Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 6, pp. 2455–2467
DOI : 10.47974/JDMSC-2331

A study on quantum computing for IoT security

Pragya Vaishnav [‡]
Department of Computer Applications
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Rajat Goel [†]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Vishal Sharma [§]
Amity Institute of Information Technology
Amity University Rajasthan
Jaipur
Rajasthan
India

Naresh Kedia *
Manisha Choudhary [@]
Department of Business Administration
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

[‡] *E-mail:* pragya.vaishnav@jaipur.manipal.edu
[†] *E-mail:* rajat.goel@jaipur.manipal.edu
[§] *E-mail:* er.vishu1983@gmail.com
* *E-mail:* naresh.kedia@jaipur.manipal.edu (Corresponding Author)
[@] *E-mail:* manisha.choudhary@jaipur.manipal.edu

Abstract

Quantum computing represents the quantum mechanical concept, may have important benefits over the traditional computing. This benefit of quantum computing offers solutions to numerous challenges in secure communication and banking that were previously intractable. The Internet of Things (IoT) is a new technology which works with a large amount of data. Securing IoT data communication is necessary. Cryptographic algorithms like RSA and ECC are the foundation of the IoT security architecture that is now in place. These algorithms' security was significantly impacted by quantum computing. As a result, our research examines the security issues with quantum-based technologies and IoT smart applications. This article offers an overview of the foundations of quantum computing and how it affects the security of IoT devices. This work intends to present a comprehensive view of IoT communication facilitated by quantum technology. In our work, we also analyse the main obstacles to deploying quantum-enabled communication.

Subject Classification: *18M35, 32U35.*

Keywords: *Quantum computing, Quantum key distribution (QKD), Internet of Things (IoT), Quantum entanglement.*

1. Introduction

The use of IoT is growing across a wide range of applications, including smart grids, cities, and intelligent surroundings. The quantity of connected devices in IoT communication gives users the power to make decisions. This broad range of IoT equipped applications [1], as shown in Figure 1, transmit a tremendous quantity of information, that presents problems for security and Confidentiality. IoT applications won't be capable of meet significant requirements without identity and privacy. Additionally, it could pose major security risks to those users. IoT faces difficulties with things like identification, confidentiality, and privacy. Now IoT application scenarios are based on RSA and ECC-based algorithms [2]. Therefore, as quantum computers become more prevalent, such encryption primitives will become insecure. These challenges are solved by quantum computers using conventional cryptography primitives. Quantum computing hence ensures the security of this Internet of Things communication network. The no-cloning theorem [3] and the uncertainty principle [2] are the cornerstones of quantum computing. The primary goal of investigating quantum computing is to develop quantum resistant protocols and algorithms [4] to address IoT security challenges. While a quantum computer uses qubits, a classical computer manipulates individual bits. The quantum state is represented by these qubits and their corresponding probabilities. These qubits are built on principles of

quantum physics including superposition and entanglement. Qubits can be in multiple conceivable set of values at once thanks to superposition. Quantum particles become strongly dependent on one another due to entanglement. But as quantum computing develops, the security of current encryption techniques is seriously threatened. In the area of quantum computing, quantum key distribution (QKD) [5] is an area of intense investigation. It makes it possible for participants to a communication to create secret keys for safe communication. The future world gains a lot from quantum computing, including the development of life-saving drugs, the advancement of artificial intelligence, and the development of intelligent infrastructure [6]. Cyber security methods are under attack as a result of recent advances in quantum computing. Numerous benefits of using quantum computing for safeguarding BB84-based IoT connectivity have already been suggested in the literature [7-8].

According to author, QC analysis is for providing the securing to the IoT communication model while taking into account various attacks on each layer is still not available. In this study author examined IoT layered architecture assaults [9].

