The Vital Role of Quantum Cryptography in IoT Network Security

Allanki Sanyasi Rao[1], Dr. Sreeja Mole S S[2]

(Dept. of Electronics & Communication Engineering,

Christu Jyothi Institute of Technology & Science, Jangaon-506167, Telangana)

srao_allanki@cjits.org[1], sreeja@cjits.org[2]

ABSTRACT

The Internet of Things (IoT) is a cutting-edge technology that continues to evolve. The IoT is an integral part of our lives today. It serves as a direct service provider in our surroundings through connected sensor-based networks. It also offers us various value-added services over cellular platforms, both directly and indirectly. Despite all these advantages, there is a demanding need for enhanced security to counter existing security threats including data breaches, virus propagation, side-channel attacks, and authentication issues, are associated with IoT. Consequently, it is imperative to employ methods that bolster IoT security and safeguard our sensitive data. Emphasizing the need for stronger security, this paper highlights the transition to Quantum Cryptography (QC) to protect IoT devices amid their expanding commercial use. The Quantum Bit Error Rate (QBER) is also proposed as a key solution, employing error-correcting servers for secure quantum communication.

Keywords: IoT, Quantum Cryptography, Quantum Bit Rate, Quantum Communication,

DOI: 10.31838/ecb/2023.12.9.164

1. INTRODUCTION

The IoT is an emerging paradigm enabling communication between electronic devices and sensors via the internet, enhancing various aspects of our lives [1]. Through connected devices, IoT is essential in enhancing people's lives and connecting the physical and digital worlds [2]. Due to the widespread adoption of Internet, Wi-Fi, and Bluetooth technologies, the field of computer security is gaining increasing importance. Various forms of misuse, such as hacking, phishing, the dissemination of computer viruses, worms, or Trojans, can occur within a computer network. As technology advances, an emerging field called the (IoT) is developing, which involves greater automation of processes and increased availability of user data on the Internet, thus heightening the need for security in contemporary times.

The convergence of multiple technologies, including machine learning, advanced sensors, wireless sensor networks, management systems, and various forms of automation, all contributes to enabling IoT. IoT extends internet connectivity beyond conventional devices, encompassing a wide range of traditionally non-internet-enabled physical devices and everyday objects. IoT facilitates the transfer of information among various devices within a network, thus presenting a high likelihood of exposing this information to potential attacks and hacking [3]. In light of the vastness of the internet, data and information are exposed to security threats and cyber-attacks, compelling IoT to address these concerns with effective solutions. Ensuring security is the utmost priority for IoT in trade and economy, prompting intensive efforts from developers to establish a secure collaboration between social networks and privacy concerns [1]. In the realm of network security, attackers and eavesdroppers attempt to disrupt, alter, steal, monitor, or gain unauthorized access to sensitive information, which poses a significant challenge in the context of IoT. To address this challenge, numerous security algorithms and diverse methods for generating encryption keys are employed to secure the transmission and decryption of information among the involved parties.

This paper introduces a novel approach to quantum computing, involving the transmission of data via photons through a fiber-optic channel. Notably, this method possesses the characteristic of non-cloning, as it is impossible to replicate the state of a photon [4]. Moreover, in the presence of an eavesdropper attempting to access the information, the photon undergoes immediate alteration [5]. This research employs quantum key distribution (QKD) to generate a private key, a technique commonly referred to as the BB84 protocol. The BB84 protocol generates a series of qubits with randomized lengths, as dictated by the encryption algorithm outlined in this paper. Furthermore, the paper utilizes the QBER method to rectify errors. QBER involves error correction by comparing the number of incorrect values with the entire list of values and subsequently retransmitting the information after error removal in the context of QKD [6].

2. IoT SYSTEMS AND THEIR SECURITY CONCERNS

The number of IoT devices has significantly expanded as a result of the growing reliance on the Internet and the associated rise in connectivity demand [7]. Fig. 1 shows the four layer architecture of IoT. In an IoT system, the initial layer involves "things" or endpoint devices that bridge the physical and digital realms. The term "perception" refers to this physical layer, which includes sensors and actuators capable of collecting, receiving, and processing data through the network. These sensors and actuators can establish connections, either wirelessly or through wired interfaces, and the architecture does not impose limitations on the components' scope or placement.

The network layer provides an understanding of how data flows within the application. It encompasses Data Acquiring Systems (DAS) and Internet/Network gateways. DAS plays a crucial role in aggregating and converting data, collecting information from sensors, and converting analog data into digital format. Its primary function is to transmit and process data collected by sensor devices. This layer facilitates connections and communication among devices, servers, smart devices, and network equipment while managing all data transmissions.

The processing layer serves as the central intelligence of the IoT ecosystem. Here, data undergoes analysis, preprocessing, and storage before being sent to the data center for accessibility by software applications. These applications monitor, manage data, and initiate subsequent actions. The processing layer also incorporates Edge IT and edge analytics into the IoT framework.

The application layer serves as the user interface for interacting with the IoT system. It offers application-specific services, such as controlling devices through a mobile app or monitoring device status through a dashboard. The IoT finds diverse applications in areas such as smart cities, smart homes, and smart health, showcasing its versatility across various domains.

