EXPLORING THE INTERSECTION OF QUANTUM COMPUTING AND INTERNET OF THINGS SECURITY: A COMPREHENSIVE SURVEY

Dr. B. Sathananth[1], J. Selvin Jeba Singh[2]
[1,2] Department of Electronics and Communication Engineering,
The Rajaas Engineering College, Vadakangulam, Tirunelveli–627116.

Abstract
The quick deployment of the Internet of Things (IoT) has caused security concerns, hence, exposing critical vulnerabilities across various regions, including smart cities, healthcare, and agriculture. This comprehensive survey of quantum computing and IoT security devices delimitates the benefits of quantum algorithms and the possibilities of making communication secure. Protocols that include quantum principles like superposition, entanglement, and quantum interference, which consequently results in things like secure key distribution and authentication algorithms, are discussed. The survey covers quantum key distribution (QKD) protocols, quantum authentication approaches that are presented as solutions, and the challenges of applying quantum cryptographic techniques to IoT systems. Moreover, this survey estimates the viability of quantum-enabled communication, search through the utilization in different sectors, and looks at current quantum software tools. This purpose is to lay a foundation for both future research and successful practical solutions in the ever-changing environment of IoT security.

Keywords—Authentication, Cryptography, Internet of Things (IoT), Post-quantum Cryptography, Quantum Computing, Quantum Key Distribution (QKD), Secure Communication, Security.

I. INTRODUCTION

The Internet of Things (IoT) refers to a network of physical objects, or "things," that are embedded with sensors, software, and various technologies. It enables them to connect and share data with other devices and systems to the Internet. The use of IoT is growing across a wide range of applications, including smart grids, cities, and intelligent surroundings[1]. The rapid expansion of IoT applications has led to a significant rise in securityand privacyissues, stemming from the vast amount of data generated by these interconnected devices. Ensuring identity and privacy becomes paramount for IoT applications to meet the growing demand effectively while safeguarding potential users' security[2]. By utilizing the ideas of quantum physics, quantum computing is essential in protecting the IoT communication network. It offers effective security controls for IoT components, including data processing, communication, and handling of dynamic data[3].Creating quantum-resistant techniques and mechanisms for IoT safety problems is the key goal of quantum computing development. Unlike quantum computers, which use qubits, traditional computers control individual bits. These qubits represent the quantum state and the probability attached to them. Based on concepts from quantum mechanics like superposition and entanglement, these qubits are a type of information storage. Strong dependence between quantum particles is produced via entanglement [4]. The fundamental benefit of quantum computing is the ability to supply safe data and apply intelligent applications for efficient decision-making by employing quantum combination,

quantum properties authorization, and distribution of quantum keys (QKD).In thefield of quantum computing, QKD is a very active study are a that makes it possible for participants to communicate to create secret keys for safe communication[5].

Large amounts of data can be handled in actual time by using quantum computing, this may ultimately form the basis for incredibly potent computer systems. This is especially relevant for compute-intensive applications in healthcare, particularly in today's highly integrated IoT health IT model, which includes interconnected medical devices that can connect via the Internet or cloud services [6]. The transition from bits to qubits could significantly advance pharmaceutical research in the medical field [7]. This research includes studying protein folding, determining molecular fit [8], including that of medications and enzymes, and evaluating the strength of binding connections between individual biomolecules. By making on-demand computing possible, reframing medical data security, predicting chronic illnesses, and developing efficient medications. Qubits can help with whole-genome sequencing and analytics, which can be completed more quickly even if it is a labor-intensive process [9]. Researchers have investigated DNA sequence alignment usingGrover's method, doing pairwise alignment using the quantum Fourier transform (QFT). Additionally, a framework has been developed that uses the quantum approximate optimization method (QAOA) to makeit easierto reconstruct denovo DNAsequences. Thesequantum computing techniques enable de novo assembly, a powerful method for synthesizing the original DNA sequence from an unstructured collection of reads, without prior knowledge of the length, organization, or composition of the source DNA. When examining unknown species or detecting structural genomic changes that conventional read mapping approaches are unable to detect, this method becomes essential. Additionally, after genomic sequences have been produced, there has been a lot of interest in the examination of algorithmic data that is present in those sequences. To understand the complexity of the information encoded inside these sequences, a combination of Grover's technique and phase estimation has been investigated. The development of effective imaging systems with improved real-time fine-grained clarity for clinicians may be enabled by quantum computers. Additionally, it can resolve intricate optimization challenges related to creating the best radiation plan to kill cancerous cells while sparing the surrounding healthy tissue damage [10].

