IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 11, 2021, accepted August 31, 2021, date of publication September 1, 2021, date of current version September 17, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3109816

Survey of Promising Technologies for Quantum Drones and Networks

ADARSH KUMAR[1], SURBHI BHATIA[2], KESHAV KAUSHIK[1], S. MANJULA GANDHI[3], S. GAYATHRI DEVI[3], AND DIEGO A. DE J. PACHECO[4], AND ARWA MASHAT[5]

[1]Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India
[2]Department of Information Systems, College of Computer Science and Information Technology, King Faisal University, Hofuf 31982, Saudi Arabia
[3]Department of Computing, Coimbatore Institute of Technology, Coimbatore, Tamil Nadu 641014, India
[4]Department of Business and Technology, Aarhus University, 8000 Aarhus, Denmark
[5]Department of Information Systems, College of Computing and Information Technology, King Abdulaziz University, Rabigh 25732, Saudi Arabia

Corresponding author: Adarsh Kumar (adarsh.kumar@ddn.upes.ac.in)

ABSTRACT Due to recent advancements in quantum drones, the Internet of Quantum Drones (IoQDs), and Drone-to-Satellite connectivity, several advantages have been anticipated for real-time applications. This work examines quantum computing issues, including quantum data processing, techniques, circuits, and algorithms important for quantum drones or their networks. Here, we discussed the current research trends on quantum computing, quantum-safe computing, or post-quantum cryptography important to quantum networks, followed by the numerous advantages, limitations, future advancements, and research issues connected with quantum technologies, drones, and their network. This work has also prepared a taxonomy of quantum-related areas depending upon the logic of their learning, followed by a review of each of these areas. We review the most recent work over quantum algorithms used in various-quantum-related areas and networks, the role of quantum satellites for drone-based networks and communications, how quantum artificial intelligence and quantum machine learning are important for quantum drones, networks and futuristic applications, quantum attacks, quantum genetic algorithms, and the importance of post-quantum and quantum-safe cryptography. The challenges and research directions in these domains are explored as well. Lastly, this work presents an overview of the current state of knowledge in various promising technologies that are recently found to be important for quantum drones and networks.

INDEX TERMS Constellation of drones, post-quantum cryptography, quantum algorithms, quantum architecture, quantum cryptography, quantum drones, satellites.

ACRONYMS

Acronym	Explanation
5G	Fifth Generation.
AI	Artificial Intelligence.
ALA	Algebra Linear Algorithms.
APP	Antenna Positioning Problem.
AQM	Adaptive Quantum Mutation.
BSM	Bell State Measurement.
CFS	Courtois, Finiasz, and Sendrier.
CQC	Component Quantum Computation.
DF	Decode and Forward.
DLP	Discrete Logarithm Problem.
ECC	Elliptic Curve Cryptography.
ECDLP	Elliptic Curve Discrete Logarithm Problem.
ES	Entanglement Swapping.
ESA	European Space Agency.
FANETs	Flying Ad-Hoc Networks.
FTQC	Fault Tolerant Quantum Computing.
GIS	Geographic Information System.
HAS	Hamiltonian Simulation Algorithm.
HMM	Hidden Markov Models.
HSTN	Heterogeneous Satellite Terrestrial Networks.
HSTRN	Hybrid Satellite Terrestrial Relay Networks.
HUP	Heisenberg Uncertainty Principle.
IFP	Integer Factorization Problem.
IIR	Infinite Impulse Response.
IoD	Internet of Drones.
IoT	Internet of Things.
IoQD	Internet of Quantum Drones.
LMSS	Leighton Micali Signature Scheme.
LWE	Learning With Error.

The associate editor coordinating the review of this manuscript and approving it for publication was Jiankang Zhang.

ME	Multi-granularity Evolution mechanism.
MEQGA	Multi-granularity Evolution based Quantum Genetic Algorithm.
ML	Machine Learning.
Mo-QIGA	Multi-objective Quantum Inspired Genetic Algorithm.
MSS	Merkle Signature Schemes.
NAI	Node Availability Index.
NISQ	Noisy Intermediate-Scale Quantum.
PLS	Physical Layer Security.
PQAs	Post- Quantum Algorithms.
PQC	Post-quantum Cryptography.
QAI	Quantum Artificial Intelligence.
QAOA	Quantum Approximate Optimization Algorithm.
Q-Bit	Quantum Bit.
QC	Quantum Cryptography.
QEA	Quantum Evolutionary Algorithm.
QEC	Quantum Error Correction.
QFA	Quantum Finite Automata.
QFSA	Quantum Fourier Sampling Algorithm.
QFT	Quantum Fourier Transformation.
Q-ISTAR	Quantum Intelligence Surveillance, and Target Acquisition and Reconnaissance.
QIA	Quantum Insertion Attack.
QIT	Quantum Information Technology.
QKD	Quantum Key Distribution.
QML	Quantum Machine Learning.
QoS	Quality of Service.
QPE	Quantum Phase Estimation.
QR	Quantum Repeater.
QRCS	Quantum Radar Cross Section.
QSeS	Quantum Secret Sharing.
QTM	Quantum Trajectories Method.
QUBO	Quadratic Unconstrained Binary Optimization.
QUICs	Quantum Interconnections.
RSA	Rivest-Shamir-Adleman.
SDS	Sequential Diagnostic Strategy.
SDN	Software Defined Networking.
SE	Single-granularity evolution mechanism.
SSL	Secure Sockets Layer.
TLS	Transport Layer Security.
VQE	Variational Quantum Eigensolver.
QGIS	Quantum Geographic Information System.
UAV	Unmanned Aerial Vehicle.
USV	Unmanned Surface Vessel.
UUV	Unmanned Underwater Vehicles.
WDM	Wavelength Division Multiplexing.

I. INTRODUCTION

Integration of quantum computing or technology, AI, drones, and security aspects will yield many applications in the future. Quantum sensors integrated with drones or UAVs, USVs, or UUV can be helpful in various applications like collision detections in delivery-based systems, human-made structures (e.g., tunnel or underground living places), surface albedo and spectral measurements, and many more [1]–[4]. Further, drones can be used for distributing quantum keys as well [5]. Drones are preferred for key distribution between two reconfigurable entities. Here, drones can act as a trusted party and help any two moveable or re-orient entities retrieve the key. Robotics autonomy is another important area in which experimentations are performed using quantum entanglement and QC [6]. Additionally, cooperative tasks of robotic systems are other experimental work that is important for many applications. For example, various experiments are performed to make the quantum internet a reality. In these experimentations, two or three quantum devices are used so far. It is expected that the quantum devices' connectivity will increase with an increase in quantum networks to ensure internet services.

Quantum radars, sensors, and other objects can be integrated with drones or aircraft that can be useful in real-time applications. Cartlidge [7] discussed the lightweight gravimeter sensor (named ''wee-g'') using quantum technology. These sensors help track humans, tunnels, or various other objects. Thus, the feasibility of the quantum field with domain has made the exploration of those things which are either difficult to access or lies in remote areas. In [8], drone-based entanglement distribution has been experimented with over a 200 meters distance. The authors have discussed the possibilities of covering local-area coverage using low-altitude drones and wide-area ranges using high-altitude drones. Additionally, this work has experimented with all-weather entanglement distribution with less loss. In [9], the use of two quantum drones for constructing a network is discussed. This discussion emphasizes drone-based air-to-ground photon transmission compared to optical fiber-based data transmission. In an optical fiber-based system, the chances of photons losing their entanglement is higher, especially over long distances. This is because the photons bounce off the sides of fiber opticals. In [10], the advantage of quantum technology is discussed for climate change. Quantum can help in identifying new catalysts that can reduce carbon dioxide in the air, environment-friendly fertilizers, energy production, and storage. The Quantum sensor attached to the drone can be directed to a particular location for carbon dioxide capture. Likewise, many more advantages can be taken out of it. Thus, there is a need to explore quantum drones, their integration, construction of the quantum drone network, usage of quantum drones in real-time applications, quantum sensors or circuits for drones, and many more. The present studies do not discuss these aspects altogether. Further, the recent advancements, technologies, attacks in the quantum domain are explored.

In quantum computing, QC, or quantum-based robotics, few surveys are available in recent studies. For example, Bosheng *et al.* [11] surveyed nature-inspired computing. There are two types of computing in the nature-inspired computing category: quantum computing and molecular

computing. The article focuses on membrane computing at large (in molecular). The importance of quantum computing aspects or drone-based systems is not touched in-depth survey. Quantum computing is widely used in quantum image processing to capture, manipulate, and analyze quantum images in different applications [12]. In [12], the advancements in quantum image representation are discussed. These advancements show the similarities, differences, and applications in this area. Drones usage with QGIS can be used for distance learning using image processing [13]. At the University of Southern Queensland, QGIS is used to teach GIS with hands-on skills to on-campus and off-campus students. Many students found that QGIS software is helpful to have hands-on experience in learning GIS skills. In [14], drone-based aerial image collection and processing using the open-software system are discussed. This system is projected to be enhanced with drone-based air pollution monitoring frameworks and models. This work has proposed to develop a plan that integrates various other types of sensors. If the quantum sensor is attached to drones, it will be useful in climate change, one of the significant applications. With the possibilities of quantum drones [15], the application of drones and quantum computing increases for various domains. Areas like quantum-safe cryptosystem, quantum-safe security solutions, and PQC are widely discussed in security areas. Although QC and PQC are independent domains, a quantum-computing-based attack analysis is performed in both cases. For example, Prasanna *et al.* [16] surveyed lattice-based key sharing schemes in detail. This is a type of PQC. This survey discusses various lattice-based key sharing schemes, advantages, disadvantages, and attack scenarios in detail.

The lattice-based cryptosystem is an important cryptography candidate for resource-constraint devices. Thus, the feasibility of this type of cryptosystem is valuable for resource-constraint drones. This survey discusses the strongness of lattice-based systems against quantum attacks. PQC approaches suitable for quantum or classical drones are not explored in this survey to avoid quantum attacks. Thus, there is a need to study these aspects in detail. A comparative analysis of various recent surveys in the quantum and post-quantum area is presented in Table 1 [17]–[26]. This comparative analysis shows that quantum drones, satellites, network building, and a constellation of drones or networks along with quantum computing are not discussed in recent studies. There are many challenges in drone-based systems, quantum computing, quantum technologies, and quantum-drone integrated solutions in the present scenario. Some of these challenges are briefly discussed as follows [15], [27], [28].

- Many sensors can be mounted over drones and can be used in various applications. However, these sensors are sensitive and can give false predictions as well. For example, a tiny gravity sensor can detect the much smaller up-and-down motions of the earth's surface because of sun or moon movements. In contrast, the sensor is deployed over the drone to identify the drug tunnel or mineral deposits. Thus, there is a need to explore the possibilities of quantum sensors over drones that can function with fewer error probabilities.
- IoQDs are another important aspect. In IoQD, drone's collaborative efforts, the constellation of quantum drones, group strategies, and services are important aspects that need to be explored. Quantum drone is a new domain, and not many experiments are performed in this area. Thus, there is a need to develop software tools and techniques which will be helpful to simulate or implement this concept for better understanding.
- A drone can be a resourceful or resource-constrained device. In resourceful drone devices, data protection from quantum attacks is possible through quantum-safe mechanisms or PQC. Likewise, resource-constrained devices require lightweight cryptography. In PQC approaches, lattice-based and code-based cryptosystems have the solutions in lightweight cryptography for resource-constrained devices. Lightweight QFA can also ensure security states and models to protect resource-constrained devices from attacks. Thus, the analysis of quantum-safe cryptosystems or PQC is required for drones or IoQDs.

Likewise, many domains in the quantum world are yet to be explored in detail. Figure 1 shows one such quantum field and taxonomy. Various important areas in this domain are briefly explained as follows.

- *Quantum Computing and Simulation:* Quantum information science and technology are used for computational tasks in quantum computing. The machine which performs these tasks is known as a quantum computer. In [29], quantum computers are classified as digital or analog computers. Presently, quantum computers or quantum systems are used on the ground for secure communication. However, few drone and satellites experiments are conducted for space and air-based quantum computing to provide internet services and long-distance connectivity. There are three important quantum computing stages [30]. These stages are (i) CQC, (ii) NISQ Computing, and (iii) FTQC. CQC examines and tests quantum computing and then works on creating the essential quantum components. CQC's processing power is low, making it useful for demonstrations of proofs of concept, but not much more. To prove the benefits of quantum computing, the NISQ stage quantum computer will need many qubits. Researchers are expected to continue to do extensive research, which may lead to an increased quantity and quality of qubits. When a flawless logical qubit is achieved, the FTQC stage begins.

  Quantum simulations were the initial use of quantum computers and, in many respects, continue to be the most promising application today. Two important types of quantum simulation are QPE and VQE. QPE may be

TABLE 1. Comparative analysis of recent surveys over quantum or post-quantum studies.

Author	Year	A	B	C	D	E	F	G	H	I	J	Key Findings	Major Shortcomings
Shaikh and Ali [17]	2016	✓	×	×	✓	×	✓	×	✓	×	S	This work has explored the importance of quantum computing and technology in big data. Its application to healthcare is briefly touched upon.	This is more of a discussion and development work in quantum computing for big data area. This work can be extended to explore healthcare domain in-depth.
Gyongyosi et al. [18]	2019	✓	×	×	✓	✓	×	✓	✓	×	L	This work has explored the quantum technological aspects and compared it with classical computing technologies. Further, challenges and future directions in various quantum-related area are explored.	This work is largely based on existing studies and their observations. This work can be extended to explore quantum drones, satellites and other areas.
Savchuk and Fesenko [19]	2019	✓	×	×	✓	✓	×	✓	✓	×	L	This study is focused over quantum computing aspects, algorithms, developments and technologies. The research challenges in quantum hardware development and quantum computer feasibility are also discussed.	This work does not discussed the quantum attacks, cryptography, drones or satellites-based stuies. Work can be extended to study quantum design in various areas.
McGeoch et al. [20]	2019	✓	×	×	✓	✓	✓	✓	✓	×	S	This work discusses the properties of quantum computer-based on quantum annealing paradigm. Fous is drawn towards evidence-based predictions.	Quantum annealing applications are briefly described. This work can be extended to study these applications and associated challenges in detail.
Li et al. [21]	2020	✓	×	×	✓	×	✓	×	✓	×	L	This work has surveyed the quantum algorithms from optimization and learning perspectives. Experiments to compare quantum and traditional intelligent algorithms is also performed.	This work is an in-depth study over quantum algorithms. However, this work can be extended to explore the feasibility of these algorithms in specific application along with complexity calculations.
Ramezani et al. [22]	2020	✓	×	×	✓	×	✓	✓	✓	×	S	This work presented the use of machine learning algorithm in quantum computing. A comparative analysis of algorithms based on speed and complexity is performed.	This work discusses the machine learning algorithms very briefly. This work can be extended to explore the algorithms in-depth and evaluate their significance in different quantum networks.
Egger et al. [23]	2020	✓	×	×	✓	×	✓	×	✓	×	L	This work state that quantum computing may benefit issues in finance if properly used. Algorithms focuses in simulation, optimization, and machine learning problems for finance sector are identified.	This survey focuses in-depth over use of quantum algorithms in finance sector. Challenges and future directions are discussed as well. This work can be extended to identify the use of similar algorithms in other application areas.
Fernandez-Carames [24]	2020	✓	×	×	✓	✓	✓	✓	✓	✓	L	This work has discussed the pre-quantum and post-quantum security aspects, taxonomies and analysis in detail.	This work is an in-depth analysis in specific domain with lot of statistics for comparative analysis.
Fernández-Caramès et al. [25]	2020	×	×	×	✓	×	×	×	×	✓	L	This work focuses over PQC aspects and their integration with blockchain technology. A broad view of quantum attacks in PQC scenario is also discussed.	This work covers lot os statistics to discuss the importance of PQC aspects and blockchain technology integration. This work can be extended to discusses these aspects for some specific applications.
Saki et al. [26]	2021	✓	×	×	✓	×	×	✓	✓	×	M	This work provides study over quantum computer assests, programs, vulnerabilities, attacks, and other security issues. Study over vulnerabilities and possible safeguard is helpful in attack resilience.	This work has provided a theoretical discussions and developments over various security aspects. This work can be extended to have comparative analysis of statistical analysis-based security properties.

A: Quantum Computing, B: Quantum Drones, C: Quantum Satellites, D: Quantum Information Processing, E: Quantum Electronics (Registers, Gates, Circuits, Memories), F: Quantum technology-based applications for advanced technologies (like Big data, cloud computing, machine learning, artificial intelligence, serverless computing), G: Quantum Computers, H: Quantum Algorithms, I: Post-quantum Cryptography, J: Survey Type (Short(S) i.e. less than 10 pages, Medium (M) i.e. 11 to 20 pages, Long (L)).

used to calculate a quantum computing system's ground state energy. QPE is a critical subroutine in quantum computing, but it is also one of the most complex subroutines to construct. This building block, which is utilized as a fundamental building block for many quantum algorithms, can be used to measure almost any Hermitian operator. The VQE algorithm uses both conventional and quantum computers. It allows you to identify the collection of values that fulfill the optimum solution to a particular optimization problem. VQE is a quantum-classical technique that merges the best aspects of both the quantum and classical worlds. The primary goal of the endeavor is to discover the upper bound on the Hamiltonian's smallest eigenvalue.

- *Quantum Communication and Cryptography:* Quantum communication deals with the exchange of quantum information through a quantum network. In most instances, a photon is used as the quantum information carrier. To overcome the photon restrictions, quantum network components such as a quantum repeater or quantum switch are included.

