of selecting cryptographic schemes that can provide strong security in spite of the constrained capabilities of IoT devices.

Keywords: Internet of Things, Lightweight Cryptography, Symmetric Encryption Algorithms, Asymmetric Cryptographic Techniques, Post-Quantum Cryptography

Received: 2026-02-26
Accepted: 2026-03-27
Published Online: 2026-04-06
DOI: 10.70454/JRICST.2026.30202

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

1. Introduction

The Internet of Things (IoT) has rapidly transformed our lives by connecting billions of devices, including sensors, wearables, smart homes, industrial machines, and healthcare systems, to form intelligent, data-driven environments. Increasingly, these IoT ecosystems are becoming larger and more dynamic, with substantially more data being produced and shared among a wide variety of devices, such as heterogeneous and resource-constrained ones. It is now a major problem to secure that data, keep it private and unaltered [1]. Traditional security systems, developed for environments with ample computing resources, are not suitable for IoT applications, given the energy, processing, and memory constraints of IoT devices. Cryptography is at the heart of securing IoT communication to provide data confidentiality, data origin authentication, and access control. Nevertheless, the choice of adequate cryptographic algorithms is application-dependent and must consider both security strength and computational efficiency. Recently, several lightweight cryptographic primitives have the property to be suitable for IoT and constrained devices, ranging from symmetric encryption schemes, asymmetric key schemes, hash functions or even combinations of them. At the same time, new paradigms, such as post-quantum security and blockchain-based security frameworks, are shaping the design of future secure IoT systems [2][3].

Rethinking cryptographic algorithms for IoT systems is mainly motivated by the stringent resource constraints {energy, CPU cycles, RAM/ROM} of trillions of sensor nodes and smart objects that form the backbone of IoT, which do not have the luxury to run traditional, resource-hungry algorithms such as AES-256 or RSA. This requirement has given rise to the domain of Lightweight Cryptography (LWC), in which the algorithms are tailored to achieve the minimum hardware size, memory, and power consumption at the cost of providing the maximum security for the specific application scenario. Some of the most relevant are: PRESENT and SIMON/SPECK (symmetric block ciphers, with PRESENT geared towards hardware and SPECK towards software implementation), and Elliptic Curve Cryptography (ECC) (asymmetric), favored over RSA for its significantly smaller key sizes that nonetheless provide the same level of security. The international standardization efforts led by NIST Lightweight Cryptography Standardization Process recently has been completed by selecting Ascon family of algorithms to be the standard for authenticated encryption with associated data (AEAD) and hashing, this represents a significant milestone delivering a suite of publicly reviewed, resource-aware building blocks which are now strongly advised to be adopted to secure the next wave of constrained IoT devices from threats such as side-channel attacks and data integrity violations.

This paper presents a review that focuses on the design principles, performance, advantages, and disadvantages of the cryptographic algorithm used in the Internet of Things (IoT). Consideration of classical cryptographic as well as lightweight cryptographic schemes gives a comprehensive overview of how security may be efficiently realized in a wide range of IoT applications, including smart agriculture, industrial IoT, health care monitoring, and smart city frameworks. The review also explores current research challenges and the increasing demand for efficient, scalable, and quantum-secure cryptographic techniques to support the future generation of IoT.

Received: 2026-02-26
Accepted: 2026-03-27
Published Online: 2026-04-06
DOI: 10.70454/JRICST.2026.30202

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

2. Literature Review

The security issue of the Internet of Things (IoT) has been attracting more and more research interests in recent years, because of the increasing number of connected devices and critical information communicated. Initial researches were concentrated on traditional cryptographic algorithms like AES, RSA, and SHA and their related protocols, which were developed for IoT environments. Although these algorithms are highly secure, there are some known constraints such as the computational expense and the energy consumption. This led to the need of a lightweight cryptography designed for constrained environments [4].