This work makes several key contributions:

- After reviewing IoT security concerns, this survey of quantum technology for securing IoT smart applications is presented.
- An explanation of the basic ideas behind quantum technology and the way they interact with safety mechanisms
- In-depth talks about how to maintain secure IoT communications using quantum keys are provided.
- The analysis focuses on evaluating the implementation and effectiveness of quantum-enabled communication in IoT systems.
- Applications of quantum computing in IoT applications are explored and discussed in detail
- The analysis of quantum software too ls and comparison of the existing models that incorporate routing and data aggregation
- The main challenges facing an IoT cryptosystem based on quantum computing are outlined

II. LITERATURE SURVEY

According to Xie et al. [11], lattice-based encryption is the foundation of upcoming post-quantum cryptography and a promising defence against quantum computer assaults. Lattice-based algorithms have benefits in terms of speed, efficiency, security, and less energy usage. An extensive study and comparison of the most well-known lattice-

based cryptosystems are presented in this research. The creation and standardization of a reliable post-quantum algorithm remain the primary obstacle in the ongoing investigation of cryptographic solutions for the quantum era.

Broadbent et al [12] proposed establishing the fundamentals of QKD, then going into the evolution of QKD networks and their practical application. The general architecture of the QKD network, its components, interfaces, and protocols are then described. The corresponding physical layer and network layer solutions are then thoroughly described, and finally, the standardization initiatives and QKD network application scenarios are covered. Finally, addresses potential avenues for future study and offers design principles for QKD networks.

Yuan et al. [13] discuss current research topics such as quantum computing, quantum walks, cryptography, big data, autonomous cars, image processing, AI, fuzzy logic, systems that cooperate, swarming optimization, and security. They employed a unique search approach to collect data from the Dimensions database, emphasizing that the findings are confined to the published publications on quantum computing-based IoT security. Further research will use a larger range of data sources.

Aslam et al. [14] introduced a new quantum-classical neural network, Res-QCNN, based on deep latent training. To provide a training approach for assessing IoT platforms, the model comprises a residual structural block coupled to a quantum neural network. The paper investigates the advantages and disadvantages of incorporating quantum ideas from deep residual learning. Res-QCNN outperforms earlier models while learning a unitary function and is resilient to noisy input.

Ygalet al. [15] submitted changes to four lightweight hash functions that made it to the final round of the National Institute of Standards and Technology (NIST) standard competition: PHOTON-Beetle, Ascon, Xoodyak, and Sparkle. These upgrades resulted in exceptional hashing throughput ranging from 70 Gbps to 1000 Gbps on a GPU platform, making them ideal candidates for high-performance data integrity checks in IoT applications. The study also employed ProjectQ to evaluate the efficiency of these hashing algorithms on a quantum computer.

Vuiket al. [16] advocated for a thorough examination of the implications of quantum computing on the security of 5G mobile communications. This analysis leads to a series of straightforward, incremental enhancements designed to provide the security of 5G, as well as 3G and 4G. They proposed a multi-phase strategy to bolster security to facilitate a smooth transition to a post-quantum-secure system by utilizing the backward compatibility features inherent in the 5G security architecture.

Bansaletal[17] proposed guidance for the upcoming generation of IoT developer son how to construct quantum-resistant solutions. The concept of quantum encryption is new in the field of cryptography. Compared to conventional encryption, its main advantages are sniffer detection and unconditional security. More effective quantum cryptography has been developed for private-sector businesses like banking. The moment for quantum cryptography methods is now, however, as the IoT has exposed billions of people to the risk of their personal information, device data, and advanced quantum computer development.

Yanget al [18]proposed to solve a binary optimization issue using A nnealing of Quantum (QA) in an IoT network too btain the best scheduling strategy. Real-time solutions can be provided by formulating specific problems based on specific design criteria. QA outperforms the competitors in terms of computational time. However, there is an embedding process that, in the event of significant issues, may delay the convergence at the appropriate time.

Liu et al. [19] developed a clever Deep Learning-Associated Quantum Computerization (DLAQC) framework for optimizing Edge caching in Fog-Radio Access Systems (F-RANs). The system prioritizes cached material at the network edge using Self Organizing Maps (SOMs), which are stored in a quantum memory module (QMM) that uses the Two-Level Spin Quantum Process (TLSQP). This method allows for quick cache refreshes and plenty of store space to handle variable user requests. The DLAQC framework was tested on multimedia material and found to dramatically reduce computation time and overhead.

Janietal [20] proposed methods capable of securing a post-quantum Internet of Things. To specifically assess how the IoT security solutions from the third-generation partnership project (3GPP) perform in a post-quantum setting. Additionally, evaluate the securityaspects of fifth-generation (5G) networks, make suggestions for improvement, and go over how a quantum computer can jeopardize security. To demonstrate that the present IoT architecture andimplementationscontainnumerousvulnerabilities.To do this, describe promising lattice-driven cryptographic methods that demonstrate to be quantum resistant.

