Received: 3 July 2023 | Revised: 1 November 2023 | Accepted: 13 November 2023

IET Quantum Communication

DOI: 10.1049/qtc2.12079

REVIEW

Quantum computing applications for Internet of Things

Mritunjay Shall Peelam | **Anjaney Asreet Rout** | **Vinay Chamola**

Department of Electrical and Electronics Engineering, BITS Pilani, Pilani, India

Correspondence
Vinay Chamola, Department of Electrical and Electronics Engineering, BITS Pilani, Old Workshop, Near FD-1, Pilani Town, Rajasthan 333031, India.
Email: vinay.chamola@pilani.bits-pilani.ac.in

Abstract

The rapidly developing discipline of quantum computing (QC) employs ideas from quantum physics to improve the performance of traditional computers and other devices. Because of the dramatically improved speed at which it processes data, it can be applied to various issues. QC has many potential applications, but three of the most exciting applications are unstructured search, quantum simulation, and network optimisation. Several existing technologies, such as machine learning, may benefit from its increased speed and precision. In this study, the authors will explore how the principles of QC might be applied to the Internet of Things (IoT) to improve its accuracy, speed, and security. Several approaches exist for achieving this goal, such as network optimisation in IoT using QC, faster computation at IoT endpoints, securing IoT using QC, a quantum sensor for IoT, quantum digital marketing, quantum-secured smart lock etc.

KEYWORDS
quantum computing, quantum computing techniques, quantum entanglement, quantum information, telecommunication security

1 | INTRODUCTION

Internet of Things (IoT) is a modern paradigm focused on creating an ecosystem of intelligent gadgets to provide betterment in our daily lives [1]. This is made feasible by the interconnectivity of sensors and actuators, which allows intelligent choices based on the analysis of existing data. IoT technologies are expected to give hitherto unheard-of opportunities for linking people. Figure 1 depicts the general operational architecture of IoT. In IoT, data processing and analysis is one of the difficult tasks. Computational data allows real-time data analysis and provides important insights. Machine learning (ML), data mining, and quantum computing (QC) have been developed to handle and analyse IoT device data. Computational data enables real-time analysis of linked devices' massive data streams in IoT. QC provides insights that help to enhance decision-making in different fields [2]. Edge computing systems increase IoT data processing and analysis, allowing new and creative solutions.

The widespread use of radio frequency identification devices (RFIDs) has aided the emergence of the IoT [3]. RFID employs radio tags with relatively low power consumption to identify real-world objects electronically. Although RFID tags are passive and dumb, they enable wireless intelligent tracking of goods in limited places [4]. These qualities prevent them from recording or understanding their surroundings. Gadgets cannot communicate, preventing evolution and data analysis. These gadgets have become active, cooperative, and intelligent because their interconnection may improve real-world services and infrastructure. The IoT is a worldwide interconnection where gadgets and sensors enable a new age of internet-linked products to improve our lives [5]. Massive data collection and analysis are needed. The developing world has proven IoT's importance and promise. Data and information security are also crucial but challenging to maintain. Internet-connected gadgets have led to unsecured networks and cyberattacks, putting sensitive data at risk. Yet, the IoT seeks innovative data and information security solutions. Businesses and the economy are most worried about IoT data security. We use the idea of 'QC' to assist in resolving many modern IoT-related problems. QC uses quantum phenomena such as entanglement and superposition for computation. A research physicist, Stephen J. Wiesner, created Conjugate Coding in 1960, and a Soviet and Russian mathematician named Alexander Holevo released a paper in 1973 demonstrating that n number of Q-bits may contain more information than n number of classical bits [6]. Because there had been so little development in quantum systems up to that time, physicists were disputing whether it was even possible to build a system that could control quantum particles in a way that made computing realistic. Though the study is ongoing, it became helpful in 2000 when the Technical University of Munich installed the first operational five Q-bit Nuclear Magnetic Resonance computer [7]. About 15 years later, or approximately 2015, major computer corporations like Google, IBM, and Microsoft joined the fight for quantum dominance.

According to the theory, the suggested design may incorporate the operational protocols and architectural features of quantum systems (i.e., entanglement) into the IoT networks, enhancing their security and speed compared to current methods. Figure 2 represents each section of this paper to more clearly demonstrate how QC and the IoT interact. However, not every node in an IoT network can be replaced by a quantum device since handling that much entanglement would be difficult and complex.

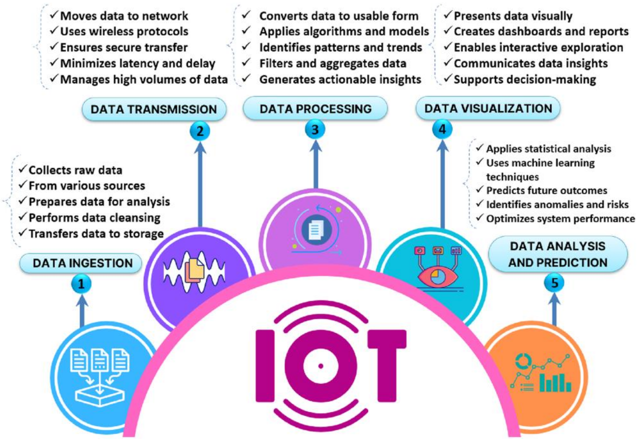
✓Moves data to network
✓Uses wireless protocols
✓Ensures secure transfer
✓Minimizes latency and delay
✓Manages high volumes of data
✓ Converts data to usable form
✓ Applies algorithms and models
✓ Identifies patterns and trends
✓ Filters and aggregates data
✓ Generates actionable insights
✓Presents data visually
✓Creates dashboards and reports
✓Enables interactive exploration
✓Communicates data insights
✓Supports decision-making
DATA TRANSMISSION
DATA PROCESSING
DATA VISUALIZATION
2
3
4
✓Applies statistical analysis
✓Uses machine learning techniques
✓Predicts future outcomes
✓Identifies anomalies and risks
✓Optimizes system performance
✓Collects raw data
✓From various sources
✓Prepares data for analysis
✓Performs data cleansing
✓Transfers data to storage
DATA INGESTION
1
DATA ANALYSIS AND PREDICTION
5
IOT

FIGURE 1 General operational architecture of IoT. IoT, Internet of Things.