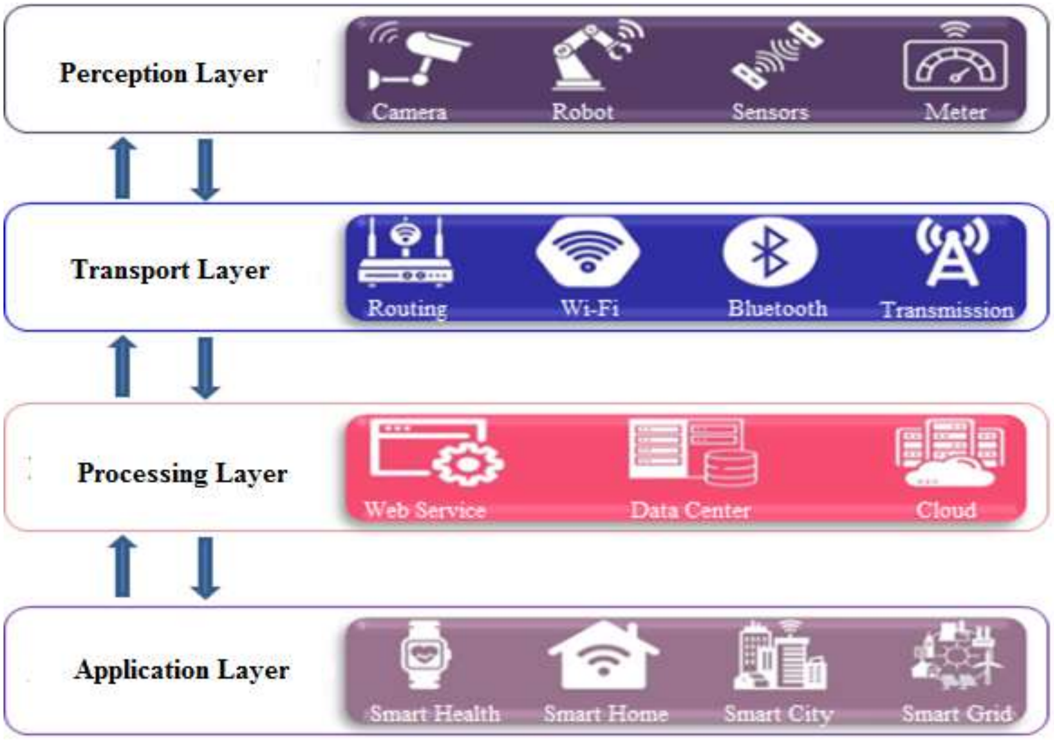

Fig. 1: IoT Architecture Layers

Researchers identified some of the major security issues that needed to be addressed in IoT infrastructure. Following are common vulnerabilities:

Data Breaches: The volume of data flowing between IoT devices and servers is substantial compared to traditional client-server architectures. Much of this data contains sensitive or personal information, as it constitutes a primary asset of IoT devices. Prior to transmitting this data over the internet, robust data encryption and protection measures are essential. However, it's important to note that merely storing data on these devices doesn't ensure security. Storing data on IoT devices presents an extra challenge, especially given that an IoT network can involve numerous devices, making them vulnerable to unauthorized access by third parties.

Irregular Updates: Amidst the tumultuous evolution of the IoT sector, there exists no assurance that every device comprising an IoT network is diligently fortified and subject to regular updates. With the envisioned interconnectivity of billions of IoT devices in the foreseeable future, a surging trajectory [Fig. 2] foretells a momentous proliferation. In this new era, modern IoT devices must exhibit the innate capability to securely receive forthcoming updates. The converse eventuality portends a disconcerting scenario wherein devices may no longer be considered secure after the passage of a mere few years, should the mantle of regular updates not be borne.