There have been a number of analysis on the symmetric key ciphers, which include AES and its strength is not doubted but its suitability for low-power sensors has been questioned. Light weight Balanced review such as PRESENT, LED, HIGHT and SIMON/SPECK give better performance in terms of execution speed and lower memory consumption. Studies have compared these algorithms and showed that lightweight ciphers significantly reduce the energy consumption while providing sufficient levels of security. Regarding asymmetric cryptography, RSA was considered impractical for IoT because of its large key size and high computational cost. Instead, Elliptic Curve Cryptography (ECC) became a better choice. Several papers also proved how ECC-based key exchanges provide enhanced security while still being practical for devices with limited resources. Research has also been done on identity-based encryption and certificate less cryptography as means of simplifying key management. Researchers also surveyed hash functions for authentication and integrity checking. SHA-256 and SHA-3 are well established, however in the context of IoT a number of lightweight hash functions such as PHOTON and SPONGENT have recently appeared [5][6].

Recent literature highlights the rise of **post-quantum cryptography** to counter future threats from quantum computers, which can break traditional systems. Additionally, **blockchain-based IoT security** models provide decentralized trust management and tamper-proof communication [10] [11].Broadly, the literature explores a transition from classical algorithms to efficient footprint, energy-aware_footprint, scalable, and quantum-safe cryptographic primitives and protocols. Nevertheless, the choice of a proper algorithm is still application-dependent in terms of power, latency, storage, and threat model. Figure 1 about Classification of Cryptographic Algorithms.

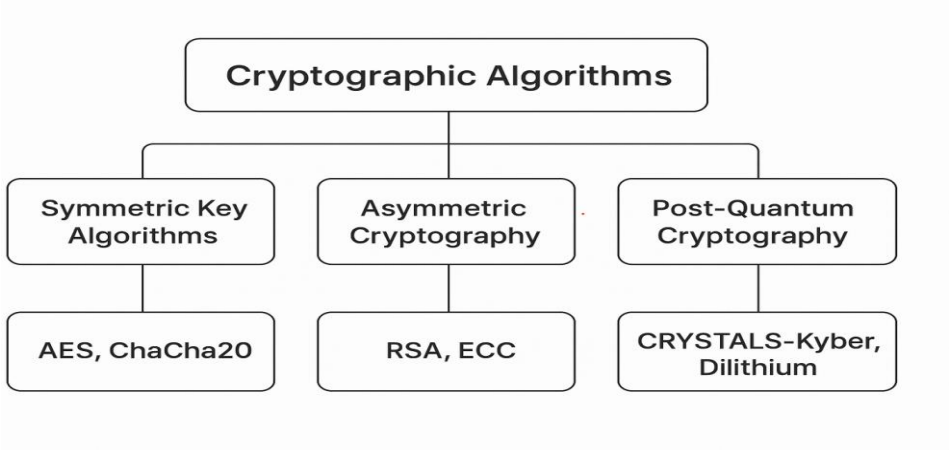

Figure 1: Classification of Cryptographic Algorithms

Received: 2026-02-26
Accepted: 2026-03-27
Published Online: 2026-04-06
DOI: 10.70454/JRICST.2026.30202

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

Table 1: Symmetric Key Algorithms Used in IoT Systems

Algorithm	Type	Key Size	Block/Stream Size	Advantages	Limitations	Suitability for IoT
AES (Advanced Encryption Standard)	Block Cipher	128, 192, 256 bits	128-bit blocks	Highly secure, fast, widely supported in hardware; energy efficient	Implementation complexity for ultra-low-power devices	Excellent – most recommended for IoT
DES (Data Encryption Standard)	Block Cipher	56 bits	64-bit blocks	Simple design, easy to implement	Weak security, vulnerable to brute-force attacks	Poor – outdated for IoT
3DES (Triple DES)	Block Cipher	112 or 168 bits	64-bit blocks	Stronger than DES, legacy compatibility	Very slow; high computational cost	Low – not efficient for IoT devices
RC4	Stream Cipher	40–2048 bits	Stream-based	Simple, lightweight	Serious security vulnerabilities; deprecated	Not suitable for IoT
ChaCha20	Stream Cipher	256 bits	Stream-based	Very fast, highly secure, resistant to timing attacks	Less hardware support compared to AES	Very good – used in modern IoT communication
Blowfish	Block Cipher	32–448 bits	64-bit blocks	Flexible key size, efficient	Slow re-keying process	Moderate – works on some IoT but not ideal
Twofish	Block Cipher	128, 192, 256 bits	128-bit blocks	Strong security, efficient on various platforms	Slightly complex design	Good – secure and fast

Table 1, Symmetric key algorithms are optimal for the security of IoT systems as they are efficient in terms of speed and energy consumption. The same key is used by the sender and the receiver to lock and unlock the data in this process. This makes it ideal for small IoT devices, such as sensors and smart gadgets, that typically have limited battery life and computing capabilities. The prime candidate for this has always been AES since it is very secure and runs well on modern chips. ChaCha20 is also very good for simpler devices. In general, symmetric encryption can keep data secure without exhausting a device's resources [20].