We briefly review Industrial IoT, which finds many relevant use cases where QC can assist IoT operations that emerged due to the advancement of technology for machine-to-machine communication, the IoT, and the associated ecosystem. The IIoT encompasses all industrial sectors, including factories, warehouses, shipyards, transportation etc. It may be used in various fields, including supply chain management, quality assurance, maintenance and control, resource optimisation etc. [8]. The problem is that because a large volume of sensor data may often cause latency and storage issues, cloud-based data processing and analytics may be unable to manage IIoT [9]. IIoT systems must have improved connection, interoperability, and data security, be robust and energy-efficient to lessen network burden and use cloud tiers [10]. However, specific heterogeneous approaches represent a dilemma regarding total energy efficiency, network connection, and temporal criticality. This is where quantum-inspired optimisation approaches may be used for efficient routing. Quantum particle swarm optimisation is one approach capable of meeting the required conditions [11].

By enhancing overall interconnection and smart automation, the employment of QC-inspired technologies, in general, may accelerate the speed of change in technology, industries, and social patterns and processes in the 21st century [12]. In other words, Industry 4.0 may come much sooner than

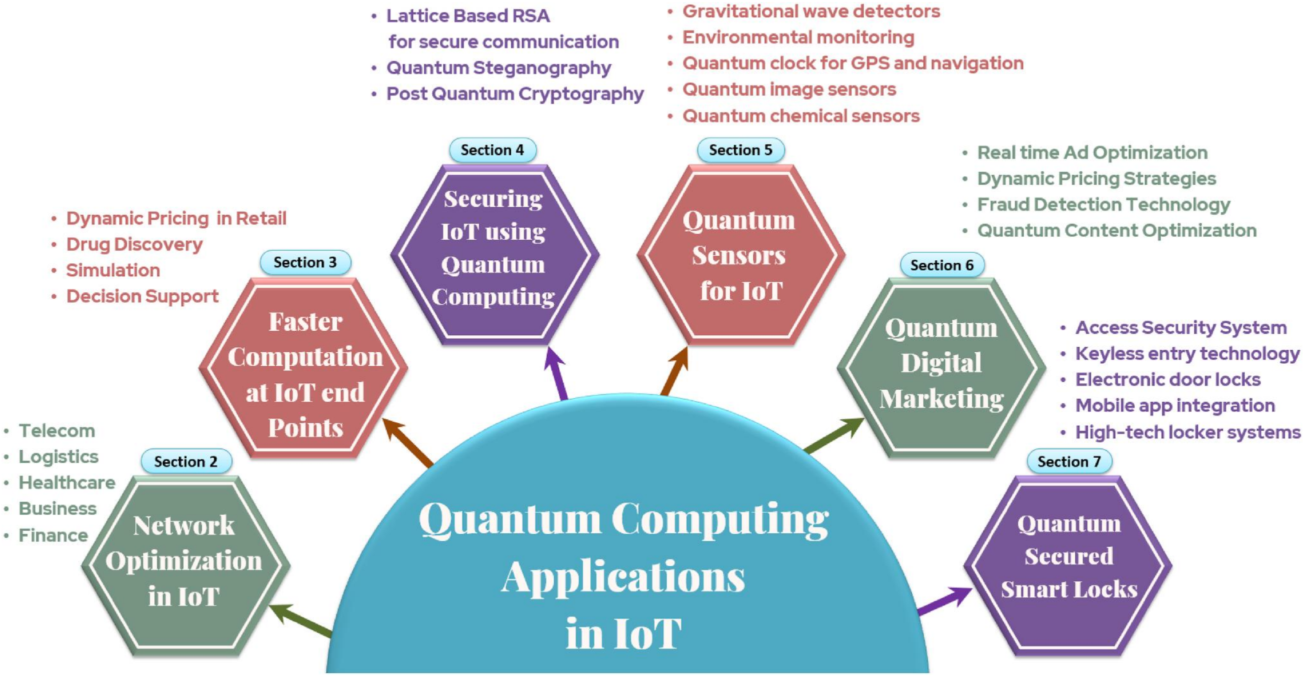
• Lattice Based RSA for secure communication
• Quantum Steganography
• Post Quantum Cryptography
• Gravitational wave detectors
• Environmental monitoring
• Quantum clock for GPS and navigation
• Quantum image sensors
• Quantum chemical sensors
Section 4
Securing IoT using Quantum Computing
Section 5
Quantum Sensors for IoT
• Real time Ad Optimization
• Dynamic Pricing Strategies
• Fraud Detection Technology
• Quantum Content Optimization
• Dynamic Pricing in Retail
• Drug Discovery
• Simulation
• Decision Support
Section 3
Faster Computation at IoT end Points
Section 6
Quantum Digital Marketing
• Access Security System
• Keyless entry technology
• Electronic door locks
• Mobile app integration
• High-tech locker systems
• Telecom
• Logistics
• Healthcare
• Business
• Finance
Section 2
Network Optimization in IoT
Section 7
Quantum Secured Smart Locks
Quantum Computing Applications in IoT

FIGURE 2 Section-wise interaction of quantum computing and Internet of Things (IoT).

expected. Consequently, the manufacturing process would become more flexible and adaptive to client demands, allowing the manufacture of highly customised items without requiring an extensive reconfiguration of the manufacturing base. However, there are still a few implementation issues:

1. To transform quantum technology solutions to commercial effect, one must have a thorough grasp of quantum technology and domain and integration expertise.
2. The QC environment and market are diversified. Existing benchmarks mainly concentrate on low-level hardware performance and do not accurately reflect application performance. Due to a dearth of community-driven, application-centred benchmarks, users cannot quickly estimate the performance they may expect from offered solutions.

In our research, we are exploring various aspects of applying QC in the field of the IoT. In Section 2, we focus on network optimisation in IoT using QC, aiming to enhance the efficiency and reliability of IoT networks. Section 3 investigates achieving faster computation at IoT endpoints, leveraging quantum algorithms for accelerated data processing. Section 4 addresses securing IoT using QC and developing quantum-based encryption and authentication methods. In Section 5, we explore quantum sensors for IoT, enhancing sensing capabilities for precise data collection. Section 6 delves into quantum digital marketing, leveraging quantum algorithms for improved marketing analytics. Lastly, Section 7 focuses on quantum-secured smart locks, applying quantum cryptography for robust security in IoT-enabled environments. Through our research, we aim to revolutionise the capabilities, efficiency, and security of IoT systems using QC technologies. However, despite these challenges, QC has too much promise to be dismissed without more thought. As a result, we will cover the six key facets of QC that make it a valuable complement to the IoT paradigm in the parts that follow (IoT). Table 1 compares frequently utilised standard terms and their respective acronyms within the manuscript. Table 2 represents the systematic contribution of QC Applications in the IoT. The major subsections of the manuscript are also summarised in Figure 2.