QC is not hackable since it utilizes the laws of quantum physics to transmit secure communications. The important elements of QC include QKD, quantum

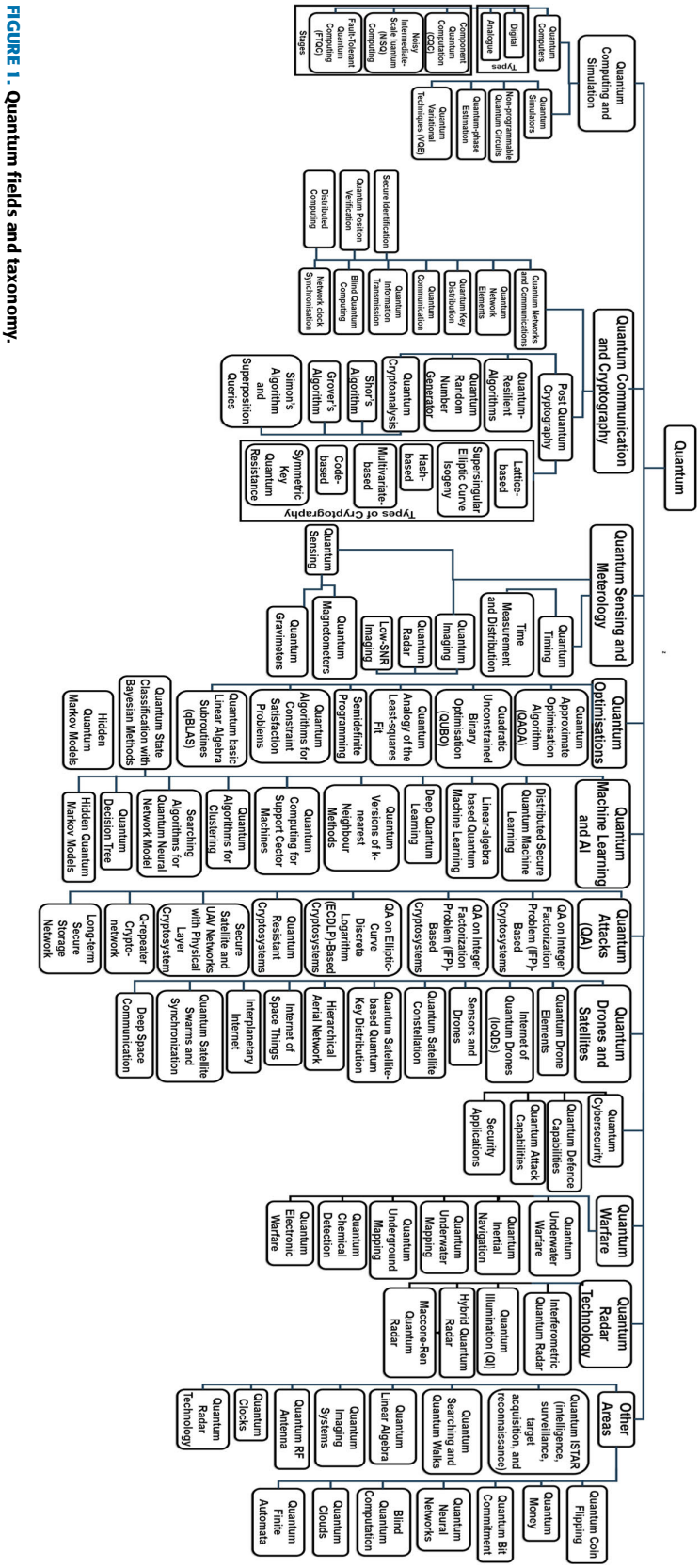

FIGURE 1. Quantum fields and taxonomy.

coin flipping, quantum commitments, bounded and noisy quantum storage, position-based QC, device-independent quantum cryptosystem, quantum entanglement, quantum uncertainty, and no-cloning theory. PQC is a cryptosystem believed to be safe against a cryptanalytic assault by a quantum computer. This can be classified as lattice-based, supersingular elliptic curve isogeny, hash-based, multivariate-based, code-based, and symmetric key quantum resistance. The other security-related concepts in PQC are quantum resilient algorithms, quantum random number generation, and quantum cryptanalysis.

- *Quantum Sensing and Meteorology:* This branch of quantum technology (i.e., Sensing and Meteorology) is farthest forward in timekeeping, sensing, or imaging. The term ''quantum sensing'' describes using a quantum system, quantum characteristics, or quantum events to measure a physical quantity. Atomic vapors and atomic clocks are historical examples of quantum sensors. Quantum sensing has quickly grown in the recent past, with the most popular platforms being spin qubits, trapped ions, and flux qubits. New possibilities, particularly concerning high sensitivity and accuracy, are anticipated in the field [31]. According to Shih [32], the objective of Quantum Imaging is to demonstrate that both the quantum mechanical characteristics of light and the fundamental and inherent parallelism of optical signals are feasible to develop new techniques for quantum information processing. This kind of research is a new subject for quantum optics and still has most of its characteristics in its infancy. A signal must be transmitted to the target, and the radar system must wait for the signal to be reflected. However, increased accuracy and additional capabilities may potentially be achieved via the quantum mechanical method. Another important component in meteorology is quantum radars. Like conventional radar systems, quantum radars send a signal transmitted to the target, and the radar system has to wait for the signal to be reflected. However, accuracy and additional capabilities may potentially be achieved via the quantum mechanical method using quantum radars.
- *Quantum Optimisations:* The potential of solving NP-level complex problems makes quantum optimization an actively studied subject. Few well-known quantum optimization algorithms include quantum data fitting (like quantum least-squares fitting), quantum semidefinite programming, quantum combinatorial optimization, quantum approximate optimization algorithm, QAOA, QUBO, the quantum analogy of the least-squares provide, semidefinite programming, quantum algorithms for constraint satisfaction problems, and quantum basic linear algebra subroutines. There are difficulties with optimization across many industries, such as production, finance, and transit. Indeed, businesses like logistics are fully engaged in addressing issue optimization. Quantum-based optimization is a viable way to address these issues. This is theoretically assumed to be the most cost-effective. In recent studies [21], [33], various quantum optimization algorithms are discussed for real-time use. In quantum optimization, powerful global search, excellent robustness, parallel computing abilities, search speed, and intelligent optimization are some of the characteristics that can optimize an algorithm.
- *QML and QAI:* Classical computers find it very difficult to tackle some problems with intricate connections between algorithm's inputs and outputs, as quantum computers can. This indicates that quantum computer learning models may be more potent in specific applications, perhaps with quicker calculation, greater generalization on less, or both. So, in which cases such a ''quantum advantage'' might be obtained, it is of high importance to understand. QAI uses quantum computing for machine learning algorithm computation. Quantum computing has significant processing benefits that allow QAI to out-perform conventional computers in ''quantum advantage''. It is plausible to assume that quantum computers may be better at machine learning tasks than traditional computers, given that quantum systems display counter-intuitive patterns [34], [35]. Biamonte *et al.* [34] discuss the importance of QML-from system design, optimization algorithms, and deep quantum learning perspectives. Further, the importance of quantum computing to quantum data processing is also explored.
- *Quantum Attacks:* Security primitives and protocols must be thoroughly examined, given the impending development of quantum computing. Intractable computational issues are intensively studied and widely discussed quantum algorithms.
- *Quantum Drones and Satellites:* In recent years, various developments have been observed in this area [15], [36]. Choi [36] discussed the first ''quantum drone'' developed for impenetrable air-to-ground data communication. Schirber [15] discussed a kilometer-long prototype of a drone-based quantum network that successfully sent a quantum signal. This experiment shows that quantum communication can ensure secure message exchange. Here, two users can share a pair of entangled photons with a unique mechanical relationship. Optical fibers are the viable option to send these photons. Schirber [15] discussed the major challenges and shortcomings in this area as well. In [37], [38], quantum satellites-based experimentations are discussed. QKD distribution using quantum satellites in less time or at fast speed experiments. Likewise, multimedia communications (audio, video, and text) using quantum satellites have also been experimented with in recent times, and it is expected to be the future.
- *Quantum Cybersecurity:* Quantum cybersecurity deals with quantum defense capabilities, quantum attack capabilities, and security applications [29]. Quantum

attacks are broadly classified into three major categories, including ECDLP, DLP, and IFP. Additionally, QIAs in classical cryptosystems, quantum-resistant cryptosystem, satellite, and UAV-based secure communication, Q-repeater crypto network, and quantum-safe infrastructure in fiber and wireless networks are some of the important areas considered in recent studies [25], [39]–[45]. Abellan and Pruneri [46] discussed other dimensions in the quantum cybersecurity area, including quantum random number generator, its importance to applications, and association with encryption and decryption processes.

- *Quantum Warfare:* In [29], various areas of quantum warfare are discussed in addition to quantum communication and computing. These areas include (i) network building for quantum inertial navigation and integration with quantum underwater warfare, (ii) quantum internet, (iii) quantum cybersecurity warfare, (iv) quantum computing-based applications, (v) design and development of advanced quantum computers, (vi) satellite-based quantum communications, (vii) quantum radar systems, (viii) quantum electronic, (ix) quantum chemical detection, (x) quantum-based tunnel and object detection, and (xi) quantum chemical and biological simulations. All of these areas are explored in different recent studies in detail.
- *Quantum Radar Technology:* Quantum radar technology is widely used in various disciplines, including target detection, object identification, operate in areas having high background noise, easily detect and filter out deliberate jamming attempts, a potential anti-stealth technology, and many more. Daum [47] discusses quantum RADAR's cost and practical issues compared to classical radars. In important findings, it has been observed that quantum radars are helpful in medical imaging, identifying stealthy targets in clutter, jamming, or chaff, and produce pure noise waveforms. Fang [48] presented the simulation and analysis work for the QRCS. This work detects 2D or 3D targets, and the QRCS approach is helpful in simulation. This work is found to be extended for determining the diffraction effects and verification of experiments. Salmanogli and Gokcen [49] conducted experimentation to improve entanglement sustainability. Quantum entanglement is an important concept in QKD or object detection. Likewise, many application uses quantum entanglement for their purposes. In this experiment, it has been observed that some degrees of freedom are available to enhance the entanglement. Improvements are possible in coupling factor, retainment, and returned fields of quantum entanglement.
- *Other Areas:* Among other areas, Quantum clocks, quantum radar, quantum antenna, quantum imaging, quantum search, and quantum walks, Q-ISTAR are important and valuable and can be explored in the future.

The objectives of this work are:

- To list and compare the importance of quantum computing approaches in drones network. Here, those quantum computing algorithms and architectures that make drone-based communication and services secure and faster are analyzed and compared in-depth.
- To identify and analyze the importance of quantum satellite and quantum drone-based integrated systems for different applications. With the success of quantum satellites, quantum drones, and their integrated system, their applications to real-time and futuristic scenarios are massive. Thus, the aim is to explore these approaches and associated research challenges.
- To analyze the importance of quantum drones with AI and machine learning techniques.
- To study the severity of quantum attacks to classical or lightweight cryptography-based cryptosystems. These attacks can affect drone-based systems, which are dependent on traditional security approaches for their services. Thus, the aim is to explore the impacts of these attacks in drone-based systems.
- To study the PQC and/or quantum-safe cryptosystems that can secure futuristic scenarios. Here, the aim is to analyze those aspects as well that make PQC integration with drones.

This work is organized as follows. Section II discusses quantum computations' power, the feasibility of integrating quantum computing features with a drone-based system, quantum algorithms useful for drone networks, security issues in drone-based networks, and futuristic research challenges. Section III presents the importance of quantum satellites in space. Here, the constellation of quantum satellites for futuristic applications is discussed. Section IV presents the integration of quantum drones with AI and machine learning approaches. This integration can lead to many futuristic applications. Thus, these technologies, their integration, and research challenges are discussed in detail. Section V presents the severity of quantum attacks to classical cryptosystems and real-time applications. Section VI discusses the importance of PQC in securing futuristic applications from quantum attacks. Section VII presents the recently discussed PQC approaches and developments. Section VIII presents the importance of QFA for drones and small devices. Section IX shows the futuristic research challenges in quantum drones and associated quantum computing areas. Finally, the conclusion is drawn in section IX.

II. DRONE-BASED QUANTUM COMPUTING

Scientists in China and Europe are developing quantum satellite networks, which enable satellite-to-ground long-distance connections [50]. There are, however, several drawbacks to quantum satellites. These include: low-orbit satellites can only communicate with certain soil sites in a specific time frame, and space launch costs make it very expensive to set up a quantum satellite network. They eventually aim to develop a global quantum internet-based

TABLE 2. Differences between classical and quantum computing.

Classical computing	Quantum computing
Calculates with transistors, which can represent either 0 and 1	Calculates with qubits, which can denote 0 and 1 at the same time
Power increases in a 1:1 relationship with the number of transistors	Power increases exponentially in proportion to the number of qubits
Computers can operate at room temperature with low error rate	Computers have high error rates and need to be kept ultracold
Most everyday processing is best handled by classical computers	Well suited for tasks like optimization problems, data analysis, and simulations

on quantum particles transmission and enabling ultrasecure communications to create secret codes for encrypting messages using particles. A quantum web could also make it possible for remote quantum computers to work together or experiment in the limits of quantum physics. The use of fiber-optical cable quantum networks and the transmission of photons by a quantum satellite across China are already started. The advantages of being easily movable and relatively easier-to-use and cheap-to-use drones could serve as another technology.

Nanjing University scientists in China have designed a 'quantum drone' to be an airborne node in a quantum network, highlighted by the recent explosion advances in drone technology. ''It has been used as a node and built the first quantum drone similar to the quantum satellites used,'' explained the quantum scientist Dmytro Vasylyev, who was not involved in this research at the University of Rostock in Germany. ''Drones can be deployed in any given time and place for a mobile quantum connection,'' said Zhenda Xie of the University of Nanjing and one of the research team members. Drones can be repositioned easily to prevent fog or pollution. They can also be cheaper and more agile than satellite quantum systems, so that we have to concentrate on drone-based quantum technology research. This section describes the difference between classic and quantum computers, quantum algorithms and architectures, challenges of drone-based quantum computing, challenges of quantum-safe security, and vulnerable quantum cryptography.

A. CLASSIC AND QUANTUM COMPUTATION

The traditional computer stores all information as either 1 or 0 on a memory device (binary system). Due to this logic, classic computers solve specific problems with additional resources. The next level of computers that use quantum theory principles for problem resolution is Quantum Computers. A qubit is a basic unit for the quantum computer. These types of computers allow the efficiency to exhibit many logical conditions simultaneously, such as superposition and interposition [51]. A qubit is 0 or 1 or a mixture or overlay in either state, whereas a binary bit can be considered only 0 or 1 [52]. Quantum computers and bit developments have been directed towards quantum technology, like quantum recreations, correspondence, calculation, climate, and sensors. Superposition and ensnarement are utilized in these advancements by tending to and controlling quantum states [53]. Just as 'classical', It depends on the foundation of interconnected QIT frameworks. One of the essential components of these frameworks is the ''interconnect,'' a gadget or method for transferring data among various physical media such as electronic semiconductors, individual atoms, optical fiber light pulses, or microwave fields. Although the interconnections in traditional information technology have been well developed over decades, QUICs are particularly challenging because they should empower the transmission of delicate quantum states between actual parts or levels of framework opportunity. Additional challenges are associated with the variety of QIT platforms (superconducting, atomic, the center of color, optical, and so on) that structure a ''Quantum Internet''. Table 2 lists the difference between classical and quantum computing environments.

B. QUANTUM ALGORITHMS

Quantum algorithms are designed with completely different principles than traditional algorithms. Even standard algorithms, like reversible algorithms, must be cast first before being operated on a quantum computer. Quantum speed algorithms utilize specific quantum algorithms or building blocks that are not classical. Progress in quantum algorithms is critical to the success of quantum computation. The QFT, QFSA, HAS, and ALA is the primary building blocks for quantum algorithms. Typically, there are n-classical bits inputs to a quantum algorithm and standard n-bits output. With the information of n-bits x string, the quantum computer takes n-qubits in state $|x\rangle$ as an entry. After that, several quantum actions are carried out. These actions convert the state of the n-qubits to some overlap $\sum_y \propto_y |y\rangle$. Lastly, the result is the n-bit string 'y' with a probability $\left|\propto_y\right|^2$. This is the final measurement, and it is a random output. Thus, there are three things to note in quantum computers: quantum state, gates, and measurement results. A comparative analysis of these three things with a classical computer is shown in Figure 2.

At the beginning of the 1990s, there were just several significant quantum algorithms like Grover and Shor [54]. The variation quantum algorithm, based on both quantic and classic component combinations, is the most widely used among these. VQE algorithms showed excellent results

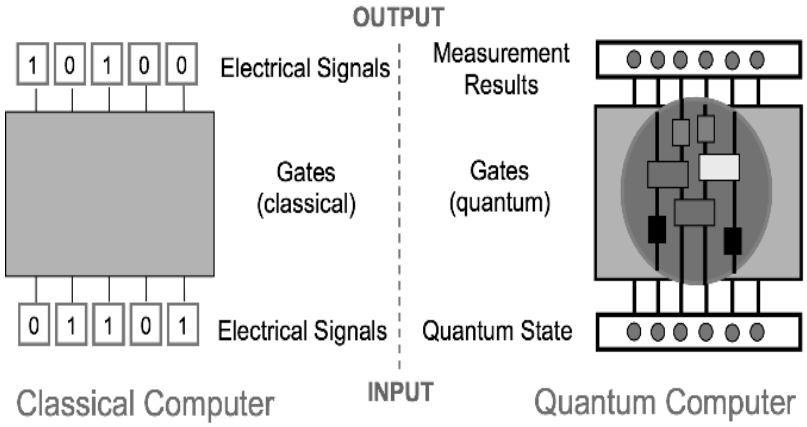

FIGURE 2. Classical computer and quantum computer's input and output.