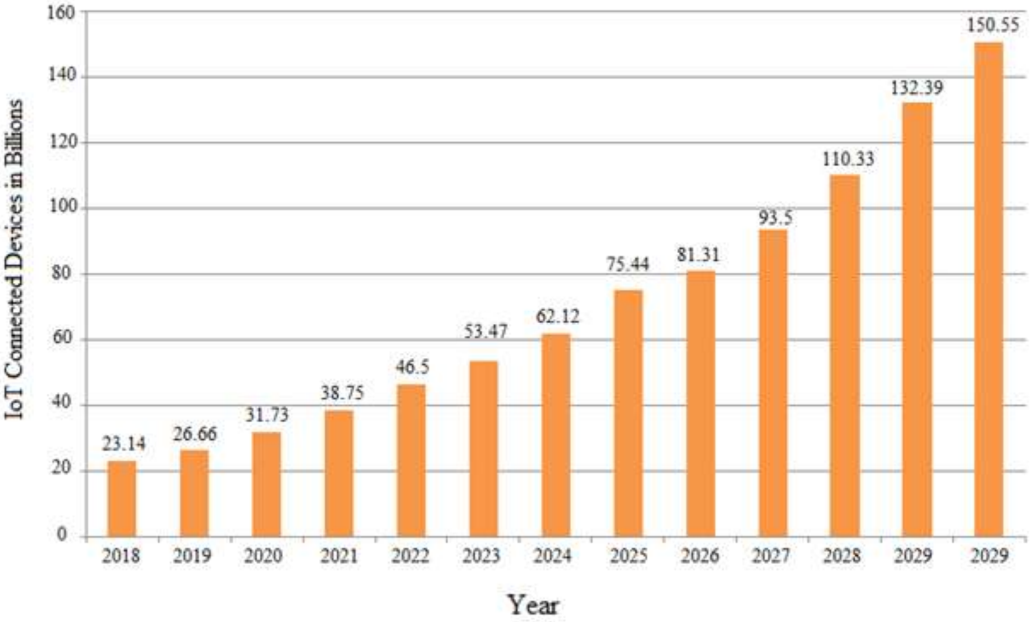

Fig. 2: The global utilization of IoT devices from 2019 to 2030

Data Authentication: Notwithstanding the implementation of robust encryption, IoT devices remain susceptible to the predations of malevolent hackers in the absence of rigorous authentication protocols governing their communicative endeavors. Hence, there is an imperative need for enhanced authentication methodologies within IoT-based ecosystems, endowed with the capacity to mutually validate the legitimacy of users and IoT devices before forging the auspicious imprimatur of secure communication sessions [8].

Side-Channel Attacks: These types of attacks concentrate on extracting data and information not by exploiting vulnerabilities in the algorithms used in system implementations, but by examining characteristics inherent to the system itself. Features such as electromagnetic fields, auditory cues, and power consumption are some of the elements leveraged to manipulate the system. For instance, Electro-Magnetic (EM) side-channel attacks utilize unintentional electromagnetic emissions to scrutinize the data emanating from IoT devices [9]. These attacks are particularly challenging to detect because they operate covertly, surreptitiously siphoning data without raising any noticeable alarms.

Malware and Ransomware: These insidious programs infiltrate devices, promoting their spread and disruption. Ransomware encrypts data within IoT devices, compelling users to pay a ransom for data decryption. These attacks are increasingly severe, potentially targeting critical infrastructure like power plants or water treatment facilities. In the face of growing contemporary threats, the emergence of cryptographic malware, such as Ransomware [10], poses a significant danger. The potency of these new threats significantly increases the risk of IoT devices falling victim to cyber-attacks or becoming entangled in cryptographic traps.

2.1 Conventional Security Techniques

Hashed Passwords: Hashing, a widely-used security technique, produces a consistent bit string from an input string. However, hashing functions are susceptible to cracking through methods like rainbow tables, which contain hash keys for common password strings. To thwart reverse look-ups, a random string called a "salt" is appended to each hash key, rendering rainbow table generation expensive and time-consuming.

Private Key Authentication: Private key authentication employs asymmetric encryption, providing both public and private keys for secure communication between endpoints. Data encrypted with the private key can only be decrypted with the public key, enhancing communication security, including interactions between IoT devices. Nevertheless, the advent of increasingly powerful computing and the potential impact of quantum computing pose new challenges to the security of current IoT systems.

Signed Firmware: Signed firmware involves embedding a secret digital signature into production deployments, preventing unauthorized access and thwarting the substitution of malicious programs with authenticated signatures. This fortifies the integrity of the firmware and safeguards against replication of authenticated signatures by hackers.

The techniques mentioned face significant challenges in real-life systems due to resource limitations. Constrained processing power and memory capacity present formidable obstacles for developers. While these techniques may be theoretically sound, real-world instances continue to reveal security breaches in IoT systems. Notable examples of malicious attacks include:

- The Mirai botnet or Dyn attack [7].
- Vulnerabilities in cardiac monitoring devices from St. Jude.
- Security weaknesses in the owlet Wi-Fi baby monitor.
- The TRENDnet webcam hack.
- The Stuxnet malware.

These instances underscore the persistent need for more robust cryptographic and security algorithms to effectively mitigate the aforementioned threats.

3. QUANTUM CRYPTOGRAPHY

Cryptography, the art of secure communication, serves as a means to establish covert communication channels between two trusted entities, even in the face of relentless attempts by third parties to intercept the information. QC, which emerged in the 20th century, is firmly grounded in the principles of quantum mechanics, specifically drawing from the Heisenberg Uncertainty Principle and the concept of photon polarization.

The Heisenberg Uncertainty Principle, a cornerstone of quantum mechanics, postulates that it is inherently challenging to measure the quantum state of any system without perturbing it. In practical terms, this means that the polarization state of light or a photon particle can only be accurately gauged at the moment of measurement. This property becomes crucial in thwarting the efforts of potential eavesdroppers in a cryptosystem based on QC. Conversely, the principle of photon polarization elucidates how photons of light can be polarized or oriented along specific axes. Notably, a photon filter calibrated to the precise polarization can exclusively detect a photon with that matching polarization; otherwise, the photon is obliterated. This characteristic, when combined with the perpetual stream of photons and the Heisenberg Uncertainty Principle, renders QC an exceptionally appealing choice for safeguarding data privacy and outsmarting eavesdropping adversaries.