TABLE 1 Comparison of common acronyms and descriptions used in the manuscript.

Acronym	Description
IoT	Internet of Things
RFID	Radio frequency identification devices
NMR	Nuclear magnetic resonance
IIoT	Industrial Internet of Things
QPSO	Quantum particle swarm optimisation
QC	Quantum computing
DA	Data accuracy
QCiO	Quantum computing inspired optimisation
QIP	Quantum information processing
DVPN	Dynamic virtual private network
NIST	National Institute of Standards and Technology
POW	Proof-of-work
PQCrypto	Post quantum cryptography
EU	European Union
JSTA	Japanese Science and Technology Agency
GPS	Global positioning system
SQUID	Superconducting quantum Interference devices
QKD	Quantum key distribution
QRNG	Quantum random number generators
CX	Controlled-X
GTCW	Glued tree based on continuous quantum walk
QIoTNO	Quantum-based IoT network optimisation
DQC2O	Distributed quantum computing for collaborative optimisation
ML	Machine learning

2 | NETWORK OPTIMISATION IN IoT USING QC

Network optimisation in IoT using QC involves a multifaceted process. It begins with collecting massive IoT data, which is efficiently analysed using quantum algorithms such as Grover's and Shor's. QC accelerates optimisation tasks, enhancing network performance, security, and energy efficiency. It enables real-time decision-making, topology optimisation, and the implementation of quantum key distribution (QKD) to secure communication. Numerous real-world scenarios often contain optimisation difficulties, and we need more potent methods to handle them with high convergence while addressing every specific problem [13]. The countless IoT-related discoveries have laid the groundwork for innovation across various industries, including banking, healthcare, logistics, and agriculture. The economy of the future is thus moving in the direction of increasing automation and improving efficiency. By 2025, it is predicted that there will be close to 50 billion linked IoT devices worldwide. Data accuracy (DA) analysis for this cutting-edge paradigm becomes even more crucial with such a high dependence on IoT. Numerous quantum-computing-inspired optimisation (QCiO) strategies have recently been found to improve the precision and optimal behaviour of data acquired by widely scattered IoT devices in a dynamic environment [14]. IoT network optimisation using QC enhances the efficiency of resource allocation and scheduling for unmanned aerial vehicles serving sensor nodes by addressing a combinatorial problem with binary constraints. Quantum annealing, a QC technique, maps the original problem into a quadratic unconstrained binary optimisation form, using quantum properties to explore multiple solutions concurrently and potentially arrive at more efficient outcomes

TABLE 2 Contribution of QC applications in IoT.

Area in IoT	QC's role in IoT
Network optimisation	• Routing of IoT data • Reducing latency • Improving overall performance
Security	• Develop more secure encryption algorithms • Harder for hackers to steal sensitive information • Fraud detection
Sensing and monitoring	• Improve the accuracy and speed • Higher degree of sensitivity
Digital marketing	• Customer segmentation • Market research • Predictive modelling • Optimisation
IoT nodes	• Network optimisation • Security • Predictive maintenance • Decision-making
Smart lock	• Access control • Fraud detection • Energy efficiency • Big data analysis

Abbreviations: IoT, Internet of Things; QC, quantum computing.

[15, 16]. However, due to the current limitations of quantum annealers, a hybrid approach combines quantum and classical computing to refine and evaluate potential solutions, making QC a powerful tool for optimising IoT network scheduling [17]. Network optimisation in IoT using QC leverages the integration of QC to enhance data transmissions and improve network efficiency. This entails optimising sensor deployment to maintain sensor performance, employing quantum algorithms such as glued trees based on continuous quantum walks (GTCW) to minimise energy consumption and reduce data transmission error rates within IoT networks. Experimental results validate the effectiveness of this QC approach, demonstrating its superiority in terms of DA, temporal efficiency, and cost-effectiveness compared to conventional optimisation techniques [18]. In network optimisation for IoT utilising QC, the quantum-based IoT network optimisation (QIoTNO) method targets time efficiency and energy conservation in edge computing perceptual task offloading scenarios. QIoTNO employs adaptability metrics, logistic chaos perturbation, and advanced genetic algorithms to enhance convergence and reduce time consumption and energy loss. Comparative assessments show that QIoTNO improves adaptability by 4.89%, enhancing convergence speed and decreasing time consumption by 4.08% and energy loss by 3.91% on average [19]. QC offers the potential to optimise IoT networks with its high-speed parallel processing. However, challenges related to qubit fidelity and quantum channel noise hinder its application in IoT. To address these issues, an adaptive approach, DQC2O, is used for managing quantum computers and networks in IoT optimisation and a quantum resource allocation model based on stochastic programming to minimise quantum resource consumption in the face of uncertain optimisation demands [20].