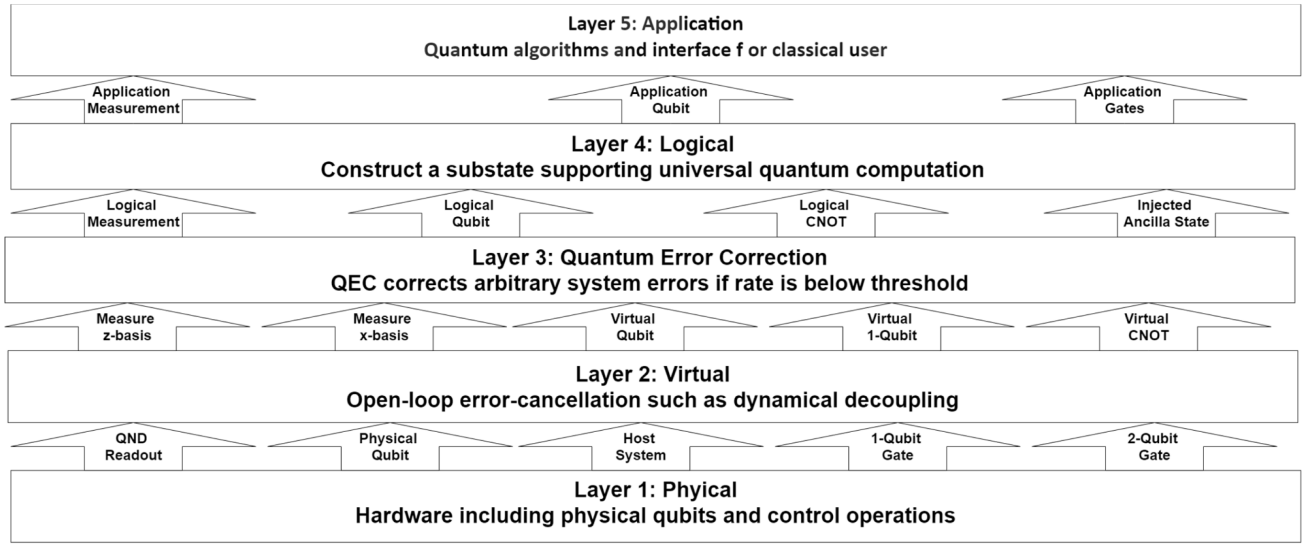

FIGURE 3. Layered architecture of quantum-computer.

for quantitative and quantum chemistry issues, machine learning issues on NISQ devices. Algebraic (like discrete or matrix verification products), searching (such as Grover and amplitude amplifies), and variation (like approximate quantum optimization) are undoubtedly other important quantum algorithm categories. The quantum internet has scattered quantum nodes separated by various distances over which a quantum communication protocol can be used, such as distributed quantum calculation or distributed sensing. Here, many quantum communications and cryptographic protocols are available, with encryption distribution [55], random number beacon and personal devices number generation, secrecy sharing [56], quantum fingerprinting [57], etc. The ''blind'' quantic calculation [58] is of particular relevance. A distant user can program a quantum computer with a certain level of interference to his owners without revealing the algorithm or computational results and the distributed quantum processing. Table 3 lists some of the quantum algorithms and their applications.

C. QUANTUM ARCHITECTURES

Many different quantum computer technologies undergo experimental research [59], but an open-ended research problem remains for each of these scalable systems architectures. Scalable systems architecture introduces DiVincenzo Criteria for sustainable quantum-computing expertise [60]. Further, Steane underlined the struggle of adequately developing systems that can correct quantic errors [61], [62]. Different additional taxonomies were outlined to address large-scale systems' architectural needs [63], [64]. Small interconnections were proposed for many technologies, but only a few researchers have addressed the difficulties of organizing subsystems using these technologies into the complete large-scale system architecture. In particular, relatively little attention has been paid to heterogeneity in system construction. Figure 3 illustrates a quantum design with a layered architecture, yet the specific interfaces between layers fluctuate contingent upon actual equipment, quantum mistake revision plot, and many more [65]. The application

TABLE 3. Comparative analysis of quantum algorithms used in various areas.

Author	Year	A		B	C			D	E	Applied Area	Key Findings
		a	b		c	d	e				
Shi et al. [75]	2020	-	-	-	-	-	X			Nondeterministic polynomial problem	With the scale of the system, the adiabatic quantum algorithm grows exponentially. Finding the best Computation Time T_E in the diabatic regime for a single evolution time.
Elaziz et al. [76]	2021	-	-	-	-	-	-	-	X	Multilevel image segmentation	The proposed strategy for improving the Marine Predators Algorithm using Quantum Theory is a global optimization method.
Hosoyamada et al. [77]	2020	-	-	-	-	-	-	X	-	Multicollisions in cryptography	The ℓ-collisions may be formed using only $O(N^{1/2})$ quantum inquiries for any integer constant ℓ. It then gives a quantum technique for finding a ℓ-collision for a random function that has an average quantum query complexity of $O(N^{(2^\ell-1)/(2^\ell-1)})$.
Mojrian et.al [78]	2021	-	-	-	-	-	-	-	X	Automatic text summarization systems	Processing stage employs a modified quantum-inspired genetic algorithm (QIGA).
Yuxing Wang et al. [79]	2021	-	-	-	-	-	-	-	X	Configurations of building with the low construction cost and low energy consumption to green building.	The quantum genetic algorithm optimises the configuration of the office building envelope at the required ENVLOAD (energy load of the building envelope) value.
Kaveh et.al [80]	2021	-	-	-	-	X	-	-	-	Optimization algorithm improvement	The Teaching-Learning-Based Optimization (TLBO) technique is enhanced by using the formulation gained from solving the time-independent Schrodinger equation to anticipate the likely placements of optimal solutions. By defining the quantum teacher phase, Quantum Teaching- Learning-Based Optimization improves the TLBO's stability and robustness.
Ding et al. [81]	2021	-	-	-	-	-	-	-	X	To tackle the big data challenge and to achieve exponential speedup for least squares SVM (LS-SVM).	For sampling the kernel matrix and classifying, an improved fast sampling technique, termed indirect sampling, is given. The LS-SVM with a linear kernel extended to nonlinear kernels.
Braine et al. [82]	2021	-	-	-	X	-	-	-	-	Combination of binary decision variables with continuous decision variable with inequality constraints via slack variables	Extend quadratic unconstrained binary optimization issues to the class of mixed binary optimization problems using variational quantum optimization techniques. Propose two heuristics and use the problem of transaction settlement to illustrate them. The exchange of securities and cash between parties is known as transaction settlement, and it is an important aspect of the financial market infrastructure.
Kang and Heo [83]	2020	-	-	X	-	-	-	-	-	Quantum circuit for 5-qubit searching	Provide a complete process for accurately implementing the quantum minimal searching algorithm, as well as a quantum circuit for 5-qubit searching.
Satoh et al. [84]	2020	-	-	X	-	-	-	-	-	NISQ-aware algorithms in noisy intermediate-scale quantum (NISQ) machines	A modification of Grover's algorithm that divides the phase flip into segments to eliminate the need for a digital counter and complicated phase flip decision logic.
Gaily and Imre [33]	2021	-	-	X	-	-	-	-	-	Finding the extreme value of a constrained goal function or an unordered database with respect to a certain constraint.	Explore analytically the classical and quantum certainty of a novel kind of quantum existence testing (QET). It restricted quantum relation testing (CQRT) with how the CQRT can be used to convert the quantum extreme value searching algorithm (QEVSA) to a limited quantum optimization algorithm (CQOA).
Mondal et al. [85]	2021	-	-	-	-	-	-	-	X	Multiple-input multiple-output (MIMO) communication system, quantum error correction and others with a polynomial order.	The previous DHA and BBHT algorithms have been modified in two ways. In DHA, a semi-quantum framework in which non-solution points are deleted after each iteration in a classical framework. This iteratively reduces the size of the data set. To determine the Grover search number based on the Gamma distribution instead of the uniform one in the BBHT algorithm, which gives more possibilities to new greater values and improves the probability of success. When compared to their existing BBHT and DHA counterparts, the proposed QSAs show a credible improvement in search success performance.
Bhatia and Ramkumar [86]	2020	X	-	-	-	-	-	-	-	RSA algorithms	Because entanglement and superposition of qubits aid fast computation, Shor's methodology outperforms traditional computer methods in breaking various encryption algorithms.
Chivilikhin et.al. [87]	2020	-	-	-	X	-	-	-	-	Circuit topology	The multiobjective genetic variational quantum eigensolver (MoG-VQE) is based on multiobjective Pareto optimization, in which the non-dominated sorting genetic algorithm is used to optimise the topology of the variational ansatz (NSGA-II). We use the covariance matrix adaptation evolution strategy (CMA-ES), a derivative-free approach known to perform well for noisy black-box optimization, to optimise angles of single-qubit rotations for each circuit topology.
Guan et al. [88]	2020	-	X	-	-	-	-	-	-	Computing hitting probabilities of quantum random walks	Inverting a matrix can be used to compute quantum random walk striking probabilities.

A: Quantum Fourier transformation algorithms(a: Shor's algorithm, b: HHL algorithm), B: Grover's algorithm, C: Hybrid quantum-classical algorithm (c: Variational quantum eigen solver (VQE), d: Quantum approximate optimization algorithm(QAOA), e: Adiabatic optimization), D: Quantum error mitigation, (Error extrapolation and quasi probability decomposition), E: Other methods

layer is at the highest point of the control stack. This layer is for clients to furnish with a quantum calculation. The lower layers are utilized to help the actual crude cycles of the quantum computer. The virtual layer shapes a high exactness framework for the defective quantum measures in the solid computer states (quantum and coherent blunder remedy). In other words, a virtual layer is for open-loop error-cancellation, such as dynamic decoupling between physical and quantum error-correction layers. Another functionality of shortcoming tolerant qubits is at the application layer.

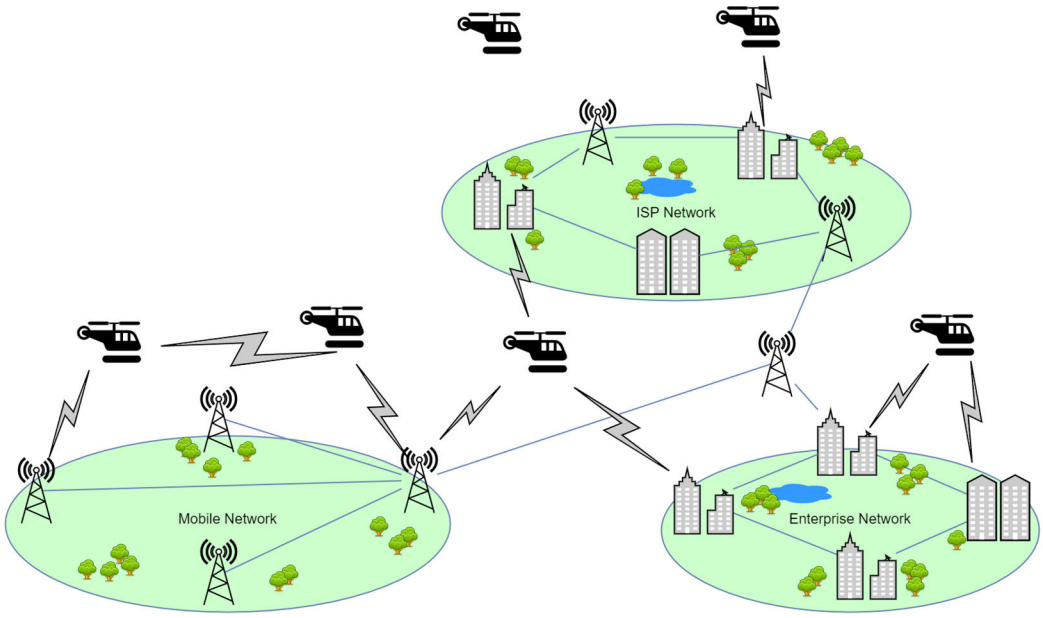

FIGURE 4. A quantum network with drone-based link nodes.

Figure 4 illustrates a plan for a quantitative drone network from wide-scale to local. The local area network can be set up for fast connection to ground stations via plug-and-play drone nodes. While high-height UAVs in the course and associated with existing quantum satellites and ground-fiber organizations [66], the wide-going organization can frame. Various robots can provoke on-interest and multi-hub quantic network associations for continuous inclusion on different reality scales. They can be utilized from many meters to many miles across a comprehensive regional organization. A quantum net can be anticipated by associating such versatile quantum hubs with existing satellites with ground-based hubs, as demonstrated in Figure 4.

D. CHALLENGES FOR DRONE-BASED QUANTUM COMPUTING

One of the main problems in the development of quantum hardware is due to the decoherence of qubits. When the qubit loses its coherence due to the interaction with the environment, it means that the qubit is decoded into a classical bit and thus converted into an overlay bit (any). The state becomes quantum advantage weight loss. In NISQ, 'Noisy' specifies how what's going on in the climate would upset the gadgets. A subsequent significant test is identified with the availability of qubits in the present quantum gadgets as it is non-trivial for performing the mapping with minor errors and less cost such as the number of CX gates, the specific qubit-tuple in the technology. These are the general challenges in designing quantum computers. Similar challenges could arise in hardware design for the drone as well. For example, incorporating the quantum node into a small drone is the critical encounter for a drone-based entanglement. Further, spreading and tracking data with precision becomes a more challenging task. In classical communications, data is sent over in the form of packets. These packets can be copied and retransmitted if there is a loss. However, the no-cloning statement and the postulate of quantum state measurement make it difficult to replicate or amplify qubits in quantum communication [67]. This presents many tough design challenges which make quantum drone-based network design functionalities more complex. Further, the generation and distribution of interconnections between different nodes across the network are among the biggest challenges for a quantum internet. This is not at all a problem in classical communication [68]. It is central to quantum mechanics. A qubit may overlap the two primary states and measure the quantum state in one of the actual states. Efforts are in process to resolve these problems in quantum networks.

E. CHALLENGES FOR QUANTUM-SAFE SECURITY

In recent decades new cryptographic techniques that protect against quantum threats came into existence. These practices are called "quantum-safe," together with strategies that prevent message interception based on light-quantum properties and classic computing techniques. All of these have been used to accelerate the research arena of quantum design [69]. Over time, and after enough research, a security clearance that can now be regarded as quantum secure today may indicate that it will become vulnerable tomorrow. Two technologies are being developed to deal with this threat in response to quantum computers: PQA and QKD. However, the next significant obstacles in security culture must be identified and resolved before achieving a secure quantum solution:

a. **Algorithm's confidence:** Some very much examined public key encryption alternatives might be utilized as

a supplement for RSA or ECC, yet a considerable lot of these substitutes are not generally used.

b. **Security protocol rigidity**: Since chronological protocol plan expectations and critical scope decisions in addition to message enlargement acceptance, the quantitative safe cipher may not fit into the established protocol.

c. **Non-urgency perception:** There is an increasing global concern and steady progress that cannot be given an exact period for the appearance of the general use quantum calculation [70].

Computer safety is weakened as quantum computing matures. Some companies require medium-term security because now worth protecting confidential information will also keep on complex and should continue to be retained isolated for some years or so shortly.

1) QUANTUM-VULNERABLE CRYPTOGRAPHY

Quantum mechanics are thought to be 100% safe and unhackable to send/receive messages. QC is based on using the tiniest single particles known to be in nature, namely photons. These photons have a feature that allows them to exist in multiple states simultaneously and only change their status when estimated. This is the fundamental property utilized by calculations in QC. Cryptography is a strategy used to conceal accidental beneficiary data [71]. Although QC alludes to cryptographic measures for securing against quantum attacks, this is at the core of a security plan [72]. Data in a quantum framework can't be replicated or perused by a snoop. Old style information might be duplicated like notes from books or chalkboards can be set up by understudies with no aggravation; quantum data can't be replicated [73]. A few calculations and conventions are proposed in this field. Not all security rules and cryptographic intentions are vulnerable to quantum attacks; some are thought to be shielded, while others are known to be susceptible. Post-quantum secure correspondence is an incredibly dynamic space of examination on the ground of quantum processing. QKD is a protected correspondence that gives a secret information insurance layer and plays out a cryptographic convention with segments for quantal mechanics [74].

On the off chance that quantum calculation turns into a reality, existing topsy-turvy measures become outdated. Web-based business, SSL/TLS, confirmation systems, and numerous different parts of organization security will be influenced. Online protection experts should comprehend the effect of quantum processing and the condition of the exploration in quantum verification calculations [89]–[91]. In an organization, quantum-safe and quantum weak items would exist together; now and again, decent progress is required. With the development of quantum estimation research, the window of opportunities for efficient advancement is contracting. The information that should be kept a mystery for a very long time to come may be shut.

III. QUANTUM SATELLITES FOR DRONE-BASED NETWORK AND COMMUNICATIONS

The future of wireless communication and initiatives were taken concerning internet security is the aim of quantum satellites. The first quantum satellite launched into space was accomplished in China [50] in August 2016. The testing done by launching the quantum satellite in space revealed that the technology is robust and it is hack-proof. The principle behind satellite communicating with earth used quantum entanglement, whereby subatomic particles become inextricably linked or ''entangled''. Since both are opposite ends of the universe, so changing one side will not allow changing the other part. This validates that hacking will not be possible easily even if attempted entangled particles. The improvement went further by demonstrating entanglement-based quantum-key distribution in 2017 to reduce the focus on the error detection rate by rendering secured communications [92]. The developments were further added on increasing the light-gathering efficiency and modified the filtering systems and other optical components that the low error rate is acquired for quantum-key distribution.

The work is also taken up by different countries to develop more secure communications between ground stations. National Space Quantum Laboratory was developed in the year 2018 that used the technology of lasers for acquiring secure connections in the international space station [93]. Quantum communication technology is being used by the USA for their defense projects also [94]. The diversions continued under a billion quantum flagship project under the quantum internet alliance by Europe. The launch of these projects took the space in generating their quantum communication-based satellite also with the UK in 2020 [95].

The limitations of the quantum communication methods can be extended by the applicability of the varied modern drones [8]. The other name of the drone is a UAV [96]–[98], and it has shown an immersive development [99] after the recognition of automatic flight control systems, and AI has taken place all over the world [100]. The drones have become popular because of the expansion of their weight coverage, altitude rise, and flight duration from grams to tons, from meters to more than 15 km, and covering more than 27 days, respectively [101]. This has successfully lead to the development of the mobile quantum network that could interconnect with satellites and fiber networks for further extension, which will finally form a practical, multifunctional global quantum network. In [8], the practical theory behind mobile quantum communication via entanglement distribution is explained, which is more robust against all weather conditions and can help in realizing full coverage over multiple space and time scales.