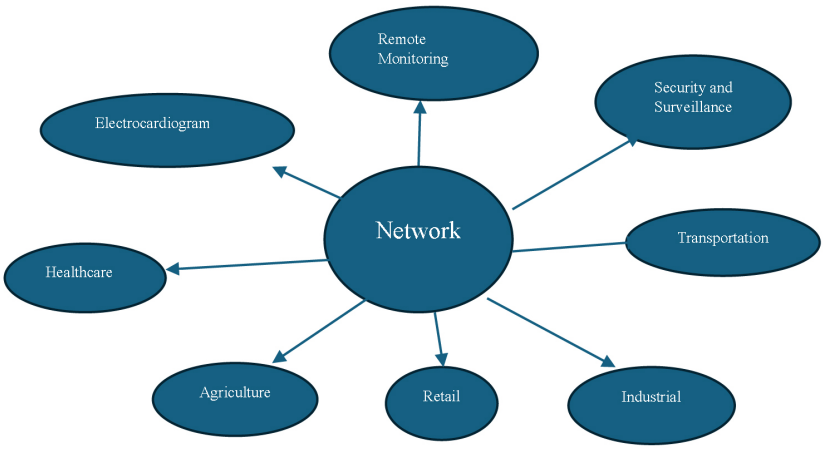

Figure 1

IOT in various Fields

1.1 *Contribution*

The primary contributions of author work are to study regarding the safety and security of IoT smart applications in quantum computing is examined after comprehending the IoT security concerns. The principles

Table 1

Previous works on quantum enabled IoT security

References	Objective	Technology Used	Result Analysis
M.S. Farash [11]	Develop an enhanced user authentication and key agreement system for heterogeneous wireless sensor networks.	BAN-logic and AVISPA tools	Without interacting with a gateway node, the IOT can authenticate with a particular sensor node from the HWSN.
Cheng et al.'s study [12]	To advancements in the field of IoT security using quantum-resistant cryptosystems	Quantum Cryptography	It defended against attacks from quantum and traditional computers alike.
Yen et al. [13]	A novel protocol that can accomplish safe QDC using authentication	QDC protocol	A novel protocol that can accomplish safe QDC using authentication
Rahman et al.'s[14]	Introduce a IoT security infrastructure that is a hybrid one that has an additional layer to guarantee the quantum state.	In the hybrid management, the "One-Time pad (OTP)" classical cryptography technique is employed.	Internet of Things (IoT) security through the integration of classical and quantum communication
Mitchell et al. [30]	It gives a thorough examination of how quantum computing will affect 5G mobile telecommunication security.	5 G system	It improved a security feature that makes the transition to a post-quantum secure system easy and seamless.

of quantum computing are covered, along with their significance for the security framework. Quantum key security provide the security IoT connectivity is thoroughly analysed and addressed. The key categories of quantum authentication techniques and communication for the Internet of Things are examined. The key obstacles for an IoT cryptosystem based on quantum computing are listed [10].

2. Literature Survey

As the number of connected IoT devices increases, ensuring security to build consumer trust will become increasingly challenging. Smartphones and other wearable IoT devices are jam-packed with sensors and integrated software. These devices all interacted with one another over the internet. In the authentication technique proposed in [11], users only receive data after successfully completing the authentication and key agreement steps. Cheng et al.'s study [12] performed their research on the most recent developments in Using quantum cryptography to protect IoT gadgets. The notable developments in "Quantum Recent advances in computing have made it necessary for the creation of a plan to protect communication between "IoT" devices. Author research covers the advantages of quantum encryption over traditional encryption techniques as well as the need for quantum-resistant encryption techniques. Article [13] explore the function of entanglement in mutual authentication. The challenges of data privacy were addressed by EL-Latif et al. in their study. To address present and potential communication frameworks, they suggested the Quantum One-Way Hash Function (QOWHF) [14-20].

As shown in Table 1, the majority of the Studies on using quantum computing to secure IoT-enabled communication have been documented in the study.

3. IOT Security Challenges

IoT-enabled communication has advanced, thanks to creative applications like smart cities, smart agriculture, and creative health care. The Internet of Things devices that facilitate these applications communicate enormous quantities of data in a variety of settings. Cyberattacks are on the rise as IoT applications develop. Additionally, it endangers the confidentiality and privacy of users. Authentication, data integrity, authorization, and trust control are the most security challenges for the IoT ecosystem. Figure 2 illustrates the main security issues with IoT

layered architecture [15]. This section discusses the advantage of implementing the Quantum layer for IoT security as well as risks to the IoT layer architecture.