3 | FASTER COMPUTATION AT IoT ENDPOINTS/IoT NODES ETC

When compared to our current computers, quantum computers are capable of operating at rates and power that are exponentially huge. They use quantum states to represent many bits simultaneously [21]. 'Atoms may be coded at the quantum level to represent all feasible input combinations, all at once, and therefore test all the possibilities concurrently'. Since IoT devices generate vast volumes of data that need intense processing and other complex optimisation, this is useful for IoT. In general, the immense processing capacity of QC may aid in solving many current difficulties. For instance, drug firms can now do hundreds of millions of comparisons and simulations involving complex interactions between large molecules using QC. It is also helpful in any circumstance where optimisation is necessary. This is achieved by iteratively analysing several scenarios and choosing the one that best meets the demands of the users. Numerous problems may be solved with this strategy, including transportation route optimisation and portfolio optimisation. Next, we focus on edge computing, a paradigm for managing data in IoT applications close to edge devices. Although computing at the logical edge of the network reduces latency and response time, more processing power is required as daily data generation increases. In contrast to pay-per-use, the most current cloud computing execution model offers service to end users based on how IoT applications use resources [22]. Using server-less computing in the edge computation paradigm accelerates data processing from IoT applications running on edge devices. A significant amount of processing power is needed for the system to operate well, which may be readily given by using QC [23]. It is still challenging to utilise QC to arrive at the most optimal answers, despite its promise, since it has several drawbacks, such as the need for a large number of error-correcting quantum bits (qubits) or challenging working circumstances. Therefore, most proposed methods combine QC with traditional ML [24]. To make QC feasible on IoT endpoints, a multifaceted approach is required [25, 26]. This entails advancing quantum technology to create smaller, more energy-efficient quantum processors, developing quantum communication channels for IoT devices to tap into centralised QC resources, exploring hybrid computing models that combine classical and quantum processing, and optimising quantum algorithms for IoT-specific applications to reduce computational demands [27]. Additionally, research into energy-efficient cooling systems, miniaturised quantum hardware, and secure QKD is essential. Collaborative efforts between QC researchers and IoT developers are crucial to address the technical challenges of implementing QC on resource-constrained IoT endpoints [28, 29]. However, this remains a long-term aspiration subject to ongoing advancements in both quantum and IoT technology.

4 | SECURING IoT USING QC

With today's cutting-edge and modern information and communication technologies, such as the 'fog cloud IoT', secure connections are urgently required to safeguard sensitive data. Location-aware, low-latency, instantaneously deployable, and scalable information technology solutions are now possible because of this revolutionary paradigm and fantastic technology. Additionally, it lowers infrastructure costs. It is a tried-and-true technique for putting cloud services and resources near consumers, optimising such services and resource utilisation in edge networks.

However, fog cloud IoT services have raised concerns about privacy and security. Sensitive data transmission across open, public networks, such as in fog cloud IoT, is problematic. One strategy for dealing with security challenges, notably the hidden handling of sensitive data in the Internet-based computing paradigm, is quantum information processing (QIP) [30] as shown in Figure 3 Scientists working on QIP's development and those interested in implementing these cutting-edge methods for processing, storing, and sending data have shown much interest in it. In recent years, interest has also been shown in several significant QIP subtopics, such as quantum teleportation, quantum cryptography, and quantum steganography. For example, one suggested paradigm offers a 'guaranteed' Intrusion Detection System, which reduces the odds of a cyber-attack being undetected significantly. Utilising lengthy Quantum Safe encryption keys, which are immune to assaults by Quantum Computers using current quantum algorithms, the risk of a successful undetected cyberattack against a dynamic virtual private network may be significantly reduced (even close to zero) [31]. Even Quantum Computers, according to the US National Institute of Standards and Technology, cannot decipher an encrypted communication utilising Quantum Safe encryption keys with thousands of bits. Another example would be its use in Blockchain technology. Blockchain technology, an open distributed ledger, processes data from IoT applications in a chain of blocks. Because data is processed in blocks, this technique restricts data processing computational speed but is especially effective at safely processing data for server-less edge computing. An aspect of blockchain architecture is the labour necessary to calculate the nonce values and hashes for each data block in the whole chain. To validate the Proof-Of-Work, this operation must run simultaneously over several distributed architecture nodes (POW). These processes might be incorporated into a Function as a Service platform using micro-services and then put up on a server-less pipeline. To address this issue, quantum computers may perform large-scale computing for resource management. Post-QC is now a promising research topic that has been sponsored since 2006 by both its conference series (PQCrypto) and other organisations that are doing standardisation initiatives and a range of projects. Even though the bulk of these programmes do not mainly target post-quantum IoT systems, it is critical to monitor their results and standardisation processes. The European Union and the Japanese Science and Technology Agency have both provided substantial financial assistance to initiatives using post-quantum cryptosystems. PQCrypto, SAFE crypto, CryptoMathCREST, and PROMETHEUS are a few examples [32].

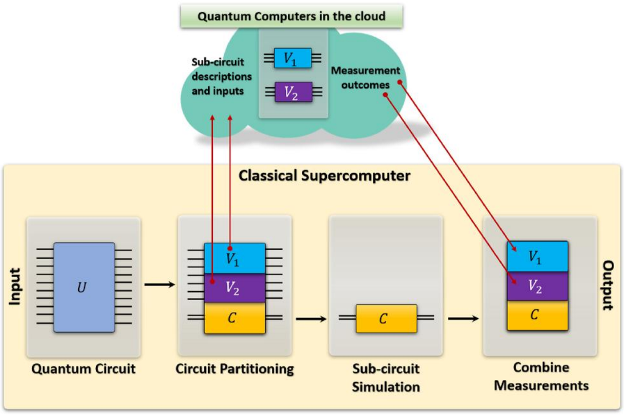

FIGURE 3 Quantum computing applied to cloud services.

It is important to remember that post-quantum security is not just about protecting individual nodes in the IoT; it is also a means of protecting the whole communications infrastructure that underpins the IoT. This is connected to the fact that the most complex processing jobs are increasingly being handled in centralised servers or clouds on the Internet nowadays because they exceed the computing capabilities of IoT end devices.

5 | QUANTUM SENSORS FOR IoT

The IoT has grown tremendously in recent years, connecting various physical devices, sensors, and systems to the Internet. This has opened up new possibilities for data collection, analysis, and control of physical systems. Still, the precision and accuracy of these systems are often limited by the performance of the sensors used. This is where quantum sensors come in. By leveraging the unique properties of quantum systems, quantum sensors have the potential to significantly enhance the performance of IoT systems and create new and innovative solutions for various applications [33]. Quantum sensors are based on the principles of quantum mechanics and can measure physical quantities with unprecedented precision and accuracy. The unique properties of quantum systems, such as superposition and entanglement, allow for measurements with a much higher sensitivity than classical sensors. This makes quantum sensors ideal for applications that require high-precision measurements, such as navigation, environmental monitoring, and healthcare. Quantum sensors differ from classical sensors because quantum sensors use network entanglement manipulation and qubit superposition, as shown in Figure 4.