A. INTERNET OF QUANTUM DRONES

IoDs is a booming field that has diverted scientists and researchers. The particles of light are transmitted with a linkage of quantum known as entanglement. The bonded

particles present in these quantum particles remain even if they are helpful at long distances. This behavior welcomes the new varieties of communication. These claims to be ultra-secure and thus aid in developing the global quantum internet by generating the secret codes for encryption of messages. The feature allows connecting quantum computers located at distances to work with the help of a quantum internet facility [102]. The network uses fiber optic cables as quantum networks. The photons are transmitted with the use of quantum satellites across China Since drones are easily movable and portable as their deployment is quick and efficient. Gharibi *et al.* [103] made use of two drones for transmitting the photons using drone technology, one by enabling entangled particles, allowing to send one particle to a station located on the ground, and using other drones for communication. The particle was then transmitted by the machine and get received by the second ground station, which is few distances away from the machine that transmitted the particle. This technique helps in transmitting the entangled particles to the different receivers located at different locations by using a group of drones. Another researcher, Schirber [15], explained how the small prototype of a drone-based quantum network relayed a quantum signal over a kilometer of free space.

B. QUANTUM NETWORKS IN SPACE

The exploration in space started back in 1957 when the Sputnik was launched and still has been in discussion with robotics missions. This paradigm shift has been well noticed and has been carried with Space 4.0 to have a human presence in celestial bodies in the solar system. A similar example has been shown with the development completed by ESA as the moon village concept [104]. The various space agencies like NASA, ESA, JAXA, and others have been continuously working to explore space transition activities. Further, a huge interest is to explore more resources present on asteroids and the moon. Quantum networks in space communications have taken an edge over the previous technologies in the exchange of information between two stations, which is very crucial for the intelligence agencies and national security [105]. Many different countries like Canada, China, and Japan have been making use of quantum communications via using entangled transmission of photons [106]. This very new and quantum communication between space and earth is achieved by developing the channel set up kilometers apart. The information transmitted between two stations as sender and receiver are unable to hack or steal. This is the beauty of quantum communications which ensures that security is crucial and critically important when attacks on sensitive information have been targeted on.

The physical phenomenon is described by Quantum entanglement, which interconnects a group of particles in a complete system, and thus, the quantum state is also identified by the system as a whole [107]. The native quantum property of the particle will be changed by changing the overall system quantum state as well concerning the entangled particles. This property is induced as a measurement factor on an entangled pair, which is aware of this feature conducted on the other particle in transferring the information that can cover many kilometers in its range.

The property in quantum mechanics, taken as one of the most counter-intuitive characteristics that consider the ideal correlations, is known as entanglement. These correlations are maintained between entangled systems and are also in exact conflict. The entanglement is one of the most counterintuitive features of quantum mechanics because of the perceptions related to classical physics [108]. These principles and theories, which are proposed to identify and apply the predictive modeling on the quantum entanglement, are limited to certain scales concerning the mass and length in environments that have gravity. To explore more on quantum mechanics for space communications, these theories have to be validated taken beyond long distances and velocities that can be acquired in experiments and in the places where the effects of the quantum phenomenon and relatively works. This is done to claims the fact that the quantum interference effects can occur with long distances and at faster speeds closer to relativistic speed.

The encryption mechanism in quantum theory can be advantageous in the case of quantum entanglement as it is very useful in identifying the eavesdroppers who enter the communication loop. Their presence will be easily detected and will collapse the quantum states, which will automatically stop the information flow and will tell about all the operators who are trying to hack or steal. It is not possible to reverse engineer the encoded quantum key in the group of photons that are polarized. This property makes it secure concerning means of digital communication because of the property of inherited quantum mechanics feature [109].

C. TRADITIONAL VERSUS QUANTUM SATELLITES

The earlier communications via satellites were limited by the use of hardware, software, and solution for the transmission between sender and receiver. Different secured communications with a lot of practical solutions are emerging with the advancement in the field of information technology and computer science [110]. The reduced size of transistors in the manufacturing process is a great advancement. The better tools and methodologies are the result of quantum computing, and Even the traditional complex issues have been resolved with the power of quantum computing [37], [90]. The advantages and limitations illustrating the differences between the traditional and quantum satellites are presented in Table 4.

D. CONSTELLATION OF QUANTUM SATELLITE

The blend of a satellite with a terrestrial network is the upcoming technology known as a quantum computing cloud. In this system of quantum computing, the entangled photons, which are the primary source of transmission, need to be developed by varied sources and inter-satellite quantum communications. This is done to ensure that the data rates fall in the range of megabit to gigabits per second to compete

TABLE 4. Comparison showing the traditional and quantum satellites.

Parameters	Traditional Satellites	Quantum Satellites
Distance	Restricted to approximately hundreds kilometers, taking distance as a measure.	Able to transmit photons over long distances with the help of free-space quantum cryptography
Channels	Limited to using optical fiber channels or terrestrial free limited to a few hundred kilometers	Have power of exploiting satellite and space-based links
Redundancy-free solutions	Redundancy free solutions are harder to achieve	Redundancy-free communications with QEC
Security	No powerful provisions available to protect security of digital communication by attackers and service providers.	To transmit information in a secured manner, novel mechanism using quantum cryptography is used.
Robust	Traditional public key cryptography does not guarantee to transmit information theoretically secure	The unbreakable feature of security is provided by QKD [78] guaranteed by the law of physics, supported by transmitting photons of light encoded in quantum superposition states.
Hacking	Limited by advance techniques of encryption techniques, hacking cannot be prevented using traditional methods.	Using encoding and decoding, share of strings of random bits is achieved by using secret keys which is secured to transmit information between two distant parties.
Noise amplifying power	No such facility of available in traditional satellites.	Owing to the quantum theorem, the power of QKD with respect to quantum signal can be noiselessly amplified [79].

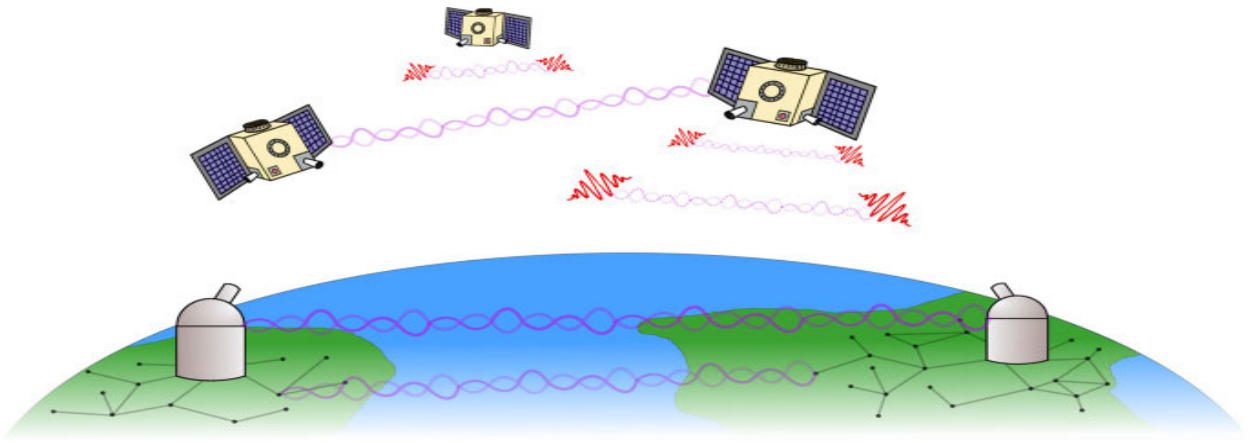

FIGURE 5. Global quantum communications network.

with traditional space-to-ground data links and optical communications using lasers. Furthermore, these will be tested with quantum entanglement by transferring the entangled quantum photons from the space to the different stations located at the ground spread over thousands of kilometers. In [111], [112], a detail on proposing a global-scale quantum internet with a constellation of orbiting satellites for constant entanglement and distribution service to ground stations is discussed. Figure 5 explains the architecture of satellites at the global level. Figure 5 explains how the entangled photon pairs, which are distributed through satellite constellation in red color to the stations on the ground, separated at a farther distance. The hubs are known as stations that can connect with local nodes using communication channels, namely fiber optic. The entanglement is shared between two nodes through swapping technique enable using entanglement principle in quantum mechanics.

E. FUTURE RESEARCH DIRECTIONS IN QUANTUM SATELLITES

Owing to the history of quantum communication and its free space, QKD came with its implementation spread over an optical path in 1991, separated at a distance of 30 cm. Further research extended to be achieved in 2002 in the daytime to check whether photons transmitted in the sun can be safe or not. Further advancements in distances were extended in 2006 to 144 km by international researchers [113]. Ground to ground and satellite to satellite quantum communication

was done in the year 2008 [114], and this was one of the primary aims of the ESA and called quantum-based satellite communication till 2013 [115]. The major advantage listed under this domain is to acquire loss-free and distortion-free optical communication. Further advancements can be seen as cloud quantum [116] as a working constellation for quantum internet with the installation of satellite quantum repeaters.

Nature has a beautiful property called entanglement, and that is explained by quantum theory. So if two particles are entangled, their state cannot be described by the individual states and need to be expressed jointly. This is a bizarre property found in the quantum world and has intrigued a lot of physicists. But this property gives the power to perform tasks that are impossible by just using the laws of a classical mechanic. Some of them include secret key sharing, quantum teleportation, dense coding, and many others. The subtlety lies in the experimental realization of such protocols. In an experiment, a system can never be isolated completely from the environment. So other undesirable effects, technically called ''noise,'' crop in and effects the system. Entanglement is such a fragile resource that a small amount of noise can destroy it. So it is a huge challenge to overcome this problem. Now, as the experimental setup increases, the amount of noise also increases. So it becomes all the more challenging. The Chinese sent a quantum satellite to space and fired entangled photons to ground stations, separated at a distance of 1203 km [117]. They did this using entangled photons which were sent from the satellite. The experiment was performed at night to avoid interactions with the photons from the sun. Still, future research directions can be looked forward to increasing the distance with noise amplifying power at larger distances.

Quantum teleportation is also an emerging field and can be taken as a future scope in which an unknown state is prepared in some other place where both are spatially separated. This is one of the protocols that can be done only using entangled states when performed at larger distances. This paves the way for new means of secure communication that can be performed using the quantum states. This communication will be completely hack-proof. This can be a target for something revolutionary in the field of communication, especially quantum computation. The series of communicating experiments are getting between the quantum science satellite and quantum communications stations on the ground [118]. The primary goal of setting up space communications digitally across the long-range channel between the ground station and satellite station will be implemented with the help of QKD as a result of secured experiments performed on the same. Many more running experiments are performed with the satellite by using its services as a repeater in order to connect the two QGS on Earth. However, the quantum entanglement is completely secure and robust, while still the challenges are there and no facts are there for securing the quantum networks against attacks and other issues related to operational security.

With the advancement of AI and ML techniques, the trend of identifying the applications of ML in communications and space has been growing widely [119]. The Satcom industries and other agencies are trying to find the potential solutions to address issues in satellite communications such as decreasing the effect of interference so that the coexistence of satellite systems and the terrestrial system can be further developed, optimal solutions in gaining spectrum power in radio resources can be looked upon. Also, the constellation satellites can be further investigated.

IV. QUANTUM DRONES, AI AND ML

This section explores quantum drones, quantum machine learning, QAI, future applications of quantum drones, and future research directions associating quantum machine learning, QAI, blockchain, and other disruptive technologies. Details are presented as follows.

A. QUANTUM DRONES

UAVs or Drones as a disruptive technology have acquired impressive coverage in recent years because of the benefits they may provide and their operational agility [120]. UAVs can be utilized for a variety of purposes, including community security, logistics delivery, regions coverage, emergency events, traffic monitoring and congestion control, coast inspections, reforestation, among others. Nevertheless, one of the most significant drone technology issues is achieving optimal deployments [121], [122]. UAVs are among the fastest expanding, high-level, and widely used unmanned aerial systems. Even so, collision detection and trajectory planning remain unresolved issues. This is because there still are practical and theoretical issues with the current practices [121]. Most importantly, in parallel with the impressive disruptions and innovations caused by UAVs in society, rapid developments in this field have been investigated by exploring the potential megatrend of quantum computing technologies.

Quantum computing is considered a research area that integrates knowledge from engineering, physics, and computer science [123]. While Paul Benioff published the principles of quantum information in 1980, it is feasible to consider that the development of quantum computing began with Richard Feynman's works promoting non-classical physics studies [124]. A variety of computer tasks can now be performed exponentially quicker on a quantum processor than on a conventional central processing unit. Quantum computing is built on quantum physics foundations, including quantum superposition, the no-cloning theorem, and quantum entanglement [18]. Due to the lack of a classical counterpart for these processes, equivalent results cannot be produced using conventional computation. Several quantum computing experiments have previously been developed, and several investigations are now underway. In a recent study [125], quantum states of 53-qubits are successfully established using a processor built with superconductors qubits. According to the findings, the processor takes two

hundred seconds to sample a million times one instance of a quantum circuit, while a supercomputer could take ten thousand years to make the same analyses. These findings show the possibilities of quantum calculations in various civil and strategic applications, such as, for example, with other cutting-edge technologies like drones.

In [126], a survey is developed that examined the challenges of using UAVs in civil applications and offering several technological and scientific limitations that should de addressed. In [127], a drone-based QKD is recently tested to minimize various types of drone incidents. They evaluated essential subsystems, such as a QKD based on resonant-cavity light-emitting diodes and a QKD based on a fiber-coupled polarization modulator. The solution under test consisted of numerous cascade elements that provided route synchronization via infrared signals with gimbals and precise realignment via director mirrors with precise encoders and sensors. They concluded that constructing links using quantum communications across drones on air is a challenge for the prospective quantum system, including entanglement transmission, distributed quantum sensing, and quantum positioning confirmation.

Quantum information processing opens up new possibilities in computing, communications, and networking [18]. Timely developments of quantum algorithms in the area of ML have led to sophisticated results demonstrating how quantum computers can be applied to solve issues of AI faster than classical methods [123]. These recent developments open new research fields integrating these disruptive technologies and inaugurate the field study on QML and QAI. These areas have the potential to lead to breakthrough developments and innovations in the use of drones for a variety of civil purposes such as logistics delivery, traffic monitoring, military, among others [18]. These advances from the extant literature are examined in the following sections.

B. QML

QML is a disruptive technology that requires a minimum direct involvement of humans that has gained significant relevance in both the scientific community and industry [128]. The QML intelligence benefit from the advantages of quantum computing applied to ML. In this case, the primary benefits are related to the unprecedented increase in processing dimensions. Typical potential realistic applications of ML algorithms included the development of quantum algorithms, information processing algorithms, circuits, devices, and materials [123]. Results from the literature present a cohesive framework on advances of QML in information processing. Schuld *et al.* [129] offered an analysis of existing QML notions and methodologies. They found that there are two distinct approaches to QML. In the first, search quantum methods that can replace classical MLalgorithms in a given problem and demonstrate the impact of increasing complexity. In the second approach to QML, the probabilistic quantum theory is used to explain stochastic processes. Pande and Mulay [130] investigated the research trends in the topic of QML. In the examined period (2016 to 2019), 148 technological patents were found, suggesting the applicability of the QML to real-world problems. Researchers also have demonstrated the quantum advantage in varied ML applications. Dunjko *et al.* [131] developed a model for the use of QML in information processing and discovered that quadratic gains are feasible. The model enabled an exponential increase in performance in a short amount of time. Riste *et al.* [132] demonstrated that a five-qubit quantum processor could handle and implement an Oracle-based dilemma with noise. They advised that complicated tolerant systems be used for experimental universal quantum computing. Benedetti *et al.* [133] investigated a quantum deep learning system used to extract a low-dimensional binary representation of data from industrial datasets in near-term machines. The proposed system is ideal for small quantum processors that can facilitate the training of an autonomous generative algorithm. Alvarez-Rodriguez *et al.* [134] investigated QML models that need any quantum measurements and developed a QML approach for addressing unitary operations issues efficiently. The system developed utilizes an iterative procedure that uses a quantum time-delayed equation for dynamical feedback and eliminates the need for quantum measurements. They claim that time-delayed equations can improve experimental QML approaches significantly. Another attractive area for QML is the use of quantum computation in recommendation systems [135]. For example, Kerenidis and Prakash [135] examined a QML algorithm for a recommendation system that operates in polylogarithmic time in the matrix. Quantum reinforcement learning algorithms have been constructed utilizing superconductive quantum circuits, allowing quantum information processing and quantum computation to be achieved [136]. The distributed training in sets of quantum computers might enhance the efficacy and time of the training process by sharing the learned models [137]. The authors introduced a federated training system based on QML, recognizing a quantum neural network with a conventional pre-trained convolutional framework. The research indicated that federated training based on QML ensures performance. Their results contribute to privacy-preserving AI and quantum computing opening research avenues for the development of safe, scalable decentralized QML architecture. The research in Lim *et al.* [120] developed a federated learning system for facilitating cooperative ML in a federation of individual drones as a service (e.g., parking lot occupancy planning and traffic forecasting). The Gale-Shapley algorithm was used to determine which drone would be the cheapest option to operate in each segment. The literature presents the recent development of QML for activities of object-detection and visual identification integrating drones. Giusti *et al.* [138] proposed an alternate technique for recognizing forest and mountain pathways employing a deep neural network using supervised learning as a classifier for one monocular image from the drone's