The concept of QC was introduced in 1984 by Charles H. Bennett and Gilles Brassard as part of a groundbreaking study at the intersection of physics and information theory. QC operates uniquely, as it doesn't transmit any conventional message signals; its sole purpose is to generate and distribute cryptographic keys. These cryptographic keys are generated based on the quantity of photons reaching a recipient and the manner in which they are received. The polarization of these photons can be adjusted to various orientations, and these orientations can then represent binary bits, with ones and zeros.

To initiate the process, a user can propose a cryptographic key by sending a sequence of photons with random polarizations. This method of encoding bits through polarized photons forms the bedrock of QC and is referred to as Quantum Key Distribution (QKD). One remarkable aspect of QC is its inherent security feature. In the event that the cryptographic key is intercepted, it can be easily detected without any adverse consequences since it consists of a set of random bits that can simply be discarded. Subsequently, the sender can transmit a fresh key. Once a secure key is successfully received, it can be utilized to encrypt a message, which can then be transmitted through conventional communication channels like telephones or emails.

In QC, the fundamental unit of quantum information is known as a 'qubit.' In this context, photons are characterized by their plane of polarization, which can range from 0° to 180°. QC leverages the unique property that when a diagonally polarized photon passes through a linear polarizer, it randomly 'chooses' either a horizontal or vertical state of polarization with a probability of 0.5. This method of representing bits through polarized photons is the cornerstone of QC, often referred to as Quantum Key Distribution (QKD).

3.1 Quantum Key Distribution

In Quantum Key Distribution (QKD), the encryption key is conveyed through a quantum channel to the intended recipients. This process employs two distinct types of channels:

- The Quantum channel is responsible for transmitting the confidential key.
- The Public channel, often featuring Alice as the transmitter and Bob as the receiver serves as a means for the end users to check for any potential alterations in the transmitted key, which might indicate eavesdropping (the presence of EVE).

The polarization state of individual photons is utilized to represent the binary bits. A concise overview of the steps involved in establishing a secure key is illustrated in Fig. 3. QKD is a highly intricate mechanism, with numerous protocols having been developed over time. Some of these protocols involve the detection of the polarization state of individual photons, while others leverage entangled photons to establish secure key communication. Among these protocols, the most widely adopted one is the BB84 protocol, whose steps are explained and demonstrated in Fig. 4 (a protocol suitable for enhancing IoT security).

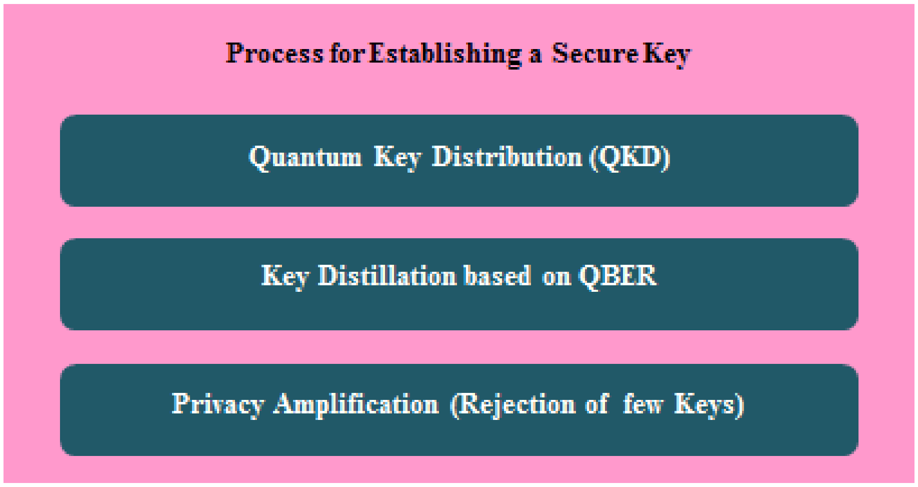
Process for Establishing a Secure Key
Quantum Key Distribution (QKD)
Key Distillation based on QBER
Privacy Amplification (Rejection of few Keys)

Fig. 3: Process for Establishing a Secure Key in QKD

Alice transmits a series of pulses, such as femtosecond pulses with an 80 MHz repetition rate, where each pulse ideally contains a single photon with a distinct polarization. She represents zeros by encoding them into H-polarized (Horizontally) photons and ones by encoding them into V-polarized (Vertically) photons, as indicated by the red arrows in the Fig. 5. However, this encoding scheme is only applicable in half of the cases. The remaining half of the bits, chosen randomly, is encoded using a diagonal polarization basis, as indicated by the blue arrows in the Fig. 5. In this case, 'D' polarization corresponds to zero, and 'A' polarization corresponds to one.