This literature survey highlights a comprehensive collection of research conducted by different authors on the subject of quantum-enabled IoT security, as presented in the below Table 1

TABLE1.EXISTING WORK DONE BY AUTHORS ON QUANTUM-ENABLED IOT SECURITY

Author	**Description**	**Advantage**	**Disadvantage**
Xieetal[11]	Lattice-based quantumcomputing	Quantum-resistant securityframework	Solving multivariate polynomials in finite fields and the LWE protocol's complexity make them hard to understand and modify.
Broadbentetal[12]	Quantum key distribution for securing IoT communication	Secure key distribution	However,aslarge-scale extension necessitates integration with reliable relays, its level of security is diminished.
Yuanetal[13]	Quantum computing-based security analysis for the IoT environment	The analysis and results indicate that the cryptosystems demonstrate improved security features and enhanced cryptographic performance.	Examining nearby pixel correlations does not reveal useful information about the encrypted image.
Aslametal [14]	Quantumcomputing optimization technique for IoT platform using the deep residual approach	Contrary to conventional computing, quantum computing may take advantage of quantum mechanics' extensive parallelism,quantum entanglement, and quantum	However, due to variancesinnetwork operation, it would be morechallenging to make such a determination in the case of an external infiltration.

		superposition.	
Ygaletal[15]	Optimizing lightweight hash functions for GPU and quantum computer implementation in IoT applications.	The highest throughput was attained by PHOTON-Beetle in this implementation.	However, in quantum computing, qubits for t must be newly allocated for each linear layer, as they cannot be recycled
Vuiketal[16]	Theimpactof quantumcomputing onreal world securityisanalyzed	Quantumcomputing for5Gmobile communication is analyzed	Securityconcerns arenotanalyzed
Bansaletal[17]	Hybrid architecture for resolving cryptographicissues in IoT employing quantumcomputing	The key can be secured, and the communications can be safe.	Reversible calculations, however, can be viewed as a significantchallenge in quantum computing.
Yanget al [18]	Optimization of Quantum Scheduling for UAV-Enabled IoT Networks	Quantum Annealing (QA) excels over competitors in computational time.	However,thereisan embedding process that, in the event of significant issues, may delay the convergenceatthe appropriate time.
Liuetal[19]	Edge caching in fog-based sensor networks using a deep learning and quantum computing framework.	The framework is tested with multimedia content and achieves successful results, significantly reducing computation time and overhead.	Although edge caching (EC) can handleeachrequest instantaneously, it is still difficult.
Janiet al [20]	Cyber security challenges associatedwiththe IoT in a post-quantumworld	NB-IoThasahigh energy efficiency	Symmetrickeysare difficultto manage.
Our survey	A comprehensive investigationofthe effects of quantum computing on the traditional cryptographically secure primitives used to secure IoT applications	Analysis of the IoT communicationlayer design and security issues	

III. IOT SECURITY THREATS

Novel applications including smart cities, agriculture, and healthcare have accelerated the development of IoT-enabled communication. These IoT gadgets generate large amounts of data in many circumstances. As the number of IoT applications grows, so does the risk of hacks that compromise user privacy. Authentication, integrity, authorization, and trust management are essential security issues in an Internet of Things environment.Figure 1 depicts the key security challenges in the IoT layered architecture. This section discusses the advantages of implementing a quantum layer to improve IoT security and tackles problems in the IoT architecture.

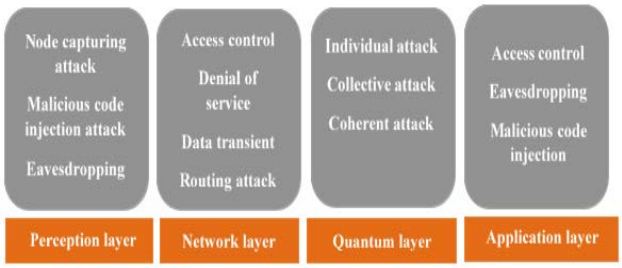

Fig.1.Securitythreats onIoTlayer architecture

Fig. 1 depicts the IoT layer architecture. This exposes numerous security vulnerabilities at different levels. The perception layer, where sensors collect ambient data, is subject to assaults including sensor node acquisition, fake data injection, and eavesdropping. Open internet connectivity exposes the network layer to access control assaults, denial of service threats, and data interception. The addition of a quantum layer enhances IoT security by enabling safe key distribution, but it also introduces new vulnerabilities, as quantum cryptography may be vulnerable to individual, collective, and coordinated assaults. Finally, the application layer, which offers services for user decision-making, confronts several obstacles, such as eavesdropping, access control violations, service outages, and malicious code penetration.