Received: 2026-02-26
Accepted: 2026-03-27
Published Online: 2026-04-06
DOI: 10.70454/JRICST.2026.30202

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

Table 2: Asymmetric Cryptographic Algorithms Used in IoT Systems

Algorithm	Type	Key Size	Security Strength	Advantages	Limitations	Suitability for IoT
RSA	Public–Private Key (Asymmetric)	1024–4096 bits	Moderate–High	Well-established, widely supported, easy key generation	High computational cost, high energy usage, slow for small IoT devices	Low–Moderate (not suitable for constrained IoT nodes)
ECC (Elliptic Curve Cryptography)	Asymmetric	160–521 bits	Very High (e.g., 256-bit ECC ≈ 3072-bit RSA)	Lightweight, faster, smaller keys, low power use	More complex mathematics; hardware/software compatibility needed	Excellent – Most recommended for IoT
ElGamal	Asymmetric	2048 bits	High	Strong security, useful for digital signatures	Slower, larger ciphertext, high computation	Moderate – possible but not ideal for low-power devices
Diffie–Hellman (DH)	Key Exchange	1024–4096 bits	High	Enables secure key exchange over insecure channels	Vulnerable without authentication; heavy computation	Moderate – use ECC-based DH (ECDH) for IoT

Table 2, Asymmetric cryptographic protocols (which are based on public key cryptography) are required in IoT systems to provide authentication (i.e., prove the identity of a device) and facilitate secure key exchange (that is securely share the password for symmetric encryption). Rather than using one key, as in symmetrical methods, these algorithms employ two separate keys: a private key for decryption and a public key for encryption. A typical algorithm is RSA, but it is frequently too heavy for small devices as it needs very large key sizes to be secure [7][8]. Thus, Elliptic Curve Cryptography (ECC) is the right standard for IoT. ECC offers the same level of security as RSA with much smaller key sizes (e.g. A 256-bit ECC key is equivalent in strength to a 3072-bit RSA key). This efficiency considerably reduces battery consumption and computational burden, thus ideal for resource-constrained sensors. Typically, IoT devices take a hybrid approach: they perform slow asymmetric algorithms (e.g., ECC) once to verify identity and share a key, then use fast symmetric algorithms (e.g., AES) to actually send data[9] [18] [19].

Received: 2026-02-26
Accepted: 2026-03-27
Published Online: 2026-04-06
DOI: 10.70454/JRICST.2026.30202

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

Table 3: Post-Quantum Cryptographic Algorithms for IoT Systems

Algorithm / Family	Category	Key / Signature Size	Security Level	Advantages	Limitations	Suitability for IoT
CRYSTALS-Kyber	Lattice-Based	Public Key: ~800–1500 bytes Ciphertext: ~700–1500 bytes	High (NIST L1–L5)	Fast, efficient, strong security; good for key exchange	Larger key sizes compared to ECC	Excellent – Best current PQC choice for IoT key exchange
CRYSTALS-Dilithium	Lattice-Based	Signature: 2–3 KB Public Key: ~1–2 KB	High	High performance, robust security, standardized by NIST	Larger signatures, increased bandwidth	Very Good – Suitable for medium-power IoT devices
Falcon	Lattice-Based (Signature)	Signature: ~700 bytes Public Key: ~1 KB	High	Small signatures, efficient verification	Complex implementation	Good – Suitable where bandwidth is limited
SPHINCS+	Hash-Based (Signature)	Signature: 8–30 KB	High	Very strong and conservative (hash-based only)	Very large signatures; slower	Moderate – Good for high-security, not ideal for constrained nodes
BIKE, HQC	Code-Based (KEM)	Public Key: ~6–7 KB	High	Strong theoretical foundation	Much larger keys than lattice schemes	Moderate – Suitable for gateways, not tiny IoT
FRODOKEM	Lattice-Based	Public Key: 9–12 KB	High	Strong security, conservative design	Very slow, heavy memory use	Poor – Too heavy for IoT
NTRU / NTRU Prime	Lattice-Based	Public Key: ~1 KB	High	Efficient and secure alternative to Kyber	Slightly slower than Kyber	Good – Works well on IoT with moderate resources