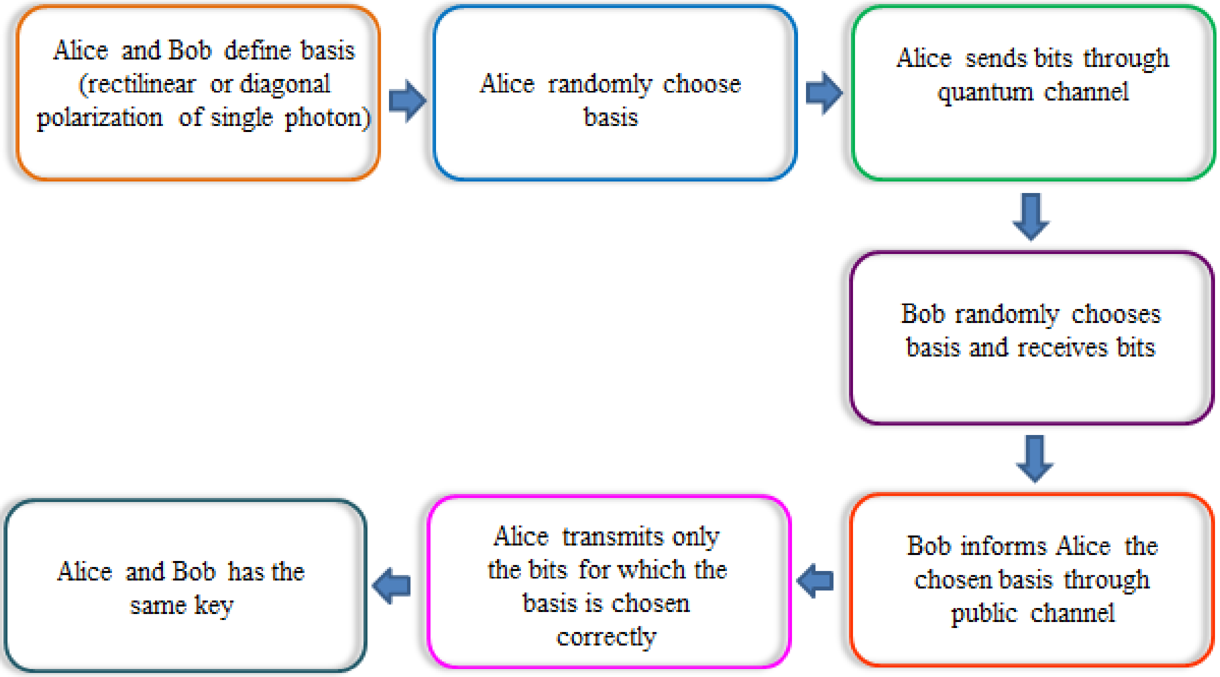
Alice and Bob define basis (rectilinear or diagonal polarization of single photon)
Alice randomly choose basis
Alice sends bits through quantum channel
Bob randomly chooses basis and receives bits
Bob informs Alice the chosen basis through public channel
Alice transmits only the bits for which the basis is chosen correctly
Alice and Bob has the same key

Fig. 4: Steps involved in the QKD process using the BB84 protocol.

The recipient, Bob, employs a standard setup (either a PBS or a Glan prism with two single-photon detectors in the output ports, or a calcite crystal followed by two detectors) to measure the polarization. This allows Bob to differentiate between H and V polarizations when he uses the HV basis (referred to as '+'). However, in half of the cases, Bob randomly switches his basis (the orientation of his prism) to AD (referred to as 'X').

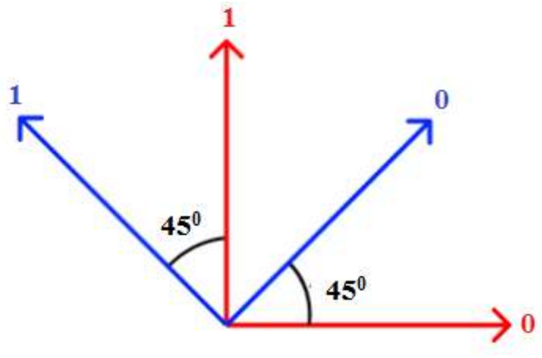

Fig. 5: Illustration of Photon Polarization in the BB84 Protocol

Once a certain number of bits have been transmitted and all photons have been detected and eliminated, Bob publicly announces which basis he used for each bit. Alice then identifies the cases where they both used the same bases, discarding bits where they used different bases. This process, known as key sifting, reduces the length of the key by half, but what remains is both random and identical for Alice and Bob. Subsequently, they perform a check for eavesdropping. To do this, they take a portion of the key, for example, 10%, and compare it. This procedure is also made public, but the 10% is subsequently discarded. If eavesdropping has occurred, the key would contain errors. When Eve measures a photon, its state changes to align with the basis Eve used. As a result, Bob may receive an incorrect outcome in some matching bases with a 50% chance, introducing a 25% error [11-12]. In such a case, the entire key is discarded, and the process is repeated.

Table 1 illustrates the transmission of an 8-bit secret key. After the key sifting process, only 4 bits are retained.