A. Quantum Fundamentals

The design of conventional computers accounts for the effects of noise on transistor performance, particularly as transistors shrink in size. As a result, their circuits are engineered to minimize the influence of quantum phenomena. In contrast, quantum computers adopt a different strategy by using quantum bits (qubits) instead of classical bits. These qubits have two quantum states, similar to classical bits representing 0 or 1, but they also possess uniquequantum properties. Theycan exist in asuperposition, simultaneouslyholding values 0 and 1, leading to the fascinating concept of superposed bits. The three characteristics are listed as follows [21].

Superposition: Superposition is a key principle of quantum mechanics that allows for the combination of two quantum states to create another valid quantum state. This principle allows a quantum system, such as a quantum particle or qubit, to exist simultaneously in multiple positions or states. It empowers quantum computing with extraordinary high-speed parallel processing, distinguishing its ignificantly from classical systems bound by binary limitations. Within there almof quantum computing, information can exist in two states simultaneously, unveiling exceptional computational possibilities.

Entanglement: Entanglement is the phenomenon in which a pair or group of particles interact in such a way that each particle's quantum state cannot be described alone; instead, it must be treated in connection to the states of the other particles in the system. This remarkable characteristic of entanglement persists even when the particlesare physically separated by significant distances.

Interference: In quantum computers, interference has a similar function to classical physics' wave interference. Two waves interacting in the same medium are said to interfere with one another. When waves are aligned in the same direction, it creates a resultant wave known as constructive interference, or when waves are aligned in the opposite direction, it creates a resultant wave

known as destructive interference, with the amplitudes of the waves being canceled out.

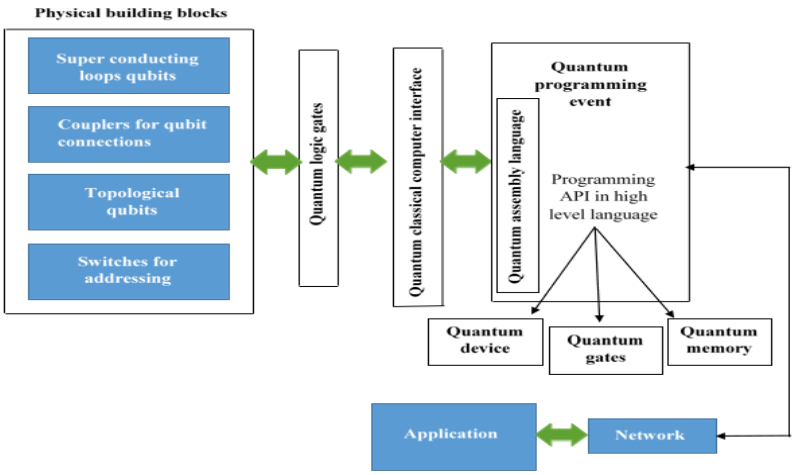

Fig.2.Architectureofquantum computing

The fundamental unit of Quantum computing comprises two layers: The Quantum computing layer and the classical computing layer,asdepictedi n Fig2.These layer stogether form the basic building block of Quantum computing.

Fig 2 shows the physical components of the quantum computer architecture, which comprise topological qubits, couplers to connect qubits, superconducting loop qubits, and switches to address qubits. These building blocks serve as inputs that are transmitted to quantum logic gates. After performing operations, the results are transmitted to the quantum-classical computer interface. The processed data is then stored in quantum devices, quantum gates, and quantum memory, all of which are situated within the quantum programming event. Subsequently, the information is transmitted through the network to carry out specific functions. Finally, based on user decisions, the application layer executes the desired operations.

A. Classical bits to quantum bits

Quantum computing makes use of qubits, whereas classical computing processes data using bits. This functions by the ideas of quantum mechanics. These particles' quantum states are denoted by the symbols |0> for spin-up and |1> for spin-down. Up to $2n$ potential values can be represented by a set of n qubits, with the probability of each value being assessed separately.

B. Quantum superposition

Quantum superposition is the term for the state in which qubits exist as a linear combination of |0> and |1>. According to quantum mechanics, a system is not constrained to just one state and can concurrently occupy all potential states. Nevertheless, the superposition collapses upon measurement, observing the qubits in a determinate state of either |0> or |1>.