3.1 *Sensing Layers*

In this layer, several sensor technologies allow IoT applications as WSN, RFID, and GPS. These technologies are all concerned with IoT actuators and sensors. Sensors are used to gather information from the environment, like temperature, ultrasonic, and camera detection [16]. This sensing layer is vulnerable to numerous assaults.

3.2 *Network Layer*

Processing of the data obtained from the bottom layer is required by computational units. The network layer's role is to transmit data obtained from the sensor layer to processing units. IoT applications can only be used if the processed data is available. Network layers, however, are exposed to major security risks because of open internet connectivity, including access control attacks, denial of service attacks, attacks during data transients, etc [17].

3.3 *Quantum Layer*

IoT applications benefit from security provided by the quantum layer. Secure key distribution is a part of it. The confidentiality and security of keys are ensured at this layer by the laws of quantum physics. However, this layer made it possible for quantum-based cryptography, which will be vulnerable to individual, group, and coherent attacks [18].

3.4 *Application layer*

The user's decision-making services must be provided by the application layer. Intelligent surroundings, smart grids, competent health care, and smart cities are the essential IoT applications [19]. IoT heterogeneous applications have significant problems with data protection, confidentiality, and authentication. Attacks on access control, service disruption, malicious code, and eavesdropping are the main problems at the application layer.

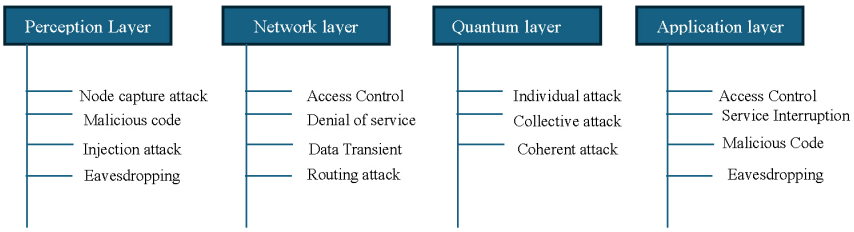

Figure 2

Security risks in the IoT layer architecture

4. Quantum Theory

Figure 3 depicts the fundamental components of quantum computing, which include quantum physical building blocks, quantum logic gates, and a quantum programming environment.

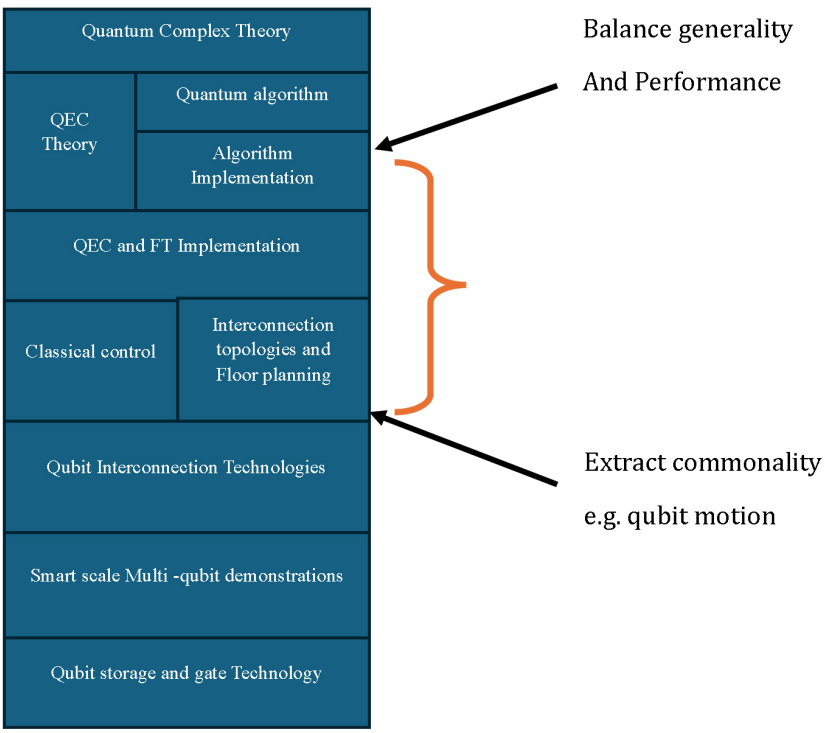

Figure 3

Quantum Computing Architecture

4.1 *From Traditional Bits to Quantum bits*

In traditional computing, bits are used to process data; in quantum computing, quantum bits, or qubits, are implemented. These qubits operate in accordance with quantum mechanical principles. The symbols for quantum particles in the spin up and down states are $|0>$ aaaaa $|1>$. With individual probabilities measuring each value, the set of n qubits can hold up to 2n valid values [20].