Table 1: Example of BB84 Protocol with 8 bits

Alice’s random bit	0	1	1	0	1	0	0	1
Alice’s random sending basis	X	+	+	+	X	+	X	X
Photon polarization Alice sends	D	V	V	H	A	H	D	A
Bob’s random measuring basis	X	X	+	X	+	+	+	X
Photon polarization Bob measures	D	D	V	A	V	H	V	A
Shared secret Key	0		1			0		1

3.2 Device - Independent Quantum Cryptography

In typical communication networks, direct communication between computers is rare, necessitating the use of intermediate devices to relay messages. However, trusting these third-party devices can be risky due to vulnerabilities to tampering and concerns about side-channel attacks [13]. Device-independent QC enhances user protection by relying on device performance statistics, eliminating the need for detailed scrutiny of their internal workings. This strategy effectively shields users from insecure connections, interference, and system degradation. The concept of device-independent QC has garnered significant interest, leading to the proposal of numerous system-independent approaches by researchers. Device-independent quantum key distribution (DIKQD) protocols enable the establishment of secret keys between two parties within a secure channel while concealing the intricate workings of the quantum devices employed. In DIQKD, these quantum devices operate as "black boxes," generating classical outputs influenced by specific classical inputs. A helpful contrast can be drawn by comparing DIQKD to the conventional approach of quantum key distribution (QKD), specifically the wrapping-based version [14] of QKD.

3.3 Shor's Algorithm

It is a groundbreaking quantum algorithm developed by mathematician Peter Shor in 1994. It is particularly significant in the field of QC because it has the potential to break widely used public-key encryption schemes, such as RSA, which rely on the difficulty of factoring large numbers into their prime factors. Unlike classical computers, which rely on sequential processes, quantum computers can perform certain calculations exponentially faster due to their ability to process multiple possibilities simultaneously. Shor's algorithm leverages this quantum parallelism to efficiently factor large integers. Factoring large numbers into their prime components is a problem considered to be "hard" for classical computers, as the time required grows exponentially with the size of the number. In contrast, Shor's algorithm can factor large numbers in polynomial time, making it a significant threat to classical encryption methods. This algorithm's potential to break widely used encryption schemes highlights the need for quantum-resistant cryptographic techniques to secure data against quantum attacks. Researchers in QC are actively developing post-quantum cryptography methods that are resistant to attacks by quantum computers like Shor's algorithm, ensuring the continued security of digital communications in the quantum era.

Equation (1) outlines the time complexity associated with classical algorithms, while equation (2) delineates the time complexity attributed to quantum algorithms when it comes to factoring ft.

$$ft = O\left((\log N)^k\right) \tag{1}$$

$$ft = O(\log N) \tag{2}$$

Given the significant disparity in runtime between classical and quantum computers, we can describe the runtime for classical computers as denoted by equation (3), while equation (4) characterizes the runtime for quantum computers. In these equations, *L* represents length, and *N* signifies the number of bits involved [15].

$$rt = O\left(\exp\left(L^{1/3} (\log L)^{2/3}\right)\right) \tag{3}$$

$$rt = O\left((L)^3\right) \tag{4}$$

Shor's algorithm relies on three key components i.e., modular arithmetic, the quantum Fourier transform, and quantum parallelism.

3.4 Quantum Bit Error Rate for Error Estimation

Quantum cryptography (QKD) plays a crucial role in securing long-distance data transmission, yet it remains susceptible to errors arising from noise or malicious activities. To assess the integrity of the transmitted data, Quantum Bit Error Rate (QBER) is calculated, which represents the percentage of errors in the key during transmission. The accuracy of QBER significantly impacts the efficiency of the information transformation system [16, 17]. In the case of properly designed QC protocols like BB84, it becomes feasible to detect the presence of eavesdroppers. Higher error rates may signal increased eavesdropping attempts [18–20]. Post QBER calculation, it is compared against a predefined threshold agreed upon by the communicating parties. If the QBER falls below 11%, it indicates that no eavesdropper has compromised the key's security [23].

$$QBER = n_{wrong} / \left(L_s + n_{wrong}\right) \qquad (4)$$

where L_s denotes the count of correctly detected bits, while n_{wrong} signifies the count of erroneously detected bits within the received series

4. IoT SECURITY WITH QUANTUM CRYPTOGRAPHY

IoT devices exhibit significant security vulnerabilities, impacting the security of the devices themselves, user data, and the overall network. The classical architecture of IoT lacks mechanisms to detect eavesdroppers within communication channels [21]. Moreover, vulnerabilities can manifest in the form of attacks, where a single compromised device in the IoT network can infect others, leading to ongoing communication until detection. Unfortunately, these breaches may go unnoticed for an extended period, allowing a substantial amount of data to be transmitted to malicious entities [22]. Certain viruses can even render systems inoperable, requiring a system reboot, which is often infrequent in industrial and enterprise settings. Consequently, IoT systems present multiple points of vulnerability and are highly susceptible to attacks, necessitating a search for solutions, including the exploration of QC [23].

QC introduces a fundamental aspect known as Quantum Key Distribution (QKD), as previously discussed [24]. Notably, one of QKD's standout features is its ability to detect the presence of eavesdroppers within the system's architecture, a sharp contrast to conventional cryptographic algorithms. However, challenges arise in the physical implementation of quantum cryptographic protocols, such as BB84, primarily related to the maximum distance that photons, essentially light particles, can travel without distortion due to environmental factors or natural calamities. This limitation becomes particularly problematic in IoT networks spanning multiple cities or countries. Additionally, quantum devices tend to be large, bulky, and expensive, making them inaccessible for many organizations. Moreover, the existing quantum key distribution protocol is designed to work with only two devices, which is impractical for actual IoT systems connecting hundreds of devices for communication [25].