One of the most promising applications of quantum sensors in IoT is environmental monitoring. Conventional environmental sensors are limited in measuring physical quantities such as temperature, pressure, and humidity with high accuracy

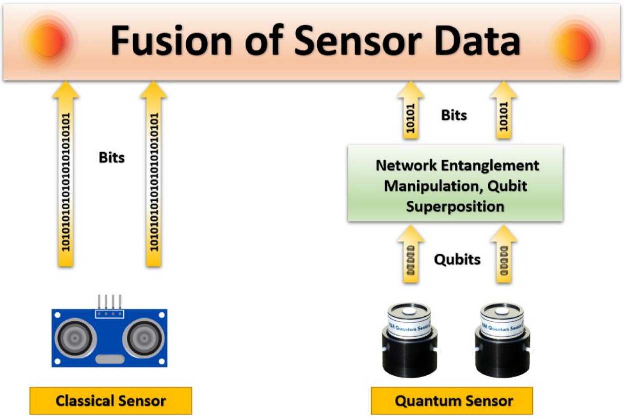

FIGURE 4 Fusion of quantum and classical sensor data.

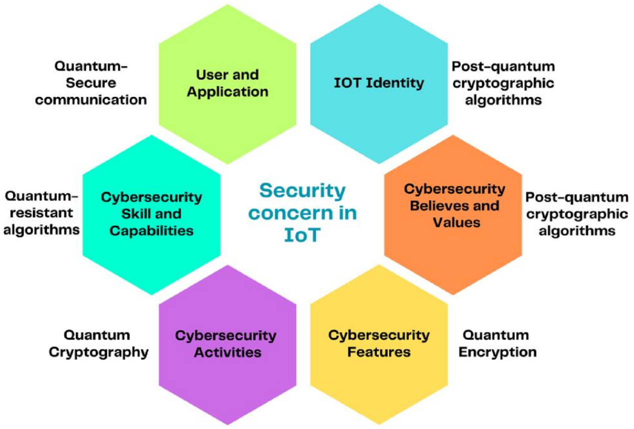
Quantum-Secure communication
User and Application
IOT Identity
Post-quantum cryptographic algorithms
Quantum-resistant algorithms
Cybersecurity Skill and Capabilities
Security concern in IoT
Cybersecurity Believes and Values
Post-quantum cryptographic algorithms
Quantum Cryptography
Cybersecurity Activities
Cybersecurity Features
Quantum Encryption

FIGURE 5 Quantum solutions for IoT security. IoT, Internet of Things.

and stability. This can result in errors in the data collected and a lack of confidence in the results. Quantum sensors, on the other hand, can make precise measurements of these quantities, even in harsh environments. This can lead to improved environmental monitoring and decision-making, particularly in areas such as agriculture, weather forecasting, and climate change research [34].

Another area where quantum sensors can make a significant impact is navigation. The increasing use of autonomous vehicles, drones, and other mobile devices requires exact navigation systems that can provide real-time data on their location, orientation, and velocity. Conventional navigation systems, such as GPS, are limited by their accuracy and reliability, particularly in urban environments where tall buildings can obstruct signals. Quantum sensors, such as those based on superconducting quantum interference devices, have the potential to revolutionise navigation by providing exact and accurate measurements of magnetic fields, which can be used for navigation and mapping [35]. Quantum sensors also have a key role to play in healthcare, particularly in the monitoring of vital signs such as heart rate, blood pressure, and oxygen levels. Conventional sensors used in medical devices are often limited by their accuracy and stability, which can result in errors in the data collected and a lack of confidence in the results. Quantum sensors, on the other hand, can make exact measurements, even in challenging environments such as inside the human body [36]. This can lead to improved patient monitoring and diagnosis, particularly in remote or resource-limited areas where access to medical facilities is limited. Industrial monitoring is another area where quantum sensors can make a significant impact. Quantum sensors' ability to measure physical quantities with high precision and accuracy can be used to monitor industrial processes and apparatus, providing data in real-time that can be used to enhance control and efficiency. This can result in reduced downtime, increased productivity, and improved safety, particularly in areas such as oil and gas production, mining, and manufacturing [37]. By combining quantum sensors with IoT systems, it is possible to create secure communication networks that are highly resistant to cyber threats, as shown in Figure 5. This is due to the inherent security of quantum systems, which makes it extremely difficult to eavesdrop on or interfere with quantum communications. This can lead to more secure and reliable communication networks, particularly in financial transactions, critical infrastructure, and military communications. The sectors of the IoT have emerged as a result of QC due to the remarkable performance of quantum sensors in the future. Quantum sensors are progressively making their way out of the laboratory and into practical applications in the real world, as evidenced by the increasing number of startups entering this field. Their ability to harness the atomic scale and exploit exceptional coherence properties provides unmatched spatial precision and sensitivity. Despite the promise of quantum technologies in various industries, it can be challenging to gauge their potential impact. The primary focus is on two promising quantum sensing platforms: optically pumped atomic magnetometers and nitrogen-vacancy centres in diamond. A broad spectrum of potential applications, from brain imaging to single-cell spectroscopy, is exemplified through four case studies [38].

6 | QUANTUM DIGITAL MARKETING

Quantum digital marketing is a new and emerging field that combines the principles of quantum physics with traditional digital marketing strategies. This new approach aims to provide more accurate and efficient methods for targeting and reaching potential customers by using quantum algorithms to analyse data and predict consumer behaviour [39]. Quantum digital marketing leverages the principles of QC, such as quantum parallelism and quantum entanglement, to process and analyse large amounts of data at much faster speeds than classical computers. This allows for more precise predictions about consumer behaviour and the optimisation of marketing campaigns. For example, quantum algorithms can be used to analyse vast amounts of customer data and make predictions about which products or services will be most appealing to specific segments of the market by the right user at the right time with the right messages. One of the key benefits of quantum digital marketing is the ability to provide highly personalised marketing experiences to customers. With quantum algorithms, marketers can target and reach specific groups of customers with tailored messaging and content that is most likely to resonate with them. This personalisation can lead to higher conversion rates and customer engagement, as well as increased brand loyalty. Another benefit of quantum digital marketing is its ability to provide insights into customer behaviour and preferences at a much faster pace than traditional methods. With the speed and accuracy of quantum algorithms, marketers can quickly analyse and respond to changes in customer behaviour and preferences, allowing them to stay ahead of the competition.