4.2 *Quantum superposition*

The qubits are in quantum superposition, which is the linear combination of both $|0>$ and $|1>$. A system is not limited to any one state and can exist in superposition [16] of all potential states at the same time. Measurement, however, causes the superposition to collapse. Qubits are designed to be observed in one of their possible values, $|0>$ oooo $|1>$.

5. Quantum Authentication

The communication is safeguarded through identity authentication, which verifies the authenticity and confidentiality of messages. Two-way authentication between entities guarantees non-repudiation, message integrity, and message validation. Quantum Signature and Entanglement can be employed to establish quantum-based identity authentication.

5.1 *Quantum Engagement*

$$\phi^{\pm} = \frac{1}{\sqrt{2}}(|00> \pm |11>)$$

$$^{\pm} = \frac{1}{\sqrt{2}}(|01> \pm |10>)$$

Quantum entanglement is the surprising aspect of quantum communication. It is necessary to define each particle's state in relation to the other when two particles are entangled. The Bell states are another name for the entangled states [17]. Equations (1) and (2) [21] give the following four mutually orthonormal entangled states:

5.2 *Quantum Signature*

The authenticated user is confirmed using quantum signatures. Quantum signature protocols come in a several of forms, including quantum group signature, quantum blind signature, and arbitrated

quantum signature (AQS) [18]. There has also been talk of a quantum signature based on the quantum walk. Applications that guarantee non-repudiation and protect against user impersonation attacks, like Quantum Cheque [19], can benefit from quantum signatures.

6. Quantum Sensors For IOT

Since it began linking numerous actual objects, sensors, and systems to the Internet a few years ago, the Internet of Things has evolved exponentially. This has created new opportunities for gathering, analyzing, and controlling physical systems data [20]. Nevertheless, the accuracy and precision of these systems are frequently constrained by the functionality of the employed sensors. This is the application of quantum sensors. Quantum sensors can greatly improve the performance of Internet of Things (IoT) systems and develop fresh, creative solutions for a range of applications by utilizing the special qualities of quantum systems [21]. Based on the ideas of quantum mechanics, quantum sensors are able to measure physical quantities with previously unheard-of accuracy and precision. Measurements using quantum systems' special qualities—like superposition and entanglement—are far more sensitive than those using classical sensors. Because of this, quantum sensors are perfect for high-precision measurement applications like environmental monitoring, healthcare, and navigation. Because they make use of qubit superposition and network entanglement manipulation, quantum sensors are distinct from classical sensors [21-24].

Environmental monitoring is one of the most exciting uses of quantum sensors on the Internet of Things. The great accuracy and stability of conventional environmental sensors is limited when it comes to detecting physical quantities like temperature, pressure, and humidity [25-28]. This may lead to inaccuracies in the information gathered and a lack of confidence in the findings. However, even in challenging conditions, quantum sensors are able to measure these quantities precisely. Better environmental monitoring and decision-making can result from this, especially in fields like agriculture, climate change research, and weather forecasting.

Navigation is another area where quantum sensors can have a significant impact. The growing usage of drones, autonomous cars, and other mobile devices need precise navigation systems that can offer real-time information on their orientation, velocity, and location. The precision and dependability of traditional navigation systems, like GPS, are

constrained, especially in urban settings where towering buildings may impede signals. With their ability to measure magnetic fields precisely and accurately, quantum sensors—such as those built on superconducting quantum interference devices—have the potential to completely transform navigation and mapping [23].