To address these challenges, a potential solution combines classical and quantum approaches. This proposal maintains current semiconductor chips but leverages quantum techniques to create long, unique cryptographic keys for each device. Quantum Random Number Generation (QRNG) is utilized to generate noise sources with high levels of randomness efficiently and rapidly. Consequently, guessing the key becomes extremely difficult, as each device possesses a unique key. Unauthorized access to the physical device configuration, without detection, is an arduous task, ensuring the security of the key and the safety of communications [26]. Furthermore, device-independent QC can be employed to verify the trustworthiness of manufactured devices, bolstering overall IoT security.

5. CHALLENGES IN USING QUANTUM CRYPTOGRAPHY FOR IoT

The implementation of QC for the IoT presents several challenges that need to be addressed:

Distance Limitations: One of the primary challenges is the limited distance over which quantum signals can be transmitted without significant loss. Due to the properties of quantum mechanics, the transmission distance for QC is limited to approximately 200 kilometers [27]. Quantum signals, typically carried by photons, can become attenuated or distorted over long distances. This limitation can be a hindrance in large-scale IoT networks that span extensive geographical areas.

Cost and Complexity: QC relies on a number of components such as single photon detectors, laser systems, and multiplexers that are very expensive. and complex to deploy. This cost factor can be a significant barrier to entry for many IoT applications, particularly those with budget constraints.

Scalability: Many existing quantum cryptographic protocols are designed for point-to-point communication between two devices. Scaling these protocols to accommodate the numerous interconnected devices in IoT networks can be challenging. Ensuring that each device can securely communicate with multiple other devices is a complex task.

Integration: Integrating QC into existing IoT infrastructure and protocols can be challenging and it requires a significant amount of time and effort. IoT devices often rely on traditional cryptographic methods, and transitioning to QC requires careful planning and adaptation.

Environmental Factors: Quantum signals are sensitive to environmental conditions, such as temperature and electromagnetic interference. These factors can introduce noise and errors into the quantum communication channel, affecting the reliability of the security measures.

Key Distribution: Quantum key distribution (QKD) relies on the secure exchange of quantum keys between communicating parties. Ensuring the efficient distribution of these keys across a vast IoT network is a logistical challenge.

Quantum-Resistant Attacks: While QC is designed to be secure against quantum attacks, it must also be resistant to potential future attacks by quantum computers. Ensuring long-term security in the face of evolving technology is a concern.

Standardization: The field of QC is still evolving, and there is a lack of standardized protocols and best practices. Developing widely accepted standards for QC in IoT is essential for its widespread adoption.

Interoperability: Ensuring that different IoT devices and platforms can effectively communicate using QC is crucial. Achieving interoperability between various vendors and protocols is a significant challenge.

Education and Expertise: QC requires a high level of expertise in quantum physics and cryptography. Training professionals and IoT developers in these specialized fields is essential for successful implementation.

6. CONCLUSION

In conclusion, QC stands as a beacon of hope for fortifying the security of IoT systems. Its distinctive characteristics, including unassailable security, suitability for distributed IoT environments, and resilience against quantum computing threats, position it as the ideal solution for securing the future of IoT. QC not only guarantees unparalleled confidentiality but also enhances data integrity, addressing critical aspects of IoT security. By adopting this groundbreaking technology, IoT systems can safeguard their networks against evolving threats and ensure the privacy and reliability of data transmission. As IoT continues to expand and become increasingly integral to our daily lives, QC emerges as a vital and future-proof security measure, setting the standard for safeguarding the interconnected world of tomorrow.

REFERENCES

[1] Allanki Sanyasi Rao et al. Navigating the Internet of Things (IoT): Towards a Smart and Sustainable Future - Opportunities, Issues and Challenges in International Journal of Early Childhood Special Education (INT-JECSE), ISSN: 1308-5581, Vol 15, Issue 04, July 2023, Page 20-31, DOI:10.48047/INTJECSE/V15I4.4

[2] Dr. Nookala Venu, Dr.A Arun Kumar, Mr. A.Sanyasi Rao. Internet of Things based Pulse Oximeter for Health Monitoring System in Neuroquantology, May 2022, Volume 20, Issue 5, Page 5056-5066, DOI: 10.14704/NQ.2022.20.5.NQ22781

[3] Anca D. Jurcut, Tom Coffey, and Reiner Dojen. Design requirements to counter parallel session attacks in security protocols. In 2014 12th Annual Conference on Privacy, Security and Trust, PST 2014, number April 2018, pages 298–305, 2014.

[4] Heng Fan, Yi Nan Wang, Li Jing, Jie Dong Yue, Han Duo Shi, Yong Liang Zhang, and Liang Zhu Mu. Quantum cloning machines and the applications, 2014.

[5] Miloslav Dušek, Norbert Lütkenhaus, and Martin Hendrych. Quantum cryptography. In Progress in Optics, volume 49, pages 381–454. 2006.