Table 3, Post-Quantum Cryptography, is the design and implementation of new “digital locks” that can resist being cracked by a super-powerful future quantum computer. At the moment, IoT devices

Received: 2026-02-26
Accepted: 2026-03-27
Published Online: 2026-04-06
DOI: 10.70454/JRICST.2026.30202

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

employ traditional keys (like RSA) that could be broken by a quantum computer, potentially exposing sensitive information. PQC schemes, such as CRYSTALS-Kyber (encryption) and Falcon (digital signatures), rely on advanced mathematics that is believed to be resistant to these attacks [12] [13] [14].

The biggest challenge for IoT is that these algorithms are "heavy" – they frequently require large keys, and more processing power than tiny, battery-run sensors can handle. As such, the researchers are now working towards rendering these algorithms lightweight and power-efficient so that our smart devices will continue to remain secure in the future without running out of battery [15] [16] [17].

2.1 Problem Statement

The proliferation of the Internet of Things (IoT) has resulted in billions of interconnected devices that collect, process, and exchange sensitive information. Yet, these devices are usually subject to very stringent constraints, including limited computing power, low memory, minimal energy capacity, and insecure communication media. Conventional cryptographic algorithms, which were developed with traditional high-performance computing systems in mind, do not necessarily cater to the specialized security and efficiency needs of IoT networks. Consequently, IoT systems continue to be susceptible to cyberattacks such as data tampering, illegal access, device impersonation, and man-in-the-middle attacks.

Despite the variation of cryptographic algorithms, which can be classified, e.g., into symmetric and asymmetric schemes and also take post-quantum approaches, there is no universally accepted know-how that defines which ones are the best in several IoT use-case conditions. This uncertainty in relation to the performance, security strength, resources needed, and applicability of an algorithm into the real world leads to the fact that both researchers and IoT system designers have problems. As a consequence, a comprehensive survey on cryptography is required so that existing cryptographic algorithms could be analyzed, compared and assessed in addition, based on security, efficiency, and scalability considerations a best suitable cryptographic algorithm can be identified that adequately fulfils the requirements of lightweight constrained IoT devices. Most traditional security algorithms are too heavy and slow for tiny IoT devices, making their batteries run out fast or their systems lag. And with that, a lot of people skipped strong security, and ended up with devices full of holes that hackers can take over almost instantly.

3. Research Gap

There is a lack of practical execution guidance. Nevertheless, a number of those algorithms with good theoretical performance have not been studied enough in real implementations, considering hardware limitations, battery life, or interoperability. Additionally, the study on post-quantum lightweight cryptography for the Internet of Things (IoT) is still in its infancy, and there are no standardized policies.

Security solutions tend to be best designed to meet the needs of individual applications, and are ill-suited to providing flexible and scalable protection for diverse IoT environments. Therefore, it is desirable to develop a unified, flexible, and energy-efficient cryptographic framework that can support long-term security in the face of evolving cyber threats.

Received: 2026-02-26
Accepted: 2026-03-27
Published Online: 2026-04-06
DOI: 10.70454/JRICST.2026.30202

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

4. Challenges of Cryptographic Algorithms in IoT

A. **Resource Constraints of IoT Devices:** IoT nodes typically have limited CPU power, memory, and storage. Many standard cryptographic algorithms (like RSA or AES-256) are computationally intensive and cannot run efficiently on ultra-low-power devices, making secure implementation difficult.
B. **High Energy Consumption:** Cryptographic operations increase energy usage, especially public-key algorithms. Since many IoT devices rely on small batteries or energy harvesting, heavy encryption significantly reduces operational lifespan.
C. **Scalability and Key Management:** Managing secure key generation, distribution, storage, and periodic updates becomes extremely challenging when networks scale to thousands or millions of devices. Traditional PKI infrastructures are not always suitable for large IoT deployments.
D. **Heterogeneity of IoT Devices and Protocols:** IoT ecosystems contain diverse devices with varying capabilities, operating systems, and communication technologies. Designing cryptographic solutions that remain efficient, interoperable, and secure across all platforms is difficult.
E. **Vulnerability to Physical and Side-Channel Attacks:** IoT devices are often deployed in open or unprotected environments, making them vulnerable to tampering, device capture, power analysis, and timing attacks. Even strong algorithms can fail if the hardware is exposed.