7. Difficulties Associated with Quantum based Internet of Things (IOT)

- Quantum Key Distribution": This offers the trustworthy manner to transmit cryptographic keys. That is, if it was possible to identify an unauthorized listener in the "quantum communication" channel. In these cases, the complete process is nullified, and communication won't begin again if in case all information interceptions have not been eliminated from the channel [24].
- "Communication over a limited physical distance": Due to Quantum Key Distribution's (QKD) limited range for short-range communication, mass communication among Internet of Things (IoT) users via the quantum channel is difficult [25, 29-30].
- "Cybersecurity Breach": Quantum-based communication can be the target of specific attacks. In this case, the attacker implements a new "quantum channel" by intercepting a "quantum signal" that is being transferred between Alice and Bob [25].
- "Quantum Reversible Computing": The existence of Eve poses a serious threat to quantum-based reversible computation [26].

8. Conclusion

IoT involves the connection of various heterogeneous devices since all connected devices provide consumers numerous advantages to help with making choice. This type of technology must be safe since it holds the vital information we need on a daily basis for applications in the military, intelligent cities, and even healthcare. Numerous traditional cryptographic primitives offer secure communication based on intricate mathematical concepts. Due to assaults using quantum computing, the security based on traditional cryptographic frameworks is not secure anymore. Therefore, quantum-based security is needed for IoT-enabled communication in order to fend off future quantum threats. We investigated quantum-based cryptographically secured IoT communication topologies in our survey.

This article offers a comprehensive overview of security threats to IoT-based applications, quantum-resistant IoT communication security solutions, quantum authentication techniques, Quantum Sensors For IO, QKD, and Difficulties Associated with Quantum based Internet of Things.

References

[1] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Secur. Commun. Networks*, vol. 2017 (2017). doi: 10.1155/2017/6562953.

[2] A. Lohachab, "Using quantum key distribution and ECC for secure inter-device authentication and communication in IoT infrastructure," *SSRN Electron. J.* (2018). doi: 10.2139/ssrn.3166511.

[3] S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, and R. Buyya, "Quantum computing: A taxonomy, systematic review and future directions," *Softw. Pract. Exp.*, vol. 52, pp. 66–114 (2022). doi: 10.1002/spe.3039.

[4] V. Hassija, V. Chamola, A. Goyal, S. S. Kanhere, and N. Guizani, "Forthcoming applications of quantum computing: Peeking into the future," *IET Quantum Commun.*, vol. 1, pp. 35–41 (2020). doi: 10.1049/iet-qtc.2020.0026.

[5] A. Kumar, P. Dadheech, V. Singh, L. Raja, and R. C. Poonia, "An enhanced quantum key distribution protocol for security authentication," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 22, no. 4, pp. 499–507 (2019).

[6] J. Ahmed, A. K. Garg, M. Singh, S. Bansal, and M. Amir, "Quantum cryptography implementation in wireless networks," *Int. J. Wirel. Netw. Syst.*, vol. 3, pp. 129–133 (2014).

[7] S. T. Cheng, C. Y. Wang, and M. H. Tao, "Quantum communication for wireless wide-area networks," *IEEE J. Sel. Areas Commun.*, vol. 23, pp. 1424–1432 (2005). doi: 10.1109/JSAC.2005.851157.

[8] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Des. Codes Cryptogr.*, vol. 78, pp. 351–382, 2016. doi: 10.1007/s10623-015-0157-4.

[9] S. R. Moulick and P. K. Panigrahi, "Quantum cheques," *Quantum Inf. Process.*, vol. 15, pp. 2475–2486 (2016). doi: 10.1007/s11128-016-1273-4.

[10] A. Kumar, M. Kumar, S. K. Dhiman, and S. K. Ray, "An improved quantum key distribution protocol for verification," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 491–498 (2019).

[11] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176 (2016). doi: 10.1016/j.adhoc.2015.05.014.

[12] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, pp. 116–120 (2017). doi: 10.1109/MCOM.2017.1600522CM.

[13] C. A. Yen, S. J. Horng, H. S. Goan, T. W. Kao, and Y. H. Chou, "Quantum direct communication with mutual authentication," *Quantum Inf. Comput.*, vol. 9, pp. 376–394 (2009). doi: 10.26421/QIC9.5-6-2.