C. Quantum key distribution

Quantum key distribution (QKD) is a prominent application of quantum cryptography that offers information-theoretic security for sharing symmetric secret keys between two legitimate parties, relying on the principles of quantum physics. Symmetric-key cryptosystems can then employ these secret keys to encrypt private messages that will be transmitted via a public channel. Utilizing larger key sizes offers an avenue for achieving quantum-safe properties in various symmetric-key cryptosystems, including the widely adopted Advanced Encryption Standard (AES). However, traditional secret key structures are extremely vulnerable to quantum computers so securely sharing the secret key remains a significant challenge in symmetric-keycryptography, and this challenge can be overcome through the use of QKD in asymmetric key structures. Despite the current infancy of quantum computers, QKD remains essentialasitprovideslong-termsecurity.Itsafeguardsagainstpotentialfutu readvancements in quantum computing and associated algorithms that could potentially

decrypt encrypted messages captured and stored by eaves droppers. This becomes particularly crucial for sensitive information like long-term government secrets that must be kept confidential for extended periods. Employing QKD in such scenarios can significantly enhance the security and confidentiality of the information [23]. For a secure IoT communication system, quantum-based keys are essential. This approach involves communicative entities sharing a secure key. Notable quantum key distribution protocols include BB84, SARG04, BBM92, and E91. By utilizing both quantum and conventional channels, QKD seeks to safely distribute and transfer keys. The secret of key distribution is to deliver random bits at random times to the recipient. The constraints of quantum physics restrict how much information can be taken out of a quantum system.

D. Quantum Authentication

Identity authentication, which confirms the veracity and secrecy of communications, guarantees the security of communication. Three assurances are provided by mutual authentication: message integrity, non-repudiation, and verification. Entanglement and quantum signatures can be used to create quantum-based identity authentication.

Quantum Entanglement: Quantum entanglement is a surprising aspect of quantum communication in which the states of two entangled particles are linked. These entangled states are generally known as Bell states. Equations 1 and 2 show the mutually orthonormal entangled states.

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

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

In this case, Bob's side of the two-level quantum system is represented by |0'> and |1'>, while Alice's side is represented by |0> and |1>, which together constitute an orthogonal basis.

QuantumSignature: Quantum signatures are employed to confirm the identity of authenticated users. There are several varieties of quantum signatures, including arbitrated quantum signatures (AQS), quantum group signatures, and quantum blind signatures. Quantum walk-based quantum signatures have also been discussed. These quantum signatures can be used for non-repudiation and defence against user impersonation attacks, such as in Quantum Cheque applications.

E. IoT enabled by quantum technology

The Internet of Things (IoT) framework connects various heterogeneous devices through different wireless standards, including WiFi, Bluetooth, Zigbee, and 6LOWPAN, which are key enabling technologies for IoT. These innovations facilitate data transfer for applications such as smart farming, advanced healthcare infrastructure, and smart cities. The integration of IoT with quantum computing is crucial for these applications, as they require data privacy and confidentiality. While classical cryptography, including public and private key systems, currently protects IoT communications, quantum computers are expected to undermine this security. Theoretically, the public-key-based infrastructure is already in danger from quantum-based Shor's [29] and Grover's [30] algorithm. If these security issues remain unaddressed, eavesdroppers could exploit vulnerabilities through teleportation-based attacks, man-in-the-middle attacks, and denial-of-service attacks [31]. Specific threats include pulse-energy monitoring, laser damage, laser seeding, information leakage (Trojan horses), source faults, side-channel attacks, device calibration issues, and timing attacks. To mitigate these risks, quantum cryptography offers a robust solution for secure communication, bridging the gap between theory and practical application [32]. Given the resource constraints of IoT devices, securing sensitive information requires lightweight cryptography that accommodates their limited computational capabilities [33]. Additionally, as both classical and potential quantum attacks increase, adopting quantum-resistant cryptography becomes crucial. Lattice-based cryptography shows promise as a secure and effective approach for post-quantum cryptography [34]. As IoT

communication continues to evolve, integrating quantum computing will be essential for establishing secure and resilient communication channels.

F. Applications of quantum computing in IoT

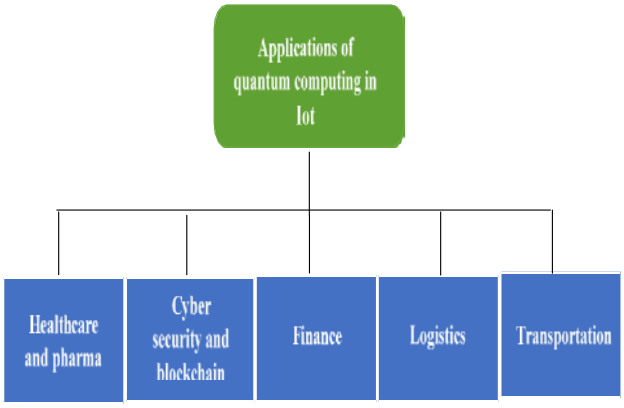

Fig.3. Applications ofquantum computinginIoT

Fig 3 showcases various applications of quantum computing in IoT, highlighting its potential to tackle a diverse array of challenges across multiple industries. Quantumcomputers can be used to tackle issues in the banking industry, such as financial-related tasks, and they have also been employed in the healthcare and pharmaceutical industries, particularlyin drug discovery. Quantum computing can support blockchain solutions for tackling supply chain problems in logistics, as well as encrypted transactions for improved cybersecurity. Quantum computing can also aid with wave transportation systems and traffic organization.