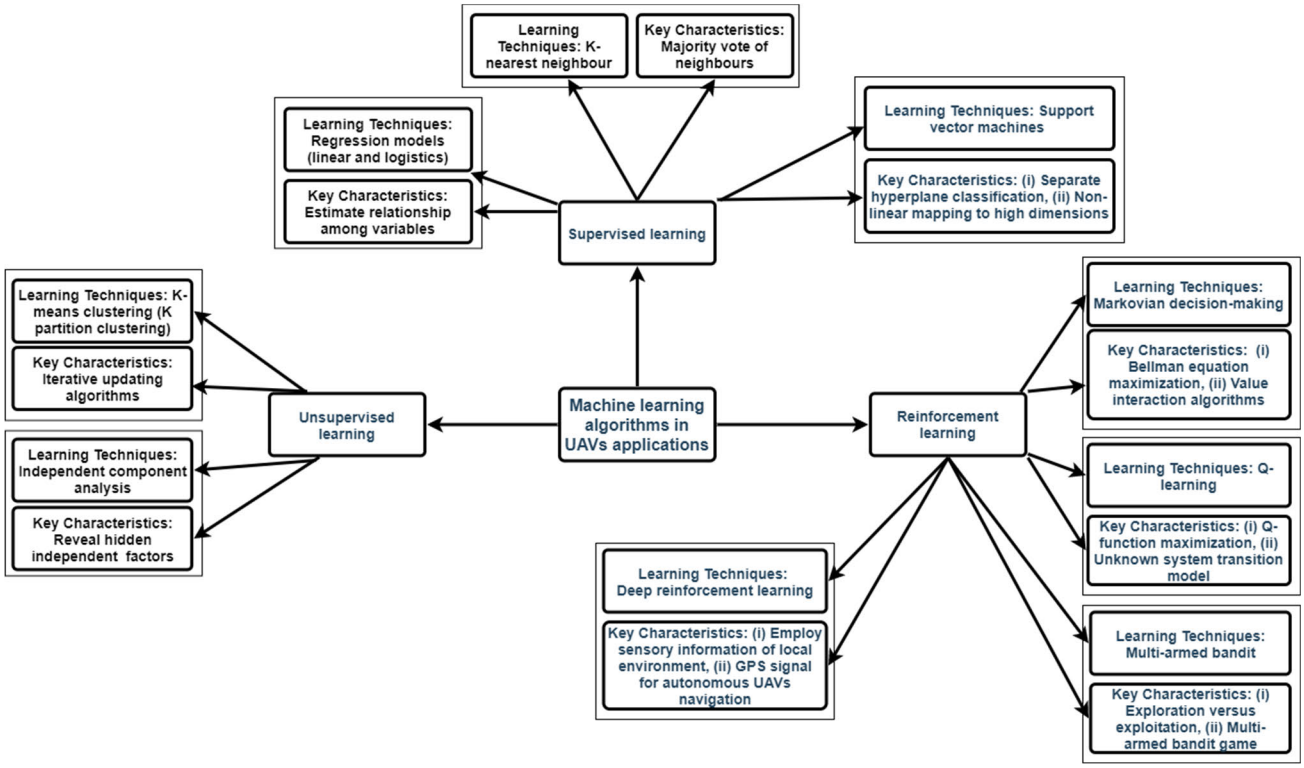

FIGURE 6. Machine learning algorithms in UAVs applications [126].

position. Outcomes suggested that the accuracy appears to be equivalent to those evaluated on the same image recognition activity. A system for assisting the searching and rescuing of people in avalanches was created by [139] utilizing drones equipped with vision cameras. The avalanche debris photos were examined through a pre-trained convolutional neural network to extract discriminant information on images. A linear vector machine was connected to the neural network to find relevant objects. The classification method prioritizes prediction accuracy using HMM. Barbeau [140] investigated the challenge of recognizing activities conducted by drone groups, exploring how traditional ML and QML might assist the development of viable solutions for drone swarms activity recognition. In [141], deep-learning-based object-detection models are applied to drones. The results demonstrate that a faster region-based convolutional neural network is the most accurate model, whereas 'you only look once' is the fastest. They found that using deep-learning-based detection algorithms in conjunction with UAV aerial data are useful to recognize birds in a variety of situations. Carrio *et al.* [142] reviewed the developments and applications of deep learning for drones. They found that feature extraction is the type of system where deep learning systems are more usually applied in the literature on deep learning-based UAVs. Shan *et al.* [143] suggest a novel MLapproach to data analysis and model establishment for drone connectivity. Their results indicated that the solution developed can establish a more complex model with less effort. Approximately 80% of the training errors have an intensity of less than 5, meaning that the error performance is stable.

Studies also have implemented ML to optimization problems in drones applications and wireless systems. Klaine *et al.* [144] designed and tested an intelligent system based on MLto discover the optimal placements for many drone small cells in an urban region where a calamity has happened, expanding the efficiency of served customers. The results indicate that the technology surpasses all other approaches on all parameters studied and that intelligent drone small cells are a viable alternative for deploying an urgent communications system quickly and efficiently. Instead of employing the computationally demanding local search technique with the central processing unit on limited-power devices, a neural network operating on induction chips may be more efficient and faster. This is critical in free-space QKD environments (e.g., drones, satellite-ground QKD, portable, etc.) with a restricted budget and request minimal real-time latency [145].

Collision prevention, warming issues, and networking security-related concerns are constraints to be solved in practical applications of drones [126]. To address these limitations, several ML supervised learning, unsupervised, and reinforcement learning algorithms have been tested in drone applications, as shown in figure 6.

Chen *et al.* [146] investigated the challenge of preemptive development of cache-enabled UAVs in a cloud radio architecture to improve wireless device quality of experience.

They simulated cache-enabled UAVs using machine-learning architecture to give mobile subscribers services reduced power consumption. Individual data were collected (e.g., requested contents, visited locations, job, gender, and device) to anticipate the sharing of each individual's content requests and mobility patterns. ML was used to identify user request distribution and mobility standards and used UAVs to cache this information. Results showed that when compared to a benchmark algorithm without caching and without UAVs, the machine learning-enabled algorithm can deliver gains in transmissions and users. The algorithm also allows echo state networks to segregate users' behavior into sets of patterns and learn these patterns using non-linear systems. Joint with QML, QAI is a key technological trend in modern times [131]. In the following section, we discussed several key contributions made to the field.

C. QAI

AI is a disruptive technology referring to computer methods for problem-solving that allows any machine (e.g., a robot, drones, etc.) to think intelligently when applied in isolation or combined with ML and other technologies [128]. AI is a decisive technology for the next developments of computational devices based on quantum technologies [123].

Recently, Dunjko and Briegel [147] highlight the fundamental principles and recent progress in a wide range of research on ML and AI in the computational quantum field. Overall, they claim that the existing research is mainly theoretical and lacks tests illustrating how quantum technology can be used for ML and AI. Moret-Bonillo [148] explores synergies and possibilities of cooperation between QC and AI. They summarize the main contributions arguing that QC could aid in increasing the efficiency of current intelligent systems. Furthermore, there are interdisciplinary opportunities to examine synergies between QC and AI. As a result, the primary synergies between QC and AI could lead to new insights in areas as statistical inference, Bayesian networks, and pattern recognition (e.g., recognition and discrimination of quantum states and quantum operations applying AI) [148].

Disruptive advances of AI in isolation or integrated with ML, Blockchain, and other cutting-edge technologies demonstrated significant benefits in terms of precision and results. For example, an optimized artificial potential field algorithm for multi-UAV operation in a 3D dynamic environment to collision avoidance was tested [149]. To overcome common issues (e.g., unachievable targets) and certify that the drone does not collide with obstructions, the approach was evaluated with a distance factor and jump tactic. To achieve collaborative travels routes, the method considers drone companions as dynamic obstacles. Then, an optimized artificial algorithm for collision avoidance was tested in simulation models. The method was tested in a simulation model urban environment with satisfactory results [149]. Many security and authentication challenges arise while using drone-enabled IoT, also recognized as the IoDs. IoD enhances the performance of services by increasing the potential of data gathering, connectivity, and processing, improving the efficiency of missions in remote areas that offer risks for humans [150]. Drone-based quantum network communication prototypes have been suggested in recent experiments [15], [151]. For example, Liu *et al.* [151] used drones to construct a pioneer optical relay to bend the wavefront of photons for their minimal diffraction losses in free-space communication. The first drone was used to distribute the entangled photons, while the second drone was utilized to function as a relay node. As a result, they produced entanglement distribution with Clauser-Horne-Shimony-Holt parameter (2.59 ± 0.11) at 1 km proximity. Significant elements for linked source, tracker, and relay are designed to result in a scalable airborne system for multimode connection enabling mobile quantum systems. Drones may be positioned or repositioned at any time, making the IoD's particularly useful in urban and rural environments. Quantum signals are employed to exchange qubits across a short distance in these prototypes and small-scale implementations. With this capability, hovering drones for quantum data exchange can be easily observed for various purposes [8].

A recent study on the reliability of drone networks developed and implemented in a healthcare-based research study, a Blockchain-based architectural design employing a 5G communications system and AI [152]. The authors used a systematic literature review and case study. They developed an infrastructure adopting the InterPlanetary File System as an information storage platform that enhances the network performance, security mechanisms, and data protection while lowering the cost of storage. They contribute by addressing the communication weaknesses, challenges, and drawbacks of drones networking and suggesting a decentralized and stable architectural design for drone-based monitoring.

Another exciting work [150] presented a supervision scheme integrating Blockchain and AI where a group of drones facilitated by the IoD is embedded with AI is engaged to supervise crises scenarios autonomously. Two types of drone swarms were used to handle multiple tasks, a lightweight Blockchain was used to act in remote areas, and a two-phase lightweight security mechanism was adopted. The system was validated through experiments. Although the investigation requires a complete real-world application, the performance was satisfactory for supervision tasks. Recently, drone-based service providers for data gathering and AI model training have risen in importance. On the other hand, the strict restrictions regulating data security are difficult data sharing between individually operated UAVs [120].

In quantum computing and AI, there are two directions that can give advantages to various futuristic applications. These directions include the importance of quantum computing for AI or related domains and applications and AI for quantum computing or related domains and applications. Various advantages of quantum computing for AI or

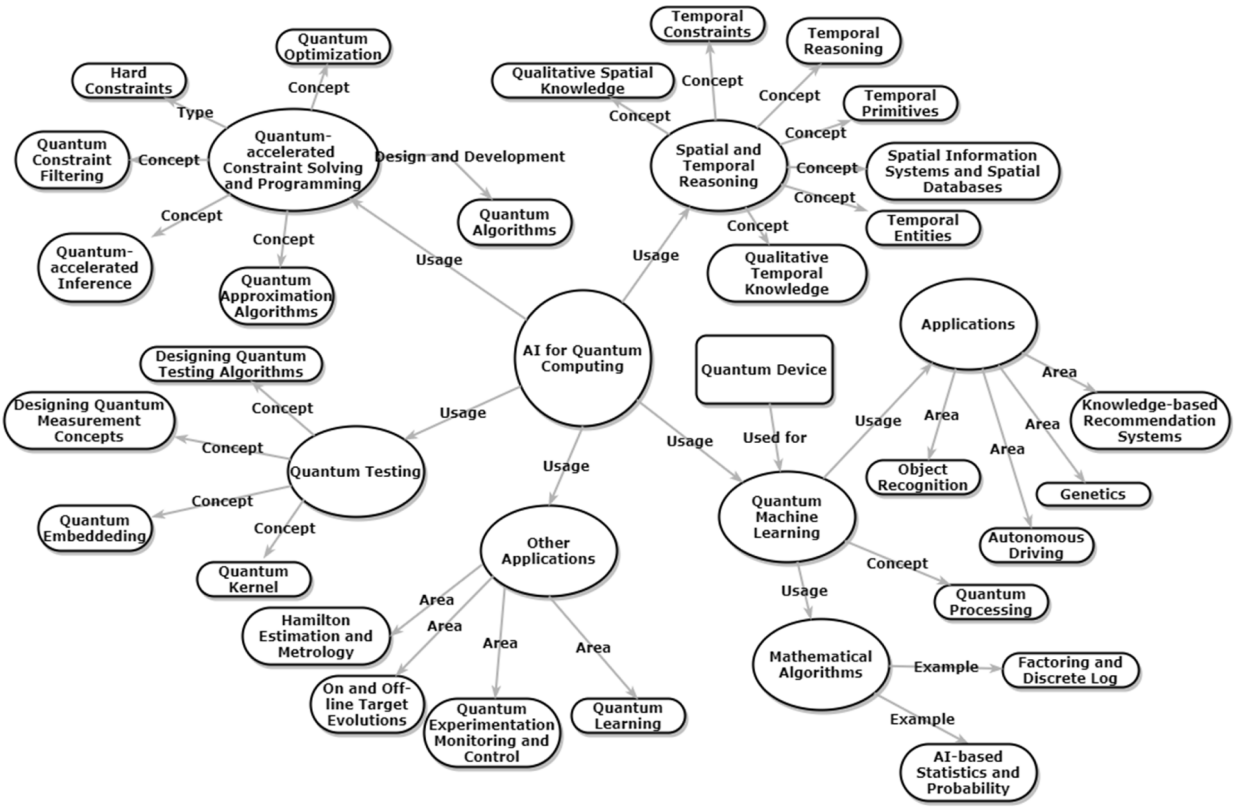

FIGURE 7. AI for quantum computing.

related domains and applications are briefly explained as follows [153], [154].

- ***Solve Complex AI Problems Quickly*:** Google says that its quantum computer is about 100 million times faster than other existing models. With the help of quantum computers, AI-based complex problems can be answered in seconds. Verification will be successfully deal with such complex problems in a short amount of time. The use of quantum computing methods allows us to upgrade our machine learning approaches. The technique may be used for AI and machine learning before the end of the decade.
- ***Solution Optimization*:** The more data we gather, the more detrimental it is to the computer industry's bottom line. Quantum computing will fundamentally alter how vast amounts of data are analyzed. In the domain of making better decisions, they provide considerable impact to businesses and consumers, respectively.
- ***Fast Searching*:** A quantum computer is expected to quickly sift through large, unorganized data sets for patterns or anomalies. This is because quantum computers may be able to access all of your database items simultaneously, making it possible for them to discover these similarities with great speed. It is conceivable that the data gathering is so extensive that it will never happen.
- **Fast Data Integration:** Quantum computers are expected to be able to handle a wide range of data sets which is a trivial task for AI. Quantum computers will allow fast analysis and integration of large data collections. In large dataset integration, language semantics research is vital to AI. This is expected to be handle easily by quantum computers or computing. However, there will always be an option for an individual to assist the system in acquiring new abilities.
- **Improved Conventional Machine learning Algorithms:** Deep learning training may either speed up or be enhanced by quantum computing. This is because of the speed and accuracy of quantum computing, and traditional machine learning algorithms may benefit by giving the optimal set of weights for artificial neural networks.
- **Faster Approach for Decision Making Algorithms:** Quantum algorithms based on Hamiltonian time evolutions are helpful in solving problems that can be represented by a decision tree. This solution will be faster compared to random walks. Thus, AI-based complex problems whose efficiency reduces with branches can easily be solved with quantum computing algorithms based on Hamiltonian time evolutions.
- **Improved Game Theory using AI:** Quantum game theory is an extension of classical game theory, which is important for AI. Quantum game theory is expected to overcome the critical issues of QAI.

In addition to the above advantages, quantum computing would be useful to AI in various applications if it is able to handle critical issues. Some of the critical issues include: (i) designing and developing less error-prone and more powerful quantum approaches for AI, (ii) inventing open-source modeling and training frameworks for the machine, deep, and reinforcement learning; and (iii) showing real-time results and improvements for AI-based applications using quantum computing and concepts compared to classical computing. The advantages can be taken in reverse directions, i.e., how AI is helpful for Quantum computing. Figure 7 shows the important usages of AI for Quantum Computing. The important AI application areas in quantum computing are briefly explained as follows [155].

- AI can represent the qualitative spatial and temporal knowledge that can be widely used in geographical information science.
- In quantum computing, AI can be helpful in constraint filtering, hard constraint solutions, accelerated inferences, optimization algorithms, and finding a solution to various approximation algorithms.
- AI with quantum computing can handle a vast amount of data. Here, AI can help design testing algorithms, property measurement concepts, quantum embedding for data, and quantum kernel instead of classical machine learning.
- Additionally, AI is useful in quantum computing-related areas, including Hamilton estimation and metrology, online and offline target evolutions, quantum experimentation monitoring and control, and quantum learning.

D. FUTURE APPLICATIONS OF QUANTUM DRONES

This section presents opportunities for future applications of quantum drones in isolation or integrated with other disruptive technologies. Most importantly, building strategies, data transfer, scalability (the significant rise in the number of qubits required for every calculation containing error correction), quantum algorithms and structures, and models are, until the moment, unanswered concerns within quantum computing [148].

A disruptive technological advance on quantum drones is quantum associated services facilitating the work in industry and academia. In this case, quantum-accelerated cloud service providers, for example, are required to deliver practical quantum computers to academia and industry, allowing quantum computing to transcend through the death zone as a feasible succeeding computation technology [156]. Consequently, these limitations should be considered to unlock the full potential of real-world applications of quantum drones. Future development in research is needed to test wireless charging approaches with energy harvesting, enabling drones to undertake detecting and training simultaneously. In addition, future applications of quantum drones could test deep reinforcement learning to optimize resource allocation in the federation of drones as a service [120]. The integration of drones with Blockchain and AI technologies also has the capacity to solve communication security questions. The extant literature is focused on 5G-based drone communication, and drone communication lacks a more precise understanding of Blockchain and AI potentials in quantum drones applications [152]. Improvements in ML will provide solutions that could further be used for QAI practitioners' sophisticated creations [147]. These developments can be replicated to drones and quantum drones solutions. Finally, additional research is required to apply information from a variety of sensors and detect a variety of activity models considering the several types of drones group missions to the activity recognition issue [140]. Future applications of quantum drones in these related areas will contribute to the progress of knowledge in the field and potentially contribute to solving the current problem of social interest.

E. FUTURE RESEARCH DIRECTIONS

Outcomes from extant literature indicate that there is still a need to expand the empirical and theoretical research on quantum drones in isolation or when associated with QML, QAI, Blockchain, 5G, 6G, and other disruptive technologies. This section presents the main of them.

Firstly, important thematic areas for future research directions on drones technologies remain unanswered until today. According to [126], the primary specific topics for developments for drones include:

- Battery capacity and good energy management are two issues that arise when it comes to charging (scheduling, planning, and replacement of battery). Because of their higher power density, proton exchange membrane fuel cells may be more convenient than Lithium-Ion in this instance.
- Further innovations on wireless charging for drones and wireless power transfer systems are required to enable autonomous charging points with the accurate landing of the drones on the charging pad. Due to their efficiency at short and medium distances, solutions such as inductive and magnetic resonant coupling could be appropriate.
- Solar-powered drones utilized in long-distance and high-altitude flights also require better path planning and optimization.
- Collision avoidance challenges with vision-based, sensor-based, and hybrid techniques, as well as swarming, involve: (i) the convergence of laser range searcher sensors with vision or ultrasound sensors to prevent multidirectional collisions; (ii) the introduction of new technology control algorithms and deep learning methods with model predictive monitors, taking into account hardware limitations in on-board processing; and (iii) new algorithms for dynamic sense, avoid algorithms, image processing and path re-planning; (iv) the establishment of international regulations and standardization rules.