[6] Sreraman Muralidharan, Linshu Li, Jungsang Kim, Norbert Lütkenhaus, Mikhail D. Lukin, and Liang Jiang. Optimal architectures for long distance quantum communication. Scientific Reports, 6(November 2015):1–10, 2016.

[7] Dr. Nookala Venu, Dr.A Arun Kumar, Mr. A.Sanyasi Rao. Botnet Attacks Detection in Internet of Things using Machine Learning in Neuroquantology, April 2022, Volume 20, Issue 4, Page 743-754, DOI: 10.14704/NQ.2022.20.4.NQ22298

[8] Mohammad Wazid, Ashok Kumar Das, Rasheed Hussain, Giancarlo Succi, and Joel J.P.C. Rodrigues. Authentication in cloud-driven IoT-based big data environment: Survey and outlook". In: Journal of Systems Architecture 97 (2019), pp. 185–196. ISSN: 1383-7621. DOI: https://doi.org/10.1016/j . sysarc .2018.12.005.

[9] Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. "A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics". In: Digital Investigation 29 (2019), pp. 43–54. ISSN: 1742-2876. DOI: https : / / doi . org / 10 . 1016 / j . diin . 2019 . 03 . 002.

[10] Ziya Alper Genc¸, Gabriele Lenzini, and Peter Y. A. Ryan. "Next Generation Cryptographic Ransomware". In: Secure IT Systems. Ed. by Nils Gruschka. Cham: Springer International Publishing, 2018, pp. 385–401. ISBN: 978-3-030-03638-6.

[11] T. Cubitt, D. Elkouss, W. Matthews, *et al.*, "Unbounded number of channel uses may be required to detect quantum capacity," *Nature Communications*, vol. 6, pp. 6739:1-4, May 2015.

[12] V. Ojha, A. Sharma, V. Goar, and P. Trivedi, "Limitations of practical quantum cryptography," *Intl. Journal of Computer Trends and Technology*, vol. 1, no. 1, pp. 90-93, 2011.

[13] S. Pirandola, C. Ottaviani, G. Spedalieri, *et al*., "High-rate measurement-device-independent quantum cryptography," *Nature Photonics*, vol. 9, no. 6, pp. 397-402, May 2015.

[14] J. Clement. Digital users worldwide 2020. [Accessed 22-Aug-2020] [Online]. URL: https : / / www. statista . com / statistics /617136/digital-population-worldwide/.

[15] Nicolas Gisin, Gr´egoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. "Quantum cryptography". In: Rev. Mod. Phys. 74 (1Mar. 2002), pp. 145–195. DOI: 10.1103/RevModPhys.74.145.

[16]Xiaojun Xiang, Qiong Li, Shahnawaz Khan, and Osamah Ibrahim Khalaf. Urban water resource management for sustainable environment planning using artificial intelligence techniques. Environmental Impact Assessment Review, 86, 2021.

[17] Osamah Ibrahim Khalaf, Kingsley A. Ogudo, and Manwinder Singh. A fuzzy-based optimization technique for the energy and spectrum efficiencies tradeoff in cognitive radio-enabled 5g network. Symmetry, 13(1):1–14, 2021.

[18] Bilal S.A. Alhayani and Haci Llhan. Visual sensor intelligent module based image transmission in industrial manufacturing for monitoring and manipulation problems. Journal of Intelligent Manufacturing, 32(2):597–610, 2021.

[19] Milind E. Rane and Umesh S Bhadade. Comparative Study of ROI Extraction of Palmprint. IJCSN International Journal of Computer Science and Network, 5(2), 2016.

[20] Osamah Ibrahim Khalaf, Kingsley A. Ogudo, and Manwinder Singh. A fuzzy-based optimization technique for the energy and spectrum efficiencies tradeoff in cognitive radio-enabled 5g network. Symmetry, 13(1):1–14, 2021.

[21] A. P. Bhatt, T. Babuta, and A. Sharma, “Quantum information processing and communication: Asian perspective,” *Intl. Journal of Computer and Mathematical Sciences*, vol. 7, no. 2, pp. 616-621, Feb. 2018.

[22] L. S. Bishop, S. Bravyi, A. Cross, J. M. Gambetta, and J. Smolin. (March 2017), Quantum volume, [Online]

[23] Nicola Jones. (June 2013). Computing: The quantum company. *Nature*. [Online]. Available: https://www.nature.com/news/computing-the-quantum-company-1.13212

[24] Timothy Hollebeek. (May 2019). Future-proofing security in a post-quantum cryptography world. [Online]. Available: https://securityboulevard.com/2019/05/futureproofing-security-in-post-quantum-cryptography-world/

[25] S. Gupta and C. Dutta, “Internet of things security analysis of networks using quantum key distribution,” *Indian Journal of Science and Technology*, vol. 9, no. 48, pp. 105551:1-11, 2016.

[26] R. Pell. (January 2018). IoT security algorithm accepted by NIST for quantum cryptography project. [Online]. Available: https://www.eenewseurope.com/news/iot-security-algorithm-accepted-nist-quantum-cryptography-project

[27] https://ts2.space/en/quantum-cryptography-for-internet-of-things-iot-and-edge-computing