Healthcare and Pharma: Because it takes a lot of computer power to simulate molecules, drug research is an expensive endeavor. Because quantum computers can successfully replicate quantum processes, they are a good fit for pharmaceutical research and development. On drug discovery applications using quantum computing, Biogen and Accenture collaborated. Quantum computing has also been advantageous to the healthcare industry.Chronic diseases require careful lifestyle monitoring.

Cyber security and blockc hain: Block chain is utilized for contracts and encrypted transactions, but its reliance on cryptographic techniques makes it vulnerable to advanced cyberattacks. Exploring quantum blockchain offers a proactive approach to future challenges. While Accenture has acknowledged the intersection of blockchain and quantum, there is a growing interest in post-quantum cryptography—algorithms designed to withstand the capabilities of powerful quantum computers developed by companies like Microsoft and Google. This area is increasingly attracting attention from cyber security firms.

Finance: Market forecasting, fraud detection, risk analysis, asset pricing, portfolio optimization, and other banking-related issues may all be handled by quantum computers.

Logistics: Traditional computers frequently have trouble handling complex supply-chain challenges, which suggests that quantum computing has a promising future.

Transportation: The traveling salesman problem, in all its variations, poses a significant challenge for NISQ devices due to its role in route optimization. Whether for autonomous or traditional vehicles, managing a large fleet presents rapidly changing optimization challenges as the number of vehicles increases. The traffic optimization project Volkswagen is working on with D-Wave is the best illustration of quantum computing in action [35].

G. H. Quantum Software and Tools

Microsoft'sQDK,Google'sCirql,Xanadu'sStrawberryFields,andQXSimulatorareafewof the well-known quantum computation simulators accessible. Q#, QCL, and Q language are a few of the well-known quantum programming languages. The IBM Q5 Tenerife, Rigetti 8Q Agave, D-wave 2000Q, and Google Bristlecone are some of the most well-known quantum processors.

A. Comparing models with routing and data aggregation

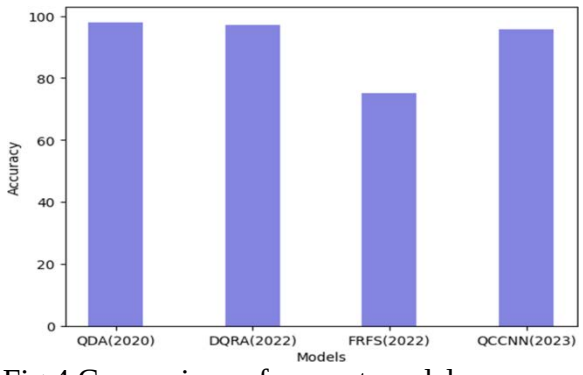

Fig.4.Comparison of current models incorporating routing and data aggregation

Fig4 presents a comparison of different models incorporating routing and data integration. The QDA model achieved an accuracy of 98%, the DQRA model achieved an accuracy of 97%, the FRFS model achieved an accuracy of 75%, and the QCCNN model achieved an accuracy of 95%

B. *Challenges of Quantum-based IoT*

Implementing Quantum-Assisted Machine Learning (QAML) algorithms to outperform classicalmachinelearningalgorithmscomeswithitschallenges.Thequantumversionsofwell-known machine learning algorithms may encounter difficulties in achieving the expected speedup due to limitations inherited from the Harrow-Hassidim-Lloyd (HHL) algorithm. Quantum Key Distribution (QKD) offers a secure method for transmitting keys. However, using quantum channels for IoT communication among numerous users presents challenges duetothelimitedrangeofQKD,whichissuitableprimarilyforshort-distancecommunication. The communication process is deemed compromised if an eavesdropper is found on the quantum channel, and it won't start up again until it's certain that there isn't another one listening in. Furthermore, eavesdropper presence is a major concern to quantum-based reversible computers. Quantum communication can be subject to individual attacks, in which a hacker creates a new quantum channel by intercepting Alice and Bob's quantum signal.