- FANETs are ad-hoc networks that connect drones. In this case, more research is needed to (i) develop new software-defined networking services to improve reliability, reachability, mobility security, monitoring, and protection in FANETs; (ii) designing new safe path protocols and networking concepts for FANETs; (iii) replacing traditional network devices with decoupled software-defined networking switching; (iv) development of customized end-to-end protocols, optimized virtual networks topologies, and dynamic networks; (v) development of new protocols to bandwidth requirement, conserve energy, and improve service levels; and vi) confidentiality (e.g., key-loggers, malware, hijacking, social engineering, eavesdropping, etc.), availability (e.g., buffer overflow, flooding), and integrity (e.g., fabrication alteration, signal spoofing) are all issues involving cybersecurity attacks face

In [150], the study is performed to add the following future research directions in drones technologies: (i) regarding data privacy, new studies are needed to ensure data protection, to develop mechanisms to ensure data privacy and accuracy as penalties, to define the appropriated hierarchies of data access (e.g., governments, service providers, other individuals); (ii) flight management, efficient trajectory, and proper flight planning are a challenge to avoid collisions with drones; (iii) the efficient distribution and allocating in zones of swarms with drones also is a challenge that requires the development of new algorithms to reduce network overhead. The development of medium access control protocols for swarms with drones is required.

Secondly, several future research directions exist to advance the knowledge on the potential of applications of QML. Scientific advances in these areas can derive new solutions and developments in quantum drones applications in the forthcoming years. In specific on QML advances, underexplored areas for future research directions include: (i) apply quantum computation to analyze learning methods of parameter optimization; (ii) the issue with quantum computing based on unitary quantum gates would be to parameterize and change the unit transitions that define the algorithm gradually; (iii) quantum computation solutions such as dissipative and measurement-based quantum computation can provide an attractive platform for QML [129]. Pande and Mulay [130] recommend that future researches on QML could investigate (i) how to use feature space in quantum computers with MLclassification problems. Further, how to integrate quantum algorithms for classification problems in supervised learning and big data classification; (ii) how to make transfer learning with hybrid classical-quantum neural networks; (iii) how to develop new quantum neural networks to improve the capacity of multi-sensor approaches for routing of vehicles. Moreover, future studies could try alternative MLalgorithms to discover the ideal places for several drone small cells [144]. In [157], four fundamental issues are indicated to be addressed in further investigations in QML areas:

- First, despite quantum algorithms' remarkable processing velocity, they rarely offer equal velocity to reading data. Consequently, in some instances, the costs of processing in the data input may dominate the costs of quantum algorithms. This is a problem related to output in QML.
- Second, it takes an exponential amount of bits to obtain the complete result from specific quantum algorithms constraining various applications of QML. This may be avoided by examining statistics for the solution condition. This is a problem related to output in QML.
- Third, the true number of gates required by QML algorithms is under-recognized. Boundaries of complexities indicate that they will provide significant benefits for large problems, although it is unknown when that point will be reached. This is a problem regarding benchmarking.
- Fourth, the claim that a quantum algorithm is always superior to classical algorithms is challenging because considerable benchmarking versus heuristic methods might be required. Lower constraints for QML can help to solve this problem in part. A promising alternative to these problems includes applying QML to classify and control quantum computers.

Carrio *et al.* [142] claim that the main challenges and opportunities using deep learning-based UAVs include: (i) to depth the experiments on systems regarding higher-level abstractions, including the supervision of drones and planning systems; (ii) even systems that operate at lesser levels of abstraction, like feature extraction systems, require a lot of computing power. Such resources are still difficult to incorporate onboard UAVs. Furthermore, most computational resources are incompatible with online processing, limiting the applications that require responsive behavior. For this reason, future studies are needed to upgrade embedded hardware technology and to develop efficient deep learning frameworks.

Furthermore, exciting unresolved issues regarding the integration of drones with Blockchain, AI, QAI, and 5G remain intact [152]. For example, (i) in terms of information privacy, there is an urgent need to develop new solutions to provide data privacy to Blockchain participants. The AI algorithms at the edge-AI layer are constrained by computing power and limited space. In our opinion, this problem could be solved by implementing the power of quantum computers; (ii) to resolve loopholes and software vulnerabilities, programmers need to conduct a risk assessment prior to deploying their code onto the Blockchain network; (iii) another issue is the Blockchain network's scalability. Additionally, QML can significantly help with AI limitations and scope, primarily through traditional ML learning algorithms [131]. Other promising and underexplored areas of applications include the use of deep learning in quantum entanglement [158], QML applications in near-term quantum computers [128], QAI in superconducting circuits [136], among others. Hence,

there is still a need to expand the research associating the synergies between QML with QAI.

Effective Blockchain governance models must be established to define who controls, administers, and debugs the Blockchain network, defines the norms, and resolves conflicts and policies in drones' Blockchain network [152]. Furthermore, a serious concern is that quantum computing can compromise Blockchain security in the near future. As a result, developing quantum-secure Blockchain networks is a current challenge. Additional challenges to be addressed include data processing delays and Blockchain standardization. Besides, the use of AI in UAVs is particularly needed through (i) deep learning to progress in areas such as battery scheduling and path planning; (ii) recurrent machine learning-based networks improving discharge models and precisely predicting the end of life of the charge; and (iii) convolutional neural networks to mapped charge stations and accurate landing in charging points [126].

We recognize the future research in these thematic areas will stimulate the consolidation of knowledge in the forthcoming years within relevant underexplored research topics of social relevance involving disruptive trends and technologies as quantum drones, QML, QAI, Blockchain,5G, 6G, among others disruptive trends.

V. QUANTUM ATTACKS

This section explains quantum attacks in different possible scenarios [159]–[168]. Figure 8 shows the major classifications of quantum attacks on cryptosystems. Details are presented as follows.

A. QUANTUM ATTACKS ON IFP-BASED CRYPTOSYSTEMS

The problem of identifying the prime factors of large complex integers has aroused mathematical interest for centuries. It is indeed of practical relevance with the emergence of public-key cryptosystems, as the security of these cryptosystems, such as the RSA systems, is dependent on the complexity of scaling the public keys. Provided with the necessary computer capacity, the highest-profile integer factorization techniques have substantially gotten better, to the extent that it is now trivial to factor a 100-decimal digit number and conceivable to factor bigger than 250 decimal digits. The only various categories of realistic public-key cryptosystems [1] in use are those based on the ECDLP, IFP, and the DLP. Because no polynomial-time methods exist for these three implausible issues, the security of these cryptosystems is highly reliant on them. However, if a real quantum computer is available, non-exponential time quantum algorithms for ECDLP, IFP [2], and DLP exist. Mostly all existing quantum computing-based attacks on public-key cryptosystems are covered in Quantum Attacks on Public-Key Cryptosystems, with a focus on quantum algorithms for ECDLP, IFP, and DLP. This even goes over quantum-resistant cryptosystems that could replace ECDLP, IFP, and DLP-based cryptosystems. We are now encircled by technologies that capture and communicate personal information. The IFP and the DLP are now the two fundamental mathematical issues that ensure Internet security. Shor's quantum algorithm, on the other hand, can readily solve both difficulties. As a result, research into encryption algorithms that operate on regular computers but are resistant to quantum computers is important. PQC is a branch of cryptography that focuses on asymmetric cryptography. As per a NIST study [3], quantum computers with cryptography capabilities are expected to debut around 2030. Given the importance of data resources for the smooth functioning of the financial system, international banking, military security, and, inevitably, the global community as a whole, more efforts in PQC will be required in the coming years to address data security issues. There are numerous parameters to cryptographic attacks, and one of them is to target the encryption method itself. Since the dawn of mathematics and computer science, large integer factorization has remained a difficult issue. The RSA algorithm, a standard cryptographic procedure, necessitates the factorization of big numbers. There is no polynomial-time method in traditional computation that can scale any huge unbounded number. Hambling [4] depict the methods for factoring numbers, including Shor's Algorithm, Quadratic Sieve Algorithm, and Trial Division, using flowcharts and implementations, and closes with the observable evidence and assessed findings.

The difficulty of traditional issues plays a crucial role in assuring the security of a conventional, well-known cryptosystem. Although quantum processing is on the rise, several classical hard problems are becoming vulnerable to already-known quantum assaults, necessitating the development of a post-quantum cryptosystem to fend against quantum attacks. From the standpoint of cryptanalysis, it is important to outline existing quantum techniques and their dangers toward certain cryptographic insoluble issues to bridge the different technologies. The suggested technique, procedural approach, and advanced enhancement of mathematically difficult issues on which conventional cryptosystems depend, namely the distinct logarithmic problem, integer factorization challenge, and its variants, extrapolated dihedral coset problem, lattice problem, hidden subgroup problems, and dihedral problem, were discussed in [5]. It explained why some cryptosystems, such as ECC and RSA, are vulnerable to quantum assaults while others, such as lattice cryptosystems, are not. Photonic systems are now used in practical quantum applications. Alice provides photon pulses encoding quantum states, and Bob selects observations on such states in many of these systems. Bob often uses single-photon threshold detectors, which are incapable of distinguishing between the numbers of photons in observed pulses. Bob is also required to notify the observed pulses due to losses and other flaws. As a result, a malevolent Alice can broadcast and monitor multi-photon pulses, gaining knowledge about Bob's measurement choices and therefore breaching the security of the protocols. In [6], the existing and new multi-photon assaults are described, as well as a theoretical framework for analyzing them.

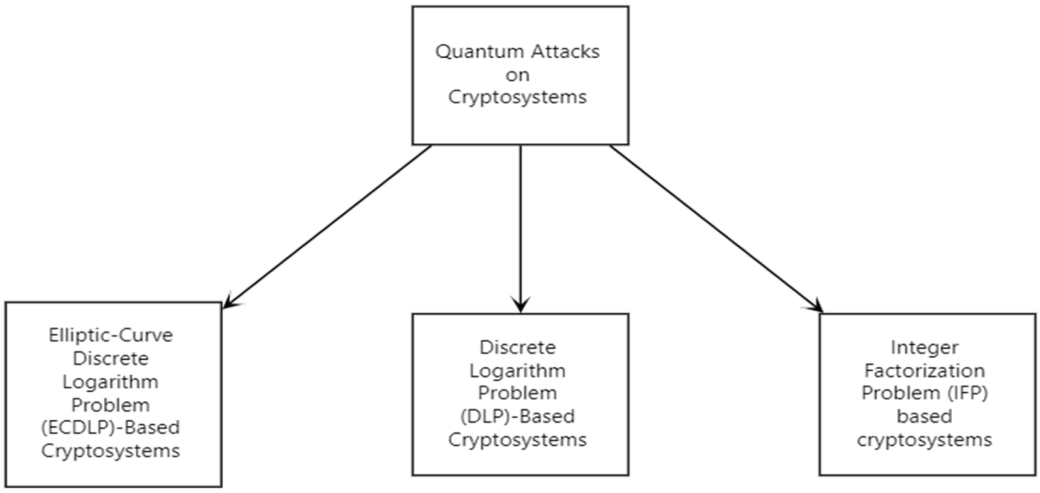

FIGURE 8. Quantum attacks on cryptosystems.

B. QUANTUM ATTACKS ON DLP-BASED CRYPTOSYSTEMS

In [7], the use of Shor's techniques for phase discovery is highlighted, and the DLP as functions to build a quantum approach for calculating discrete logarithms in semigroups. As a consequence, recommended cryptosystems that depend on discrete logarithms in semigroups' presumed complexity are susceptible to quantum attacks. On the other hand, the paper showed that while some variants of the discrete logarithm issue are straightforward in groups, they are difficult in semigroups. On traditional computing systems, the DLP is unsolvable, and all available DLP solutions are ineffective. As with IFP for RSA, this ridiculous efficacy of DLP may also be exploited to build cryptographic systems. Furthermore, because methods from one issue are frequently modified to the other, DLP and IFP are twin sister issues. Among the most common DLP attacks, as well as some of the most extensively used DLP-based protocols and cryptographic systems, are impenetrable in polynomial time by all classical assaults.

C. QUANTUM ATTACKS ON ECDLP-BASED CRYPTOSYSTEMS

Elliptic curves are a key component of contemporary cryptography architecture. They are involved in constructing public-key methods like digital certificates and key exchange that are extensively employed in various cryptographic systems more than thirty years since its inception to cryptography. The complexity of computing discrete logarithms [8] in the ECDLP is used to secure elliptic curve encryption. In [9], a new quantum method that uniquely uses Simon's sub-processes is introduced. Mostly in the case of a quantum attacker confined to conventional requests and offline quantum calculations, we can exploit the mathematical nature of cryptosystems. Numerous security solutions rely on cryptographic hash functions as a foundation. A hash function preimage attack seeks to locate a message with a certain hash value. A cryptographic function's preimage should be resistant to assaults. In [10], a novel quantum technique for hash preimage assaults is discussed that can overcome preimage resistant as circuit complexity increases. Using Shor's factoring algorithm, the technique permits gate-level evaluations to latest resource estimations. The findings back up prior estimates by Roetteler [166], indicating that the amount of qubits necessary to attack elliptic curves is fewer than that necessary to attack RSA for current parameters at comparable conventional security levels, implying that ECC is definitely an obvious option than RSA.

A QIA is a typical case of man-in-the-middle assaults that re-emerged in the headlines as one of WikiLeaks chairperson Edward Snowden's top ten largest revelations [170]. To effectively assault the target, the adversary would require surveillance skills. When the quantum servers have won the race against the original answer, the attacker can hijack important data such as usernames and passwords, banking information, and payment information, or even disseminate spyware that can communicate with a botnet Command and control server. As shown in Figure 9, the adversary waits on the connection for the victim to initiate a connection with a specific website in this quantum assault. Every quantum server is set up to meet specific requirements. The attacker is alerted of any inquiry from the victim that meets this set of requirements. The quantum servers [11] then provide a reply to the perpetrator's initial request. The infected payload is sent to the target, and the adversary has complete control over the victim. The website's initial answer packets are ignored.

D. QUANTUM RESISTANT CRYPTOSYSTEMS

Although quantum computing is still in its infancy, its development poses a danger to the most widely used public-key encryption schemes. Because of its capacity to handle the key distribution difficulty and provide strong protection in non-secure telecommunications systems that

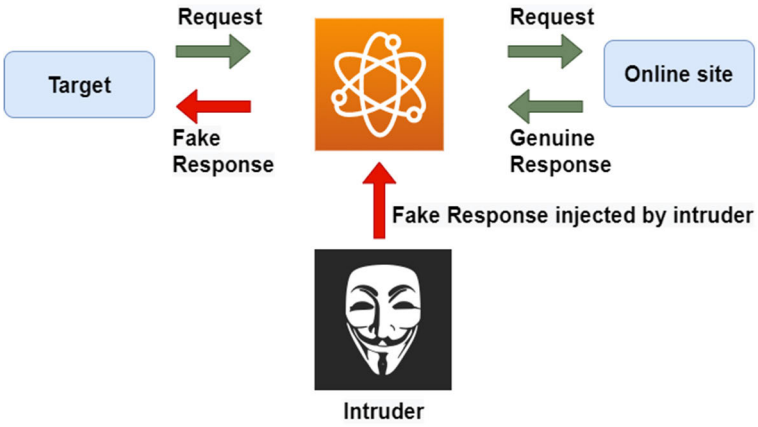

FIGURE 9. Quantum insertion attack.

allow for online browsing, e-mailing, banking transactions, digitally signed documents, and military networks, digital signatures, or health information, such systems are critical for contemporary online security [171], [172]. Researchers are working on techniques to combat quantum computing, which represents a lengthy threat to IoT device integrity. In [24], which provides a survey of what can be called post-quantum IoT systems (IoT structures safeguarded from currently available quantum computing threats), the primary post-quantum cryptosystems and proposals are reviewed, the most relevant IoT designs and difficulties are analyzed, and the anticipated future patterns are demonstrated. In [25], the examination on how to improve blockchain cryptography to withstand quantum computing assaults using Shor's and Grover's algorithms, resulting in the construction of post-quantum blockchains, is done. The paper initially presents a general overview of the present state of the art of post-quantum cryptosystems to aid scientists in the creation of such blockchains. The most significant post-quantum cryptosystems for blockchains, as well as their primary obstacles, are examined. The predicted timeframe for an attack-capable quantum computer [39], as well as the solutions for minimizing the danger, will be improved before the approval of quantum-resistance specifications. A company should develop a roadmap that follows these advancements in their particular environment, and they should keep it up to date over the next few years before quantum-resistant protection is standardized, approved, and deployed. The difficulties and drawbacks of quantum-resistant primitives, as well as the structure and possibilities of quantum computing, are well documented in the computer science, physics, and engineering literature. As quantum computing and quantum-resistant technology progress, multiple extensively researched laboratories keep this corpus of knowledge up to date. Nevertheless, there is a significant gap between practical and methodological comprehension of these innovations on the one side, and economic ramifications on the other.