Quantum digital marketing also has the potential to revolutionise the field of customer targeting and segmentation. Traditionally, digital marketers use demographic and behavioural data to target and segment their audiences. With quantum digital marketing, marketers can go beyond these traditional methods and use quantum algorithms to analyse and target customers based on more complex and sophisticated factors, such as emotions, motivations, and values. Despite its many benefits, as shown in Figure 6, Quantum digital marketing is still in its early stages of development and adoption. As a result, there are still many challenges and limitations that need to be overcome for it to reach its full potential. One of the main challenges is the lack of widespread understanding and expertise in QC and quantum digital marketing among marketers and businesses [40]. To effectively adopt and implement quantum digital marketing strategies, businesses must invest in training and education for their employees and partners. Quantum digital marketing has the potential to revolutionise the way businesses approach and interact with their customers. With its ability to provide highly personalised marketing experiences, faster insights into customer behaviour, and advanced targeting and segmentation capabilities, quantum digital marketing offers a new and exciting way for businesses to connect with customers and grow their brands. However, businesses must be prepared to invest in training and education to adopt and implement these strategies effectively.

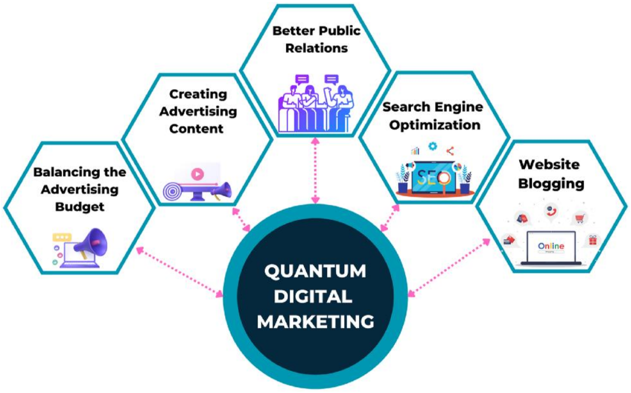
Better Public Relations
Creating Advertising Content
Search Engine Optimization
Balancing the Advertising Budget
Website Blogging
QUANTUM DIGITAL MARKETING

FIGURE 6 Future scope of quantum digital marketing.

7 | QUANTUM-SECURED SMART LOCKS

Quantum-secured smart locks are a recent development in the field of security technology, combining the principles of quantum mechanics with traditional lock and key systems [41]. These locks are designed to provide a higher level of security than conventional locks, using the unique properties of quantum mechanics to protect against tampering and unauthorised access [42]. Research in quantum-secured smart locks is focused on developing new and improved methods of using quantum mechanics to secure locks. One area of research is focused on using QKD to secure the communication between the lock and the key [43]. This involves transmitting the key information in a way that is secure against eavesdropping and tampering, ensuring that only authorised individuals can access the lock. Another area of research is focused on using quantum entanglement to enhance the security of smart locks. In this approach, the lock and key are entangled so that any attempt to tamper with the lock will destroy the entangled state, making it impossible for the lock to be opened. Using quantum physics to harness the randomness of particle behaviour to create entirely unpredictable digital keys to permit communication between devices, Quantum secured smart Lock is developing security for networked facilities and equipment. The hardware-software system interconnects all points of entry and access equipment with a central hub that encrypts all data transfers using quantum digital keys and monitors the ledger for any irregularities. Quantum-secured smart Lock takes advantage of quantum physics' intrinsic unpredictability to generate unpredictable and encrypted digital keys for securing locks, machinery, computers, and robots equipped with technologies that enable them to connect to other devices and systems via communications networks [44]. Quantum secured smart lock's goal is to improve physical security, which is increasingly intertwined with digital security. Locks and other physical equipment can be protected from local and remote cyberattacks using quantum-secured smart lock technology. Quantum eliminates this danger using secured smart Lock, which employs a QC-enabled smart lock, a smartphone, and a more secure door-opening mechanism. Some of the key benefits of using Quantum secured smart lock. Additionally, researchers are exploring using quantum random number generators (QRNGs) in smart locks. QRNGs can generate truly random numbers to encrypt and secure the communication between the lock and the key. This helps to ensure that even if a hacker can intercept the communication, they would not be able to crack the encryption and access the lock [45].

One of the significant challenges in the field of quantum-secured smart locks is the development of reliable and scalable quantum technologies. Currently, quantum technologies are still in their infancy and can be prone to errors and inaccuracies. However, with ongoing research and development, it is expected that these issues will be addressed, leading to the widespread adoption of quantum-secured smart locks in the future.

Quantum-secured smart locks are a promising new development in the field of security technology, offering a higher level of security than traditional locks as shown in Figure 7. Research in this area is focused on developing new and improved methods of using quantum mechanics to secure locks, including QKD, quantum entanglement, and QRNGs. Although there are still challenges to overcome, the future of quantum-secured smart locks looks bright, and it is expected that this technology will play an increasingly important role in securing homes, businesses, and other valuable assets.

8 | CHALLENGES AND FUTURE RESEARCH

In this article, we covered some of the most important aspects of QC. Its uses may be found in many different industries. Quantum algorithms serve to increase security and provide exponentially faster functionality. One such area is ML, where conventional ML algorithms have been improved using quantum algorithms. We have also looked at how quantum computers have affected the cryptography sector. It has been shown that quantum computers can break the present public-key encryption methods. So, it becomes essential to develop new, secure technologies for the post-quantum future. Based on the underlying mathematical problem, we can classify the post-quantum era's constructed systems into various categories. Quantum cryptography appears to be a potential solution to this problem. QKD offers a possibly safe information-based method. All of these distinct algorithms, meanwhile, are ultimately meaningless without the proper hardware to support them. When developing quantum hardware, the decoherence of Q-bits is a significant problem. When a Q-bit loses coherence due to interaction with the environment, it may be determined that it has become an overlay bit by decoding it into a regular bit (any). The circumstance now favours weight loss in a significant way. Because it is challenging to do the mapping with few errors and at a cheap cost owing to variables such as the quantity of Controlled-X gates and the particular Q-bit-tuple in the technology, it is suggested that the availability of Q-bits in the existing quantum devices is another vital test. These are common challenges involved in developing hardware based on quantum mechanics. For instance, increasing the accuracy of entanglement with drones requires incorporating a quantum node into a tiny drone. Over conventional networks, data is sent in packets. These packets may be duplicated and transmitted again if there is a loss. Due to the no-cloning claim and the postulate of quantum state measurement, it is difficult to replicate or amplify Q-bits in quantum communication. Challenges in harnessing QC for IoT and artificial intelligence (AI) applications are multifaceted. Firstly, developing quantum algorithms that can efficiently process the vast amount of data generated by IoT devices and enhance AI capabilities remains a formidable task. Additionally, integrating QC with existing IoT infrastructure, which relies on classical technologies, poses interoperability challenges. Quantum hardware limitations, such as error rates in quantum bits (qubits) and the need for error-correcting codes, further complicate the practical implementation. Future research should focus on designing quantum algorithms tailored to IoT and AI tasks, improving quantum error correction techniques and exploring hybrid quantum-classical architectures. Furthermore, addressing security concerns arising from the potential for quantum attacks on IoT networks and AI systems is paramount. Overall, the convergence of QC, IoT, and AI presents exciting opportunities, but it demands innovative solutions to overcome substantial technical and security obstacles.