IV. CONCLUSION

By connecting disparate devices, the Internet of Things (IoT) provides consumers with a wealth of benefits that enable them to make well-informed decisions. Strong security measures, however, are required due to the sensitive nature of the data handled by these applications, especially in military, smart city, and healthcare contexts. Because traditional encryption techniques rely on intricate mathematical ideas, they are becoming more and more susceptible to attacks from quantum computing. Therefore, to protect IoT communications from potential quantum assaults, it is imperative to incorporate quantum-based security. In addition to exploring quantum-resistant security solutions, quantum authentication strategies, and quantum key distribution (QKD), this review offers a thorough overview of security risks to Internet of Things applications. Additionally, it discusses the difficulties in incorporating quantum capabilities into Internet of Things systems and emphasizes the significance of quantum-based cryptography techniques for secure communication between IoT devices.

REFERENCES

[1] Deepa V Jose, A Vijyalakshmi, An Overview of Security in Internet of Things, Procedia Computer Science, Volume 143, 2018, Pages 744-748, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2018.10.439.

[2] Udoh, I.S. and Kotonya, G. (2018), Developing IoT applications: challenges and frameworks. IET Cyber-Physical Systems: Theory & Applications, 3: 65-72. https://doi.org/10.1049/iet-cps.2017.0068.

[3] Sun, Li, and Qinghe Du. 2018. "A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions" *Entropy* 20, no. 10: 730. https://doi.org/10.3390/e20100730.

[4] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy and A. Ghoneim, "Secure Quantum Steganography Protocol for Fog Cloud Internet of Things," in *IEEE Access*, vol. 6, pp. 10332-10340, 2018, doi: 10.1109/ACCESS.2018.2799879.

[5] Usenko, Vladyslav C., and Radim Filip. 2016. "Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense" *Entropy* 18, no. 1: 20. https://doi.org/10.3390/e18010020.

[6] Alshammari, Majid R., and Khaled M. Elleithy. 2018. "Efficient and Secure Key Distribution Protocol for Wireless Sensor Networks" *Sensors* 18, no. 10: 3569. https://doi.org/10.3390/s18103569.

[7] Thomford, Nicholas Ekow, Dimakatso Alice Senthebane, Arielle Rowe, Daniella Munro, Palesa Seele, Alfred Maroyi, and Kevin Dzobo. 2018. "Natural Products for Drug Discovery in the 21st Century: Innovations for Novel Drug Discovery" *International Journal of Molecular Sciences* 19, no. 6: 1578. https://doi.org/10.3390/ijms19061578.

[8] Nam, G.-M. and Makarov, D.E. (2016), Extracting intrinsic dynamic parameters of biomolecular folding from single-molecule force spectroscopy experiments. Protein Science, 25: 123-134. https://doi.org/10.1002/pro.2727.

[9] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," in *IEEE Access*, vol. 6, pp. 20596-20608, 2018, doi: 10.1109/ACCESS.2018.2817615.

[10] Lahoz-Beltra, Rafael. 2016. "Quantum Genetic Algorithms for Computer Scientists" *Computers* 5, no. 4: 24. https://doi.org/10.3390/computers5040024.

[11] Xie, J., Hu, Yp., Gao, Jt. *et al.* Efficient identity-based signature over NTRU lattice. *Frontiers Inf Technol Electronic Eng* **17**, 135–142 (2016). https://doi.org/10.1631/FITEE.1500197.

[12] Broadbent, A., Schaffner, C. Quantum cryptography beyond quantum key distribution. *Des. Codes Cryptogr.* **78**, 351–382 (2016). https://doi.org/10.1007/s10623-015-0157-4.

[13] J. Yuan and X. Li, "A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion," in *IEEE Access*, vol. 6, pp. 23626-23638, 2018, doi: 10.1109/ACCESS.2018.2831898.

[14] A. Aslam and E. Curry, "Towards a Generalized Approach for Deep Neural Network Based Event Processing for the Internet of Multimedia Things," in IEEE Access, vol. 6, pp. 25573-25587, 2018, doi: 10.1109/ACCESS.2018.2823590.

[15] Bendavid, Ygal, Nasour Bagheri, Masoumeh Safkhani, and Samad Rostampour. 2018. "IoT Device Security: Challenging "A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function" *Sensors* 18, no. 12: 4444. https://doi.org/10.3390/s18124444.

[16] Möller, M., Vuik, C. On the impact of quantum computing technology on future developments in high-performance scientific computing. *Ethics Inf Technol* **19**, 253–269 (2017). https://doi.org/10.1007/s10676-017-9438-0.

[17] I. Bhardwaj, A. Kumar and M. Bansal, "A review on lightweight cryptography algorithms for data security and authentication in IoTs," 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 2017, pp. 504-509, doi: 10.1109/ISPCC.2017.8269731.