E. SECURE SATELLITE AND UAV NETWORKS WITH PHYSICAL LAYER CRYPTO

UAVs are attracting overwhelming response across both civil and military applications to facilitate flexible satellite connectivity and deliver reliable communication due to their high agility and flexible deployment. Because UAV interactions are mostly conducted in an open environment, they can advantage from superior line-of-sight connectivity; nevertheless, this makes the UAVs more susceptible to unwanted monitoring or interference attempts. In [40], from the standpoint of PLS, a complete review of current advances in UAV-assisted wireless communications is done. The frequently used secrecy performance measures are reviewed, followed by a discussion of secrets performance evaluation and enhancement approaches for passively installed UAV systems. In the past few years, satellite communications scientific research has resurfaced in a big way. Due to the success of satellite communications' many telecom networks, safety concerns have grown, as the space information network is vulnerable to eavesdropping by illicit opponents in such a massive wireless network. PLS has recently evolved as a new security concept that uses the wireless channel's unpredictability to accomplish secrecy and verification. The PLS approach has been a success story for over a decade, and it continues to include a layer of security in satellite communications. In [41], a thorough examination of satellite communications is done, with a focus on PLS. 5G wireless technologies are a critical enabler for the emerging IoT infrastructures to fulfill their growing needs. PLS has lately attracted a lot of attention for wireless communication security in 5G IoT networks. In [42], a thorough overview of PLS approaches in 5G IoT communication systems is conducted. Perhaps one of the most formidable barriers to the incorporation of UAVs in commercial processes, including visual inspection, staff surveillance, and transportation, is the restricted source of energy and flight length of UAVs, as well as the necessity for qualified UAVs operators. In [43], the authors have proposed the AerialBlocks concept

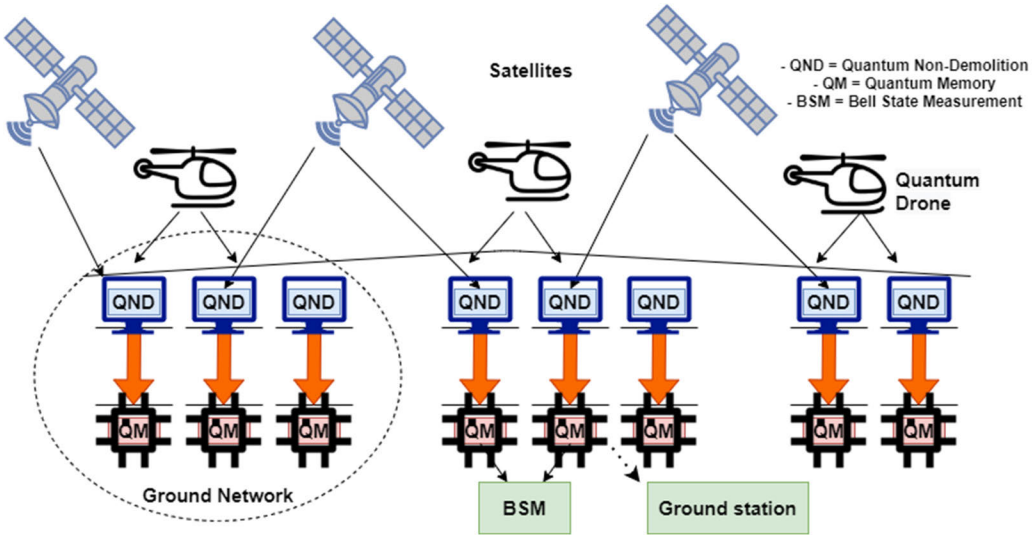

FIGURE 10. Architecture of a Q-repeater.

for blockchain-enabled UAV hybridization, intending to provide virtual UAV-as-a-service for commercial processes. AerialBlocks also wants to provide end-users with safe and enduring UAV services, as well as a semi-decentralized blockchain platform that provides security, confidentiality, quality of service, and visibility. In [44], the authors presented a novel DF-based safe 3D mobile UAV transmitting scheme for HSTNs in the vicinity of an aerial eavesdropper operating in a round area around a functioning UAV relay. In [45], the authors looked at reliable communication in a HSTRN, in which an adversary can intercept communications sent from both the satellite and interim relays. We investigate collaborative blocking by the relays to successfully shield the information from eavesdropping in these two stages, in which the jamming frequencies are designed to maximize the detection accuracy underneath the complete power limit of relays.

F. Q-REPEATER CRYPTO-NETWORK

The establishment of a universal quantum network would be a huge scientific and technical success since it would allow the transmission of quantum entanglement and quantum states between any two points on the planet's surface. The very well use of such a channel would be the quantum key transmission, a cryptography technique that guarantees connectivity with safety assured by physical rules. Additional QC concepts supported by such a network include blind quantum computing, which lets a client execute computations on a quantum computer without the computer knowing what they are doing, and personal database queries. For larger spans of a few thousand miles, low-Earth-orbit satellite connections may be the best option. Eventually, distances greater than 5,000 km will very certainly need the use of more remote satellites [173], quantum repeaters with low-Earth-orbit satellite connections, or low-Earth-orbit satellites outfitted with quantum memory, or a mix of these technologies. Long-distance coupling is a valuable asset, although it is difficult to distribute owing to light's exponential attenuation in optical fibers. Quantum repeaters relying on QEC or ES are one proposed approach. Satellite-based free-space optical communications, on the other hand, can be used to achieve improved loss-distance scaling. In [174], it is suggested to combine these two elements, quantum repeaters, and satellite-based communications, into a method that achieves entanglement distribution across long distances with only a few untrusted intermediary nodes. The presence of entanglement between two access points is required for quantum communication. Because local quantum processes can only create entanglement, pieces of the entangled structure must be distributed across separate nodes. Figure 10 shows the basic architecture of a QR, in which satellites are the sources, and every connection comprises of a low-earth-orbit satellite with an entangled photon pair source and two base stations with quantum memory and quantum non-demolition measurement devices. The QND devices, which detect the existence of a photon non-destructively and without exposing its quantum state, signal the receipt of a photon at each base station. The entanglement is then retained in the memory until a neighboring connection receives information about successful entanglement construction. Moreover, using entanglement switching based on a BSM, the entanglement may be prolonged. Spreading entanglement across vast distances is nearly impossible because of the very seasonal character of entanglement and the presence of impediments in the communication channel. To overcome this difficulty, quantum repeaters have been developed [175]. These allow long-range entanglement to be established by separating the connection into smaller sections, producing entanglement between every portion, then joining them to make the whole connection.

G. QUANTUM-SAFE INFRASTRUCTURE IN FIBER AND WIRELESS NETWORKS

The quantum computer poses a major threat to commonly used contemporary cryptography approaches, thanks to recent advancements in quantum computing and quantum cognitive science. That is because most cryptography issues that are unlikely to be resolved with traditional computing become quite simple with the supercomputer. In past times, lightweight encryption approaches have evolved that give security from quantum attacks. Such methods are referred to as ''quantum-safe,'' and they include both methodologies based on quantum nature of light that prohibit message interference and vintage mathematical methods, all of which were developed to withstand quantum attacks evolving from the rapidly advancing field of quantum computation. Quantum-safe communication protocols are incompatible with approaches used in quantum-vulnerable goods [176]. There is a period when new goods are slowly phased in, and older goods are phased out in a well-ordered and cost-effective technological transition. Quantum safe and quantum susceptible objects can now coexist in a connection; in certain circumstances, a well-ordered migration is possible. Nevertheless, the window of opportunity for a smooth transition is closing, and with the maturation of quantum computation studies, the possibility for transferring may already be closed for data that has to be kept secret for decades. Anything that has already been or will be communicated across a channel without quantum-safe cryptography is subject to snooping and public exposure. In [177], a customized SDN facilitator is explored, which estimates or configures local networks based on demands while also adding encryption using QKD and other methods. SDN administration of network resources delivered segments automatically, allowing for the adoption of encrypted connections as needed, including those that use quantum-resistant algorithms, QKD, standard Diffie–Hellman key exchange, or, as well as no encryption.

H. FUTURE RESEARCH DIRECTIONS FOR HANDLING QUANTUM ATTACKS

Massive quantum computers and the additional processing capacity they will provide might have disastrous ramifications for cybersecurity. It is believed that major problems like factorization and the continuous log, whose supposed complexity maintains the security of many commonly used protocols, may be handled rapidly if a quantum computer is big enough, ''fault resistant,'' and ubiquitous enough is constructed. There are several myths [178] if we discuss quantum computers. Some of them are mentioned below:

- Quantum computers are not quicker in the respect that they can perform more calculations per second. Quantum computers accomplish their processing speed up by allowing procedures to include actions that are exceedingly difficult for conventional computers.
- Quantum computers have an unusual technique of spanning the range of choices or computational branches. The behavior of quantum computers is analogous to that of conventional stochastic computers, with the key exception that quantum computers act as though they have ''probabilities'' that take model parameters.
- It is a required requirement, but it is not adequate. A quantum attacker can take advantage of quantumness in a range of methods, not just to solve particular classical tasks faster. Following that, we present examples of such assaults (approximation assaults) and explain why both the security concepts as well as the proof methodologies must be changed.
- BQP refers to a type of decision issue that quantum computers are capable of solving quickly. It is an (assumed) relationship to other classes. Even a small increase in speed may make a big difference in a lot of situations. It has an impact on the size of keys required to ensure a specified degree of protection in cybersecurity, for example.

QC, QKD, QSeS, and quantum direct communication have all received a lot of attention in recent years. Because these representations may be utilized to give quantum authentication, a study in these disciplines has facilitated quantum authentication research [179]. An intruder cannot measure the quantum state in motion since the recipient will immediately recognize it. Moreover, due to the HUP, an attacker cannot successfully clone or duplicate a quantum state, according to the no-cloning hypothesis of quantum computing. As a result, an attacker will be unable to analyze and then copy a quantum state, offering additional privacy and security considerations.

VI. QUANTUM ALGORITHMS AND DRONES

Discussing recent updates on quantum algorithms and drones, we have divided this section into quantum genetic algorithms, quantum genetic algorithms and drones, and future research directions in quantum algorithms and drones.

A. QUANTUM GENETIC ALGORITHMS

Quantum computing relates to the engineering area that uses quantum mechanical properties to decipher computational problems [180]. With quantum mechanical phenomena, numerous optimization issues are often solved efficiently. The key aspects behind the development of Genetic algorithms [181] are the assortment of the fitness function, size of the population, crossover probability, and mutation probability. Genetic algorithms exhibit a replacement population and produce a much better average fitness value. The combination of mutative algorithms and quantum computers gains popularity that ends up in an honest exploration of the worldwide search area in formulating quantum genetic algorithms [182].

QEA is considered by the illustration of the chromosome, the assessment function, and the underlying population forces. Rather than numeric, twofold, or symbolization, QEA mainly practices a quantum-bit (qubit) for possibility illustration that is used as a data representation. The main

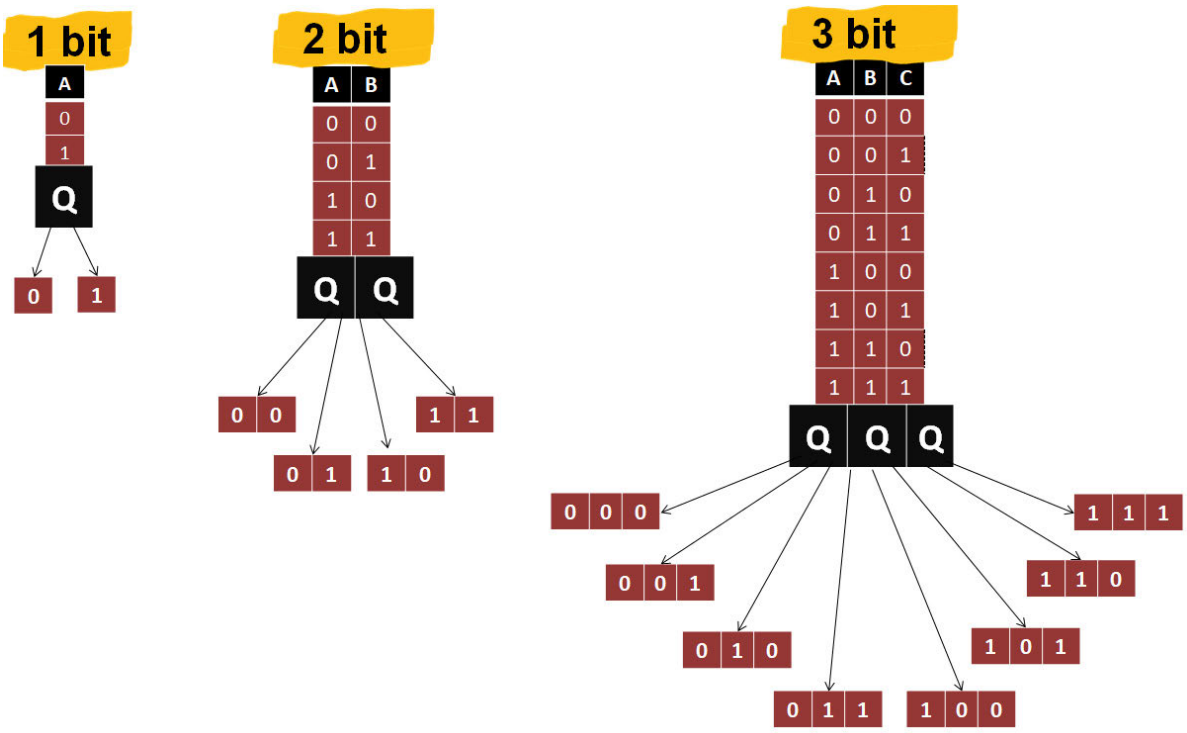

FIGURE 11. Superposition states of a quantum bit.

advantage of a qubit is that it can be in a superposition of states in a state space, meaning it can exist in multiple states at the same time. Comparing other representations, the qubit illustration has a higher character of the population. The quantum rotation gate is employed since it might facilitate the examining direction to the best space, and it also increases the speed of the algorithm. The mixture of mutative procedures and the quantum-based process from quantum mechanics together comprise the total quantum mutative algorithm. The ultimate intention is to practice the quantum doctrines like the state superpositions, quantum gates, and quantum registers to beat the extraordinary quality of optimization complications. The notable contribution includes quantum encouraged mutative computing by Han *et al.* [183] for solving the combinatorial optimization problem [184].

Quantum-encouraged genetic procedures do not need a real quantum system for solving the problem. Quantum principles which mainly comprise coherence, quantum parallelism, and superposition of states shown in Figure 11, rotation gates, and all possible spin of quantum registers, helps in maintaining the population diversity and also enlarge the scope. Lv & Liu [185] devised a quantum-encouraged genetic algorithm for cracking single objective optimization techniques and multi-objective optimization problems. The probability amplitude of the quantum bit is used for encoding. Quantum encoding is combined with crossover and mutation operators to increase the range of the population contained by minor population size and also

$$P_1 P_2$$
$$\downarrow \downarrow$$
$$\xrightarrow{Parent_1} \left|\begin{matrix}\alpha_1\\ \beta_1\end{matrix}\right|\left|\begin{matrix}\alpha_2\\ \beta_2\end{matrix}\right|\left|\begin{matrix}\alpha_3\\ \beta_3\end{matrix}\right|\left|\begin{matrix}\alpha_4\\ \beta_4\end{matrix}\right|\left|\begin{matrix}\alpha_5\\ \beta_5\end{matrix}\right|\left|\begin{matrix}\alpha_6\\ \beta_6\end{matrix}\right|\left|\begin{matrix}\alpha_7\\ \beta_7\end{matrix}\right|\left|\begin{matrix}\alpha_8\\ \beta_8\end{matrix}\right|\left|\begin{matrix}\alpha_9\\ \beta_9\end{matrix}\right\rangle$$

$$\xrightarrow{Parent_1} \left|\begin{matrix}\alpha'_1\\ \beta'_1\end{matrix}\right|\left|\begin{matrix}\alpha'_2\\ \beta'_2\end{matrix}\right|\left|\begin{matrix}\alpha'_3\\ \beta'_3\end{matrix}\right|\left|\begin{matrix}\alpha'_4\\ \beta'_4\end{matrix}\right|\left|\begin{matrix}\alpha'_5\\ \beta'_5\end{matrix}\right|\left|\begin{matrix}\alpha'_6\\ \beta'_6\end{matrix}\right|\left|\begin{matrix}\alpha'_7\\ \beta'_7\end{matrix}\right|\left|\begin{matrix}\alpha'_8\\ \beta'_8\end{matrix}\right|\left|\begin{matrix}\alpha'_9\\ \beta'_9\end{matrix}\right\rangle$$

$$\xrightarrow{Child_1} \left|\begin{matrix}\alpha_1\\ \beta_1\end{matrix}\right|\left|\begin{matrix}\alpha_2\\ \beta_2\end{matrix}\right|\left|\begin{matrix}\alpha'_3\\ \beta'_3\end{matrix}\right|\left|\begin{matrix}\alpha'_4\\ \beta'_4\end{matrix}\right|\left|\begin{matrix}\alpha'_5\\ \beta'_5\end{matrix}\right|\left|\begin{matrix}\alpha'_6\\ \beta'_6\end{matrix}\right|\left|\begin{matrix}\alpha_7\\ \beta_7\end{matrix}\right|\left|\begin{matrix}\alpha_8\\ \beta_8\end{matrix}\right|\left|\begin{matrix}\alpha_9\\ \beta_9\end{matrix}\right\rangle$$

$$\xrightarrow{Child_2} \left|\begin{matrix}\alpha'_1\\ \beta'_1\end{matrix}\right|\left|\begin{matrix}\alpha'_2\\ \beta'_2\end{matrix}\right|\left|\begin{matrix}\alpha_3\\ \beta_3\end{matrix}\right|\left|\begin{matrix}\alpha_4\\ \beta_4\end{matrix}\right|\left|\begin{matrix}\alpha_5\\ \beta_5\end{matrix}\right|\left|\begin{matrix}\alpha_6\\ \beta_6\end{matrix}\right|\left|\begin{matrix}\alpha'_7\\ \beta'_7\end{matrix}\right|\left|\begin{matrix}\alpha'_8\\ \beta'_8\end{matrix}\right|\left|\begin{matrix}\alpha'_9\\ \beta'_9\end{matrix}\right\rangle$$

FIGURE 12. Example of two point quantum crossover.

to extend the likelihood of finding the overall optimal solution.

Figure 12 and figure 13 show examples of quantum crossover and mutation operators. Quantum Bit (qubit) representation, consider a sequence of m-qubits, as given in (5.1)

$$\left|\begin{matrix}\alpha_1\\ \beta_1\end{matrix}\right|\left|\begin{matrix}\alpha_2\\ \beta_2\end{matrix}\right|\left|\begin{matrix}\alpha_3\\ \beta_3\end{matrix}\right|\left|\begin{matrix}\dots\\ \dots\end{matrix}\right|\left|\begin{matrix}\alpha_m\\ \beta_m\end{matrix}\right\rangle, \quad and\ |\alpha_i|^2 + |\beta_i|^2 = 1, \quad for\ i = 1, 2, \dots, m \tag{5.1}$$

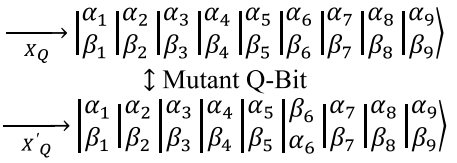

FIGURE 13. Example of a quantum bit mutation operator.