[14] M. S. Rahman and M. Hossam-E-Haider, "Quantum IoT: A quantum approach in IoT security maintenance," *in Proc. 1st Int. Conf. Robot. Electr. Signal Process*. Tech. ICREST, pp. 269–272 (2019). doi: 10.1109/ICREST.2019.8644342.

[15] D. J. Egger, C. Gambella, J. Marecek, S. McFaddin, M. Mevissen, R. Raymond, A. Simonetto, S. Woerner, and E. Yndurain, "Quantum computing for finance: State-of-the-art and future prospects," *IEEE Trans. Quantum Eng.*, vol. 1, pp. 1–24 (2021). doi: 10.1109/TQE.2020.3030314.

[16] N. Papanikolaou, "An introduction to quantum cryptography," *XRDS Crossroads ACM Mag*. Students, vol. 11, no. 3, pp. 3–3 (2005). doi: 10.1145/1144396.1144399.

[17] M. S. Kang, C. H. Hong, J. Heo, J. I. Lim, and H. J. Yang, "Controlled mutual quantum entity authentication using entanglement swapping," *Chin. Phys. B*, vol. 24, no. 9 (2015). doi: 10.1088/1674-1056/24/9/090306.

[18] L. Jian, L. Na, Z. Yu, W. Shuang, D. Wei, C. Wei, and M. Wenping, "A survey on quantum cryptography," *Chin. J. Electron.*, vol. 27, pp. 223–228 (2018). doi: 10.1049/cje.2018.01.017.

[19] B. K. Behera, A. Banerjee, and P. K. Panigrahi, "Experimental realization of quantum cheque using a five-qubit quantum computer," *Quantum Inf. Process.*, vol. 16, pp. 1–12 (2017). doi: 10.1007/s11128-017-1762-0.

[20] V. Teja, P. Banerjee, N. N. Sharma, and R. K. Mittal, "Quantum cryptography: State-of-art, challenges and future perspectives," *in Proc. 7th IEEE Int. Conf. Nanotechnol. IEEE-NANO* 2007, pp. 1296–1301 (2007). doi: 10.1109/NANO.2007.4601420.

[21] A. I. Nurhadi and N. R. Syambas, "Quantum key distribution (QKD) protocols: A survey," *in Proc. 4th Int. Conf. Wirel. Telemat. ICWT 2018*, pp. 1–5 (2018). doi: 10.1109/ICWT.2018.8527822.

[22] R. Niederhagen, S. Css, P. Michael, W. Fraunhofer, D. Fraunhofer, and S. Information, "*Practical post-quantum cryptography*," White Paper (2018).

[23] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, "Quantum cryptography for IoT: A perspective," *in Proc. IEEE Int. Conf. IoT Its Appl. ICIOT 2017* (2017). doi: 10.1109/ICIOTA.2017.8073638.

[24] A. G. Aruna, K. H. Vani, C. Sathya, and R. S. Meena, "A study on reversible logic gates of quantum computing," *Int. J. Comput. Appl.*, vol. 7, pp. 427–432 (2016).

[25] M. Peelam, M. S. Shall, A. A. Rout, and V. Chamola, "Quantum computing applications for Internet of Things," *IET Quantum Commun.*, vol. 5, no. 2, pp. 103–112 (2024).

[26] K. Diddi, S. Upadhyay, and K. Dcruz, "A survey on 'quantum computing' applications to bolster security in the Internet of Things (IoT)," *Int. J. Sci. Technol. Res.* (2023).

[27] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176 (2016). doi: 10.1016/j.adhoc.2015.05.014.

[28] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, pp. 116–120 (2017). doi: 10.1109/MCOM.2017.1600522CM.

[29] A. B. Dorothy and S. B. R. Kumar, "An approach for IoT security using quantum key distribution," *Int. J. Sci. Technol. Res.*, vol. 8, pp. 1569–1574 (2019).

[30] A. Kumar, M. Kumar, S. K. Dhiman, and S. K. Ray, "An enhanced quantum key distribution protocol for security authentication," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 4, pp. 499–507 (2019).

Received March, 2024