[18] Q. Yang and S. -J. Yoo, "Optimal UAV Path Planning: Sensing Data Acquisition Over IoT Sensor Networks Using Multi-Objective Bio-Inspired Algorithms," in IEEE Access, vol. 6, pp. 13671-13684, 2018, doi: 10.1109/ACCESS.2018.2812896.

[19] Liu, Jeremy, Federico M. Spedalieri, Ke-Thia Yao, Thomas E. Potok, Catherine Schuman, Steven Young, Robert Patton, Garrett S. Rose, and Gangotree Chamka. 2018. "Adiabatic Quantum Computation Applied to Deep Learning Networks" Entropy 20, no. 5: 380. https://doi.org/10.3390/e20050380.

[20] Suomalainen, Jani, Adrian Kotelba, Jari Kreku, and Sami Lehtonen. 2018. "Evaluating the Efficiency of Physical and Cryptographic Security Solutions for Quantum Immune IoT" *Cryptography* 2, no. 1: 5. https://doi.org/10.3390/cryptography2010005.

[21] Ruan, Y., Chen, H., Tan, J. et al. Quantum computation for large-scale image classification. Quantum Inf Process 15, 4049–4069 (2016). https://doi.org/10.1007/s11128-016-1391-z.

[22] Vermaas, P.E. The societal impact of the emerging quantum technologies: a renewed urgency to make quantum theory understandable. Ethics Inf Technol 19, 241–246 (2017). https://doi.org/10.1007/s10676-017-9429-1.

[23] Broadbent, A., Schaffner, C. Quantum cryptography beyond quantum key distribution. Des. Codes Cryptogr. 78, 351–382 (2016). https://doi.org/10.1007/s10623-015-0157-4.

[24] Usenko, Vladyslav C., and Radim Filip. 2016. "Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense" *Entropy* 18, no. 1: 20. https://doi.org/10.3390/e18010020.

[25] A. Mariano, T. Laarhoven, F. Correia, M. Rodrigues and G. Falcão, "A Practical View of the State-of-the-Art of Lattice-Based Cryptanalysis," in IEEE Access, vol. 5, pp. 24184-24202, 2017, doi: 10.1109/ACCESS.2017.2748179.

[26] M. Alshowkan and K. Elleithy, "Entanglement measurement-device-independent Quantum Key Distribution," 2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 2017, pp. 1-6, doi: 10.1109/LISAT.2017.8001976.

[27] Shi, W., Wang, Y., Li, L., Zhou, Y., Yang, Y. and Jiang, N. (2018), A Restricted Quantum Deniable Authentication Protocol Based on GHZ States. Chinese J. Electron., 27: 229-233. https://doi.org/10.1049/cje.2018.01.001.

[28] Guo, Qiang, Guoqing Ruan, and Jian Wan. 2017. "A Sparse Signal Reconstruction Method Based on Improved Double Chains Quantum Genetic Algorithm" Symmetry 9, no. 9: 178. https://doi.org/10.3390/sym9090178.

[29] W. Yin, Q. Wen, W. Li, H. Zhang and Z. Jin, "An Anti-Quantum Transaction Authentication Approach in Blockchain," in IEEE Access, vol. 6, pp. 5393-5401, 2018, doi: 10.1109/ACCESS.2017.2788411.

[30] A. Facon, S. Guilley, M. Lec'Hvien, A. Schaub and Y. Souissi, "Detecting Cache-Timing Vulnerabilities in Post-Quantum Cryptography Algorithms," 2018 IEEE 3rd International Verification and Security Workshop (IVSW), Costa Brava, Spain, 2018, pp. 7-12, doi: 10.1109/IVSW.2018.8494855.

[31] Zhu, J., Zhang, C. & Wang, Q. Biased decoy-state reference-frame-independent quantum key distribution. Eur. Phys. J. D 71, 319 (2017). https://doi.org/10.1140/epjd/e2017-80219-2.

[32] Y. -L. Gao, X. -B. Chen, Y. -L. Chen, Y. Sun, X. -X. Niu and Y. -X. Yang, "A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain," in IEEE Access, vol. 6, pp. 27205-27213, 2018, doi: 10.1109/ACCESS.2018.2827203.

[33] Kim, P., Han, D. & Jeong, K.C. Time–space complexity of quantum search algorithms in symmetric cryptanalysis: applying to AES and SHA-2. Quantum Inf Process 17, 339 (2018). https://doi.org/10.1007/s11128-018-2107-3

[34] Suomalainen, Jani, Adrian Kotelba, Jari Kreku, and Sami Lehtonen. 2018. "Evaluating the Efficiency of Physical and Cryptographic Security Solutions for Quantum Immune IoT" Cryptography 2, no. 1: 5. https://doi.org/10.3390/cryptography2010005