5. Conclusion

Exponential growth in IoT devices has been reported in the domains of healthcare, smart cities, agriculture, and industry, which makes the application security mechanism that is stronger, more efficient, and more scalable even more urgent. A diverse range of cryptographic algorithms, including symmetric, asymmetric, lightweight, and post-quantum algorithms, was reviewed, and their appropriateness for IoT environments with limited resources was considered. The speed of the symmetric algorithms, such as AES and ChaCha20, and their energy efficiency keep them in the lead for real-time data protection. Asymmetric schemes, notably ECC, solve the problems of authentication and secure key exchange with very strong security and at a fraction of the computational cost of conventional RSA. Lightweight cryptographic primitives (e.g., PRESENT, SIMON/SPECK, and NIST-recommended Ascon family) enable viable options for ultra-low-power nodes where traditional security schemes are non-applicable. At the same time, post-quantum schemes such as CRYSTALS-Kyber, Dilithium, and Salmon are the latest wave of IoT security technology, protecting users against future quantum attacks. However, many challenges remain, such as high energy consumption, limited processing capabilities, scalability of key management, hardware heterogeneity, and vulnerability to physical and side-channel attacks. In summary, the survey demonstrates that IoT security cannot be achieved via a single class of cryptosystem, but a well-rounded and contextual, tailored amalgamation exploiting the strength of different cryptosystems is vital to realize a strong and sustainable defense.

Future Scope

In the future, researchers need to work on the design of lightweight post-quantum cryptographic schemes for constrained IoT devices. An emerging requirement is for hybrid cryptographic schemes to combine symmetric, asymmetric, and PQC schemes smartly while being energy efficient. Furthermore, adaptive security models based on AI, cryptography assisted by hardware, and secure

Received: 2026-02-26
Accepted: 2026-03-27
Published Online: 2026-04-06
DOI: 10.70454/JRICST.2026.30202

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

platforms of computing at the edge could reinforce even more the IoT ecosystems. The work on standardization should be pursued in order to guarantee interoperability and performance stability, and the worldwide diffusion of secure-by-design IoT solutions.

Author Contributions

All of the writers agreed on the study's substance. The author has reviewed and approved the final manuscript.

Funding

For this work, the authors did not receive any special funding.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this work.

Reference

[1] D. A. F. Saraiva, V. R. Q. Leithardt, D. de Paula, A. S. Mendes, G. V. González, and P. Crocker, "PRISEC: Comparison of symmetric key algorithms for IoT devices," Sensors, vol. 19, no. 19, p. 4312, 2019, doi: 10.3390/s19194312.

[2] G. Sittampalam and N. Ratnarajah, "Enhanced symmetric cryptography for IoT using novel random secret key approach," in Proc. 2nd Int. Conf. Advancements in Computing (ICAC), Malabe, Sri Lanka, 2020, pp. 398–403, doi: 10.1109/ICAC51239.2020.9357316.

[3] S. Szymoniak and M. Kubanek, "Biometry-based verification system with symmetric key generation method for Internet of Things environments," Sci. Rep., vol. 15, p. 5464, 2025, doi: 10.1038/s41598-025-89226-3.

[4] C. Silva, V. A. Cunha, J. P. Barraca, et al., "Analysis of the cryptographic algorithms in IoT communications," Inf. Syst. Front., vol. 26, pp. 1243–1260, 2024, doi: 10.1007/s10796-023-10383-9.

[5] S. Kumar and C. S. Pillai, "An analysis of lightweight symmetric encryption algorithms for secure data transmission in IoT," in Proc. Int. Conf. Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India, 2024, pp. 1–4, doi: 10.1109/IACIS61494.2024.10721701.

[6] M. S. Henriques and N. K. Vernekar, "Using symmetric and asymmetric cryptography to secure communication between devices in IoT," in Proc. Int. Conf. IoT and Application (ICIOT), Nagapattinam, India, 2017, pp. 1–4, doi: 10.1109/ICIOTA.2017.8073643.