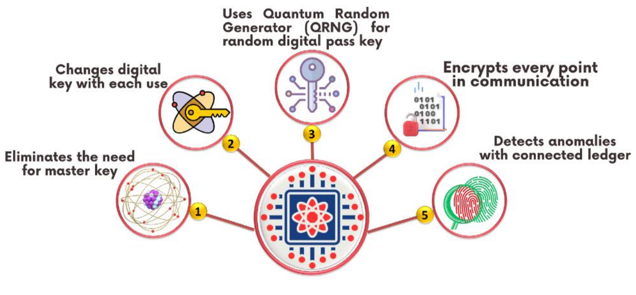
Uses Quantum Random Generator (QRNG) for random digital pass key
Changes digital key with each use
Encrypts every point in communication
Eliminates the need for master key
Detects anomalies with connected ledger
1
2
3
4
5

FIGURE 7 Key benefits of using quantum secured smart lock.

9 | CONCLUSION

Combining computer science, mathematics, and physics, QC is a fascinating field of research. Quantum-based IoT has the potential to significantly influence how we live our lives, whether via improvements to ML, logistic optimisation or financial risk analysis. It can answer some of the most challenging problems that contemporary supercomputers cannot handle. Although they will not replace current computers, quantum computer's ability to handle complex issues may unlock a hitherto unexplored field of knowledge. Better cryptography and quantum simulation are only some intriguing uses for this concept. The production of the necessary hardware alone might cost up to billions of dollars, which renders the commercial usage of this technology impracticable at present. As a direct consequence of this, it is currently solely put to use for research purposes. Once the technology is portable and reasonably priced for the average consumer to use, the world of IoT will move into a new phase. Higher-level layers may decentralise device communications and data sharing, while lower-level layers (the perception/physical layer) may permit centralisation for local networks. Not to mention, its design may help address difficulties with security, network, storage, and computing.

AUTHOR CONTRIBUTIONS

Mritunjay Shall Peelam: Writing – original draft, figures, and tables. **Anjaney Asreet Rout**: Writing – original draft. **Vinay Chamola**: Verified and checked complete manuscript.

ACKNOWLEDGEMENTS

The authors have not received funding from any of the sources.

CONFLICT OF INTEREST STATEMENT

The work is not submitted in any other journal. There is no conflict of interest.

DATA AVAILABILITY STATEMENT

The data set generated and/or analysed during the current study is available upon reasonable request from the corresponding author. However, data sets are available as an open source.

PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None.

ORCID

Vinay Chamola https://orcid.org/0000-0002-6730-3060

REFERENCES

1. Georgios, L., Kerstin, S., Theofylaktos, A.: Internet of things in the context of Industry 4.0: an overview (2019)
2. Hassija, V., et al.: Present landscape of quantum computing. IET Quant. Commun. 1(2), 42–48 (2020). https://doi.org/10.1049/iet-qtc.2020.0027
3. Dohr, A., et al.: The internet of things for ambient assisted living. In: 2010 Seventh International Conference on Information Technology: New Generations, pp. 804–809. IEEE (2010)
4. Shaikh, F.K., Zeadally, S., Exposito, E.: Enabling technologies for green internet of things. IEEE Syst. J. 11(2), 983–994 (2015). https://doi.org/10.1109/jsyst.2015.2415194
5. Hassija, V., et al.: A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7, 82721–82743 (2019). https://doi.org/10.1109/access.2019.2924045
6. Peelam, M.S., Johari, R.: Enhancing security using quantum computing (ESUQC). In: Machine Learning, Advances in Computing, Renewable Energy and Communication: Proceedings of MARC 2020, pp. 227–235. Springer (2022)
7. Schuld, M., Sinayskiy, I., Petruccione, F.: Quantum computing for pattern classification. In: PRICAI 2014: Trends in Artificial Intelligence: 13th Pacific Rim International Conference on Artificial Intelligence, Gold Coast, QLD, Australia, December 1-5, 2014. Proceedings 13. pp. 208–220. Springer (2014)
8. Javaid, M., et al.: Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability. Sustain. Oper. Comput. 3, 203–217 (2022). https://doi.org/10.1016/j.susoc.2022.01.008
9. AlGumaei, K., et al.: A survey of internet of things and big data integrated solutions for Industrie 4.0. In: 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), vol. 1, pp. 1417–1424. IEEE (2018)
10. Chalapathi, G.S.S., et al.: Industrial internet of things (IIoT) applications of edge and fog computing: a review and future directions. In: Fog/Edge Computing for Security, Privacy, and Applications, pp. 293–325 (2021)
11. Ghorpade, S.N., et al.: A novel enhanced quantum PSO for optimal network configuration in heterogeneous industrial IoT. IEEE Access 9, 134022–134036 (2021). https://doi.org/10.1109/access.2021.3115026
12. Kaur, A., Bhatia, M.: Smart classroom: a review and research agenda. IEEE Trans. Eng. Manag., 1–17 (2022). https://doi.org/10.1109/tem.2022.3176477
13. Chamola, V., et al.: Information security in the post quantum era for 5G and beyond networks: threats to existing cryptography, and post-quantum cryptography. Comput. Commun. 176, 99–118 (2021). https://doi.org/10.1016/j.comcom.2021.05.019
14. Bhatia, M., Sood, S.K.: Quantum computing-inspired network optimization for IoT applications. IEEE Internet Things J. 7(6), 5590–5598 (2020). https://doi.org/10.1109/jiot.2020.2979887
15. O'Gorman, B., et al.: Compiling planning into quantum optimization problems: a comparative study. In: Constraint Satisfaction Techniques for Planning and Scheduling Problems (COPLAS-15), pp. 11 (2015)
16. Domino, K., et al.: Quadratic and higher-order unconstrained binary optimization of railway rescheduling for quantum computing. Quant. Inf. Process. 21(9), 337 (2022). https://doi.org/10.1007/s11128-022-03670-y
17. Vista, F., Iacovelli, G., Grieco, L.A.: Hybrid quantum-classical scheduling optimization in UAV-enabled IoT networks. Quant. Inf. Process. 22(1), 47 (2023). https://doi.org/10.1007/s11128-022-03805-1
18. Krishna, G., Saha, A.K.: Optimal sensor spacing in IoT network based on quantum computing technology. Int. J. Parallel, Emergent Distributed Syst. 38(1), 58–84 (2023). https://doi.org/10.1080/17445760.2022.2126975
19. Chen, L., et al.: A novel offloading approach of IoT user perception task based on quantum behavior particle swarm optimization. Future Generat. Comput. Syst. 141, 577–594 (2023). https://doi.org/10.1016/j.future.2022.12.016
20. Ngoenriang, N., et al.: DQC2O: distributed quantum computing for collaborative optimization in future networks. IEEE Commun. Mag. 61(5), 188–194 (2023). https://doi.org/10.1109/mcom.003.2200573
21. Chakraborty, K., et al.: Hybrid PUF: a novel way to enhance the security of classical PUFs. arXiv preprint arXiv:211009469 (2021)
22. Yannuzzi, M., et al.: Key ingredients in an IoT recipe: fog computing, cloud computing, and more fog computing. In: 2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), pp. 325–329. IEEE (2014)
23. Bhatt, A.P., Sharma, A.: Quantum cryptography for internet of things security. J. Electron. Sci. Technol. 17(3), 213–220 (2019)
24. Wittek, P.: Quantum Machine Learning: What Quantum Computing Means to Data Mining. Academic Press (2014)
25. Cheruvu, S., et al.: IoT frameworks and complexity. In: Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment, pp. 23–148 (2020)
26. Tosh, D., et al.: Towards security of cyber-physical systems using quantum computing algorithms. In: 2020 IEEE 15th International Conference of System of Systems Engineering (SoSE), pp. 313–320. IEEE (2020)
27. Bagherian, M., et al.: Classical and quantum compression for edge computing: the ubiquitous data dimensionality reduction. Computing 105(7), 1–47 (2023). https://doi.org/10.1007/s00607-023-01154-0
28. Lohachab, A., Karambir, B.: Critical analysis of DDOS—an emerging security threat over IoT networks. J. Commun. Inf. Networks 3, 57–78 (2018). https://doi.org/10.1007/s41650-018-0022-5
29. Siddiqi, M.A., et al.: Improving the security of the IEEE 802.15. 6 standard for medical bans. IEEE Access 10, 62953–62975 (2022). https://doi.org/10.1109/access.2022.3181630
30. Singh, A., et al.: Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions. IEEE Commun. Surv. Tutorials 23(4), 2218–2247 (2021). https://doi.org/10.1109/comst.2021.3109944
31. Szymanski, T.H.: The "cyber security via determinism" paradigm for a quantum safe zero trust deterministic internet of things (IoT). IEEE Access 10, 45893–45930 (2022). https://doi.org/10.1109/access.2022.3169137
32. FernándezCaramés, T.M.: From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the internet of things. IEEE Internet Things J. 7(7), 6457–6480 (2019). https://doi.org/10.1109/jiot.2019.2958788
33. Passian, A., et al.: The concept of a quantum edge simulator: edge computing and sensing in the quantum era. Sensors 23(1), 115 (2023). https://doi.org/10.3390/s23010115

34. Jiang, J., Moallem, M., Zheng, Y.: An intelligent IoT-enabled lighting system for energy-efficient crop production. J. Daylighting 8(1), 86–99 (2021). https://doi.org/10.15627/jd.2021.6
35. Hathaway, H.J., et al.: Detection of breast cancer cells using targeted magnetic nanoparticles and ultra-sensitive magnetic field sensors. Breast Cancer Res. 13(5), 1–13 (2011). https://doi.org/10.1186/bcr3050
36. Quantum sensors in '23: best 8 use cases case studies. https://research.aimultiple.com/quantum-sensors/. Accessed 25 Sept 2023
37. Sureshkumar, P., Rajesh, R.: The analysis of different types of IoT sensors and security trend as quantum chip for smart city management. IOSR J. Bus. Manag. 20(1), 55–60 (2018)
38. Aslam, N., et al.: Quantum sensors for biomedical applications. Nat. Rev. Phys. 5(3), 157–169 (2023). https://doi.org/10.1038/s42254-023-00558-3
39. Story, A.C.: Recruit communications: applying quantum computing to digital marketing, 1–2 (2021)
40. Jaiwant, S.V.: The changing role of marketing: Industry 5.0-the game changer. In: Transformation for Sustainable Business and Management Practices: Exploring the Spectrum of Industry 5.0, pp. 187–202. Emerald Publishing Limited (2023)
41. Fröhlich, B., et al.: Long-distance quantum key distribution secure against coherent attacks. Optica 4(1), 163–167 (2017). https://doi.org/10.1364/optica.4.000163
42. Kumar, A., et al.: Futuristic view of the internet of quantum drones: review, challenges and research agenda. Veh. Commun. 36, 100487 (2022). https://doi.org/10.1016/j.vehcom.2022.100487
43. Xu, F., et al.: Secure quantum key distribution with realistic devices. Rev. Mod. Phys. 92(2), 025002 (2020). https://doi.org/10.1103/revmodphys.92.025002
44. Zhu, H.T., et al.: Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking. Phys. Rev. Lett. 130(3), 030801 (2023). https://doi.org/10.1103/physrevlett.130.030801
45. Kotler, S., et al.: Single-ion quantum lock-in amplifier. Nature 473(7345), 61–65 (2011). https://doi.org/10.1038/nature10010

How to cite this article: Peelam, M.S., Rout, A.A., Chamola, V.: Quantum computing applications for Internet of Things. IET Quant. Comm. 5(2), 103–112 (2024). https://doi.org/10.1049/qtc2.12079