[7] J. Furtak, "The cryptographic key distribution system for IoT systems in the MQTT environment," Sensors, vol. 23, no. 11, p. 5102, 2023, doi: 10.3390/s23115102.

[8] J. L. López Delgado, J. A. Álvarez Bermejo, and J. A. López Ramos, "Homomorphic asymmetric encryption applied to the analysis of IoT communications," Sensors, vol. 22, no. 20, p. 8022, 2022, doi: 10.3390/s22208022.

Received: 2026-02-26
Accepted: 2026-03-27
Published Online: 2026-04-06
DOI: 10.70454/JRICST.2026.30202

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

[9] S. A. Ansari and S. Ali, "A systematic review of lightweight cryptographic schemes for security and privacy in IoT," Discov. Comput., vol. 28, p. 266, 2025, doi: 10.1007/s10791-025-09755-3.

[10] A. Sharma and S. Rani, "Post-quantum cryptography (PQC) for IoT–consumer electronics devices integrated with deep learning," IEEE Trans. Consumer Electron., vol. 71, no. 2, pp. 4925–4933, May 2025, doi: 10.1109/TCE.2025.3569904.

[11] R. Asif, "Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms," IoT, vol. 2, pp. 71–91, 2021, doi: 10.3390/iot2010005.

[12] K. Mansoor, M. Afzal, W. Iqbal, and Y. Abbas, "Securing the future: Exploring post-quantum cryptography for authentication and user privacy in IoT devices," Cluster Comput., vol. 28, no. 2, Apr. 2025, doi: 10.1007/s10586-024-04799-4.

[13] M. M. Alam, A. Arora, A. Bhatt, S. Devliyal, and S. Aluvala, "Cryptographic algorithms for IoT devices: A quantum analysis," in Proc. 3rd Int. Conf. Innovation in Technology (INOCON), Bangalore, India, 2024, pp. 1–7, doi: 10.1109/INOCON60754.2024.10511982.

[14] C.-L. Chen, K.-W. Zeng, W.-Y. Li, C.-F. Lee, L.-C. Liu, and Y.-Y. Deng, "Lightweight post-quantum cryptography: Applications and countermeasures in Internet of Things, blockchain, and E-learning," Eng. Proc., vol. 103, p. 14, 2025, doi: 10.3390/engproc2025103014.

[15] P. Kaur and S. Aggarwal, "Cryptographic algorithms in IoT—A detailed analysis," in Proc. 2nd Int. Conf. Computational Methods in Science and Technology (ICCMST), Mohali, India, 2021, pp. 45–50, doi: 10.1109/ICCMST54943.2021.00021.

[16] S. K. Mousavi, A. Ghaffari, S. Besharat, et al., "Security of Internet of Things based on cryptographic algorithms: A survey," WirelessNetw., vol. 27, pp. 1515–1555, 2021, doi: 10.1007/s11276-020-02535-5.

[17] K. CherkaouiDekkaki, I. Tasic, and M.-D. Cano, "Exploring post-quantum cryptography: Review and directions for the transition process," Technologies, vol. 12, p. 241, 2024, doi: 10.3390/technologies12120241.

[**18**] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang, "A survey of post-quantum cryptography: Start of a new race," Cryptography, vol. 7, no. 3, p. 40, 2023, doi: 10.3390/cryptography7030040.

[19] R. Bavdekar, E. J. Chopde, A. Agrawal, A. Bhatia, and K. Tiwari, "Post-quantum cryptography: A review of techniques, challenges and standardizations," in Proc. Int. Conf. Information Networking (ICOIN), Bangkok, Thailand, 2023, pp. 146–151, doi: 10.1109/ICOIN56518.2023.10048976.

[20] H. Dudhat, K. Jodhani, J. Delvadiya, U. Gundaraniya, S. Padhiar, and R. Fachara, "A comparative analysis of symmetric and asymmetric cryptographic algorithms: Performance, security, and versatility," in ICT Systems and Sustainability (ICT4SD 2024), Lect. Notes Netw. Syst., vol. 1160. Singapore: Springer, 2025, doi: 10.1007/978-981-97-8591-9_27.