Quantum rotation gate [1], as given in (5.2), is used in quantum genetic algorithms.

$$R(\theta) = \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix}, \tag{5.2}$$

where θ is the rotation angle.

Figure 11 depicts the states of a quantum bit in superposition form. Examples of 1 qubit, 2 qubit, and 3 qubit states are depicted. For example, a three-qubit state can compute and work parallel on all eight different values 000, 001, 010, 011,100, 101, 110, and 111 at the same time.

B. QUANTUM GENETIC ALGORITHMS AND DRONES

Mousavi *et al.* [186] have proposed a leader-follower combination development procedure for a comprehensive UAV system. The authors propose multiple objective optimization algorithms while considering the subsequent cost minimization related to resource consumption of the combinations fashioned, increasing the trustworthiness of the fashioned combinations, and choosing the best suitable UAVs between them. Coalition Formation [187] could be a game theory problem in which the agents get together to create completely different teams with the most payoffs. There is no central controller because the failure of a controller can destroy the entire process, and also scaling up is difficult. A decentralized process of task allocation [188] is followed, where UAVs gain knowledge of the environment at runtime during the task [189]. UAV's divide tasks among themselves. They do not apprehend target locations and required resources, UAV's locations, and available resources. An important factor in coalition formation is trustworthiness. During the mission, the leader UAV will perform the assigned task by choosing the UAVs that have the highest operational capabilities. Each UAV encompasses a search state. Once a target is identified by a UAV, that UAV becomes a leader and identifies the other UAV by passing messages that are available within a small distance from the target. These chosen UAV's will have the required resources for completing the task. The leader and other identified UAV's will then form a group and complete the task by following the instructions of the leader UAV. The authors performed simulations in various scenarios with a huge number of UAVs and compared them with existing algorithms [190].

Yu *et al.* [191] considered the problem of optimizing SDS and cracked it using a quantum inherited procedure. First, from the dependency matrix of the faulty test and the diagnostic strategy, the amplitude of a quantum bit is constructed. The objective equation is framed as a dual equation by considering the expected test cost and the contributed tests. Finally, the mutative process is applied to obtain the optimum solution. The mutative process is obtained by using quantum encoding, which is constructed by considering quantum crossover and change operators. Figure 12 shows an example of a two-point quantum crossover. The benefit of using quantum encoding is, the population diversity can be increased even when a population of very small size is available. The global optimum of the problem can be reached by applying quantum Pauli rotation gates, quantum bit crossover operator, and quantum bit change operators. The authors applied their proposed algorithm to solve the control moment gyro system problem as a real-time application and proved that quantum genetic algorithms could solve sequential diagnostic problems in an optimized way.

Layeb [192] suggested a quantum-based coordination exploration procedure for solving the 0/1 optimization problem [193]. The author solved the problem of the multidimensional knapsack. Advantages of the algorithm are the representation of all possible solutions of a problem as a superposition of quantum states [194], quantum measurement as they are probabilistic offers a decent range to the problem [195], and quantum interference operation accentuates the search operation among the best solutions [196]. In a multidimensional knapsack, instead of considering one knapsack, m-knapsack of volume $c_j, j = 1, \ldots, m$ is considered. From the given items, the optimal x_i's are selected, and the selected item must be present in all the knapsack, with their weights depending on the knapsack j, for sample, an element which is selected can take load 2 in the first knapsack, can have load 6 in the second knapsack, and can have load 4 in the third knapsack and so on. The main aim of the procedure is to identify a group of elements using which the profit can be maximized, and the other constraint is the selected items must be available in all knapsacks. The authors have shown that representing solution states in a superposition of quantum states and by using the quantum interference operation, they were able to search among the best solutions to achieve the ideal result in the state space.

The idea of solving the pickup and delivery scheduling problem was considered by Rizk and Awad [197]. This is an important integration or application for the UAV system as well. The authors suggested a quantum-based genetic procedure for resolving the problem because a quantum algorithm has the capability of handling a huge set of combinations due to the state superpositions. Quantum encoding of states with equal probability of amplitudes for states 1 or 0 are used, and their mutation operator, for equality condition $\alpha^2 + \beta^2 = 1$ to be satisfied, modifies only α and β is calculated inside the algorithm. The total estimate of the problem is framed by considering the positions of start and endpoint, the distance between source and destination, the number of agents involved, and also the environmental conditions and fitness function are reciprocally proportional to the total estimate. The authors prove that their formulation

has led to an exponential increase in search space and shown that they are effective even in multiple scenarios.

Gu *et al.* [198] present a quantum chromosomal procedure for solving job-shop planning. The algorithm consists of sub-populations, and these sub-populations are further divided into clusters, and each cluster is called a cosmos [183]. The algorithm uses qubit representation, crossover, mutation, and rotation angle operators and also uses a calamity operator to evade early merging. First, the original population magnitude of all the populations, crossover likelihood, and mutation likelihood is initialized. Then represented the subpopulation in qubit representation, and for each subpopulation based on suitability value, quantum crossover and quantum mutation operator are applied. Next, apply the calamity operator. If early convergence has not occurred, apply the quantum rotation gate and recalculate the value. Next, the migration strategy is applied for each of the sub-populations in the universe. For all the universes, the quantum crossover operator is applied, and for each subpopulation, the best schedule is recorded. The process is repeated for all the cosmoses, and finally, the optimum solution is displayed.

Konar *et al.* [199] proposed a quantum-based genetic process and is used for solving multi-objective planning. First, a graph called a task graph is constructed along with priority. When the tasks arrive for execution, a queue is created. Based on the queue size, the size of the chromosome is set, and the initial population is randomly produced. The genes are evaluated, and a valid solution is selected using the capability function, and the capability value is calculated. Using the calculated capability value, the most suitable genetic material is chosen, and quantum replacement gates are applied on quantum bits constructed from the higher genetic material to generate a new population. The fitness value of each chromosome is evaluated in binary representation, and the appropriate chromosome is a selection from the population, and the job is scheduled in the selected workstation. The process is repeated for all tasks.

Xing *et al.* [200] proposed an algorithm for cracking the feature of service multicast routing problems in WDM-based optical networks. The algorithm uses the ME mechanism to increase the convergence speed, AQM operation to avoid the algorithm from limited exploration, and a reparation method for calculating fitness. Initially, an N-qubit chromosome $Q(t)$ is constructed, all legal paths are calculated using the reparation method and stored in $path(t)$. The finest $path(t)$ is chosen, and its fitness value is calculated and stored. The process is repeated till the termination condition is not met. Next, $Q(t) - 1$ is chosen, and $path(t)$ is constructed and evaluated. Find the best $path(t)$ and store it along with its fitness value and apply AQM operation in every iteration. The authors have proved that the algorithm performance has been improved drastically.

Dahi *et al.* [201] proposed a quantum-based genetic procedure supported by a quantum rotation gate for deciphering the APP. The large quality and availability of the facilities projected by mobile networks have created a trade-off with great standards. The algorithm starts with chromosome initialization, creates a mating pool by selecting a portion, applies qubit crossover, qubit mutation, and interference operators based on quantum principles, measures and evaluates the individuals, and replaces the old population with the new population. To calculate the measurability, productivity, and hardiness of the algorithm, the area of the experiment is unit administered on genuine, artificial, and arbitrary levels with totally diverse proportions, and the authors have shown that their approach can solve the APP problem efficiently.

C. FUTURE RESEARCH DIRECTIONS IN QUANTUM ALGORITHMS AND DRONES

It is observed that the Quantum drone area is not researched much. Quantum algorithms and drones will notice several applications in time-period systems, fog computing, and mobile-cellular networks. Soft real-time tasks and hard real-time tasks are the major classifications of period tasks relying on deadline compliance. The principal characteristic of exhausting time-period systems is to ensure total point compliance, and failure to satisfy deadlines ends up in ruinous consequences. Contrastingly, the presentation amount of soft real-time-period schemes mainly exists within the improvement of point compliance. The assorted requests of time-period systems embrace medical purpose, method management, technical research, satellites, control, area systems, sensing element systems, automation, and drones. Quantum based genomic process suggested by Narayan and Moore [202] has been studied to resolve a large set of problems, which includes knapsack problem, calculation of the partition problem, blind signal separation problem in signal dispensation, IIR systems, traveling salesman problem, knapsack, Max Sat problem, and image registration.

Quantum genetic algorithms are capable of solving several practical, inspiring difficulties in various manufacturing arenas, shipping, wrapping, and network-based areas, the feature assortment computation problem, traveling salesman computation problem, the variation flow-shop computation problem, the container packing computation problem, the knapsack computation problem, the lot-sizing computation problem, the job-shop computation problem, and the quadratic assignment computation problem. In the field of fog computing [203], the main challenges to be faced are security and trait, mainly for a distributed environment. Major open research areas of fog computing include network information measures and resource allocation.

VII. PQC

Quantum and Post-quantum cryptosystems are different domains. QC is likewise based on the HUP. The principle says that a particle's momentum cannot be precisely quantified. QC applies the principles of quantum mechanics to ensure that only the legitimate recipient should be able to understand the information. With quantum computers, there is always a risk of breaking the keys. Thus, longer keys are

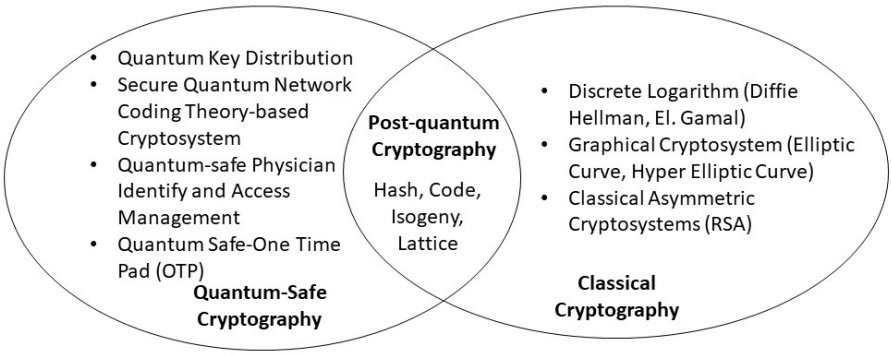

FIGURE 14. Classical vs quantum-safe cryptography vs post-quantum cryptography.

required to make the communication secure. Post-quantum cryptosystems are sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant mechanisms as well. Post-quantum cryptosystem is an approach that is theoretically proven to be secure from any cryptanalytic attack using a quantum computer. A quantum computer attack may be blocked using PQC. Complex mathematical problems require conventional computers months or even years to solve. Quantum computers, if they use Shor's algorithm, can destroy math-based systems in just minutes. On the other hand, PQC utilizes principles of quantum physics to transmit secure communications, and unlike mathematical encryption, it is completely un-hackable. Figure 14 shows the difference between quantum-safe cryptography, classical cryptography, and post-quantum cryptography. This work discusses PQC aspects. Details are presented as follows.

A. TYPES OF PQC

PQC is also referred to as a quantum-proof, quantum-safe, or quantum attack-resistant system. In the classical cryptosystem, there are three types of hard mathematical problems, including IFP, DLP, ECDLP. As discussed in the previous section, the classical cryptosystems are easy to break using Shor and Grover's algorithms running over quantum computers [1]. This section discusses the importance of PQC to secure data and applications against quantum attacks. Table 5 presents the analysis of recent post-quantum cryptosystems. In PQC, there are four major types of cryptosystems, including code, lattice, hash, and multivariate-based cryptosystems. The latest advancements in these cryptosystems are discussed as follows.

B. CODE-BASED CRYPTOSYSTEMS

This section explores code-based cryptography, i.e., cryptography primitives that use error-correcting codes for security purposes. McEliece [204] cryptosystem was the first coding theory-based cryptosystem designed in 1978. In [205], Niederreiter's public key cryptography-based error-correcting codes scheme is proposed, whose security is found to be equivalent to the McEliece scheme. Presently, McEleiece and Niederreiter schemes or their variants are popularly used in error-correcting codes-based cryptosystems. These existing code-based primitives have large key sizes. However, attempts have been made to reduce the key sizes and improve the performance. A few of these schemes are discussed as follows.

1) CODE-BASED SIGNATURE SCHEMES

This section discusses various code-based signature schemes in PQC [2]. In code-based signature schemes, hash-and-sign and Fiat-Shamir transformation are two important categories. Various variants of these schemes are briefly discussed as follows.

a: COURTOIS et al. SCHEME

This scheme is known as the hash-and-sign scheme. In 2001, CFS [206] proposed a code-based signature scheme with increased error correction capability and the ability to find the nearest word to a given codeword. This identification of codeword is tried to be identified with maximum probability. In the CFS scheme, signatures are generated using various operations like hashing, syndrome generation, multiplication in field, error pattern analysis, and counter value measurements. In this scheme, attacks are also observed [2]. For example, generalized birthday attack. To avoid such attacks with increased complexity, the signature generation time increases proportionately. Thus, this is not considered to be a good scheme.

b: STERN'S IDENTIFICATION SCHEME

This scheme is a type of Fiat-Shamir transformation-based approach in which identification schemes are modified to signature schemes. This type of scheme is considered to be secure because of the use of the random oracle model. In, this scheme is associated with a quantum-immune identification system. Further, the presence of quantum adversaries, security of quantum oracle model, presence of active adversaries, an association of Fiat-Shamir results with quantum oracle model, and modification of existing identification scheme to quantum immune digital signature scheme are some of the areas that are yet required to be explored.

TABLE 5. Comparative analysis of recent post-quantum cryptosystems.

Author	Year	PQC	PKE/DS	Major Findings	Major Shortcomings
Courtois et al. [206]	2001	Code-based	DS	This work has proposed a McEliece-based digital signature scheme. The proposed security scheme support signature of 81-bits and it is strong against syndrome decoding problem.	The major issues with McEliece-based digital signature are (i) large key size which causes implementation difficulties, (ii) large digital signature size transmission over limited bandwidth causes transmission errors, and (iii) easily prone to attacks if implemented in authentication processes.
Kabatianskii et al. [207]	1997	Code-based	DS	In this work, random error-correcting codes-based digital signature scheme. This scheme is based on the concept that inspite of the fact that the set of correctable syndroms is nonlinear in nature, it includes a sizable linear subspace.	This scheme is old and thereafter many challenges were observed in code-based cryptosystems including large key size, large digital signature size, and chances of attacks.
Zheng et al. [209]	2007	Code-based	DS	In this work, a code-based ring signature scheme is proposed. The signature size varies with number of members in the ring.	This work has performed cost and length analysis. However, this work can be extended to perform comparative analysis with existing code-based approaches to uidentify its adaptability to both resourceful and resource-constrained environments.
Malina et al. [211]	2021	Code-based	PKE & DS	This work has surveyed the important code-based cryptography approaches including encryption, key exchange and signature-based schemes.	This work has presented several use cases and hardware-level discussions for PQC. This work can be extended to analyze attacks scenarios over use cases and hardware-based implementation (theoretically or practically).
Jäämeri [212]	2020	Code-based	DS	This work has conducted in-depth survey of linear codes, and the important error-correcting codes that can be used in code-based cryptosystem. Further, important classes of code-based cryptography are presented with attacks and countermeasures.	This work can be extended to identify the taxonomies in various concepts of code-based cryptosystem. Further, structural properties and weaknesses can be explored in-depth. Likewise, novel countermeasures including rank metric adoption in code-based cryptography are found to be susceptible to structural attacks. Thus, construction of rank metric can be explored to avoid attacks.
Kumar et al. [213]	2020	Hash-based	DS	This work has focused over the eXtended Merkle Signature Scheme (XMSS) and its integration with security operation center with FPGA-based implementation.	This work is focused over specific use-case. This work can be extended for evaluation in other application domains with XMSS integration with other post quantum approaches. Here, more focus is drawn towards performance evaluation and comparative analysis. However, attack or vulnerability-based analysis or scenarios can be taken in future.
Lizama-Pérez et al. [214]	2019	Hash-based	PKE & DS	This work has proposed a digital signature scheme which is based on hash-based post quantum and public key cryptography. Here, performance of proposed approach is analyzed and it is observed that the proposed approach is good for mobile networks because of its high speed and low hardware requirements.	This work is focuses over digital signature mechanism discussion, mobile network scenario discussion and performance analysis. Work can be extended to analyze the proposed approach over alternative hardware implementation and countermeasure against various attacks. Further, lightweightness property of proposed approach for resource-constrained devices in IoT network can be explored.
Chalkias et al. [215]	2018	Hash-based	PKE & DS	Discussed the blockchain-based post quantum cryptography approaches and their advantages like short signature, computational efficiency, easy customizable option for applications,	This work can be extended to address issues like how blockchain-based post quantum cryptosystem performance can be increased with reduction in signature size. Further, various graph-based structure and their importance to blockchain enabled post quantum approaches can be explored. In hash-based digital signature approaches, protocols in stateful, stateless and postquantum cryptography can be explored in depth.
Butin et al. [216]	2017	Hash-based	DS	This work has proposed the integration of XMSS hash-based post quantum signature scheme with OpenSSL to ensure authentication.	This work has integrated XMSS with OpenSSL and performed some testing and validation of proposed scheme in a specific scenario. This work can be extended to test the proposed approach against attacks. Further, the chances of vulnerabilities and loopholes in taken scenario can be considered.
Potii et al. [217]	2017	Hash-based	DS	This work has carried out the analysis of digital signature algorithms based on hash functions. Here, XMSS algorithm is analyzed.	This work has performed experimentation to analyze the delay in key generation, signature generation and verification, and priority approach. This work can be extended to have more in-depth delay and attack analysis with better result presentation.
Wang et al. [218]	2021	Lattice-based	PKE	A LWE variant named Learning With Modulus (LWM) is proposed in this work. LWM properties with comparative to LWE with an addition of improved performance which is comparable to Linder-Peikert (LP) scheme.	This work can be extended to analyze the proposed scheme against various attacks. For example, broadcast, algebraic and generic attacks are few examples that can be explored against proposed scheme.
Lu and Zhang [219]	2021	Lattice -based	PKE	This work is a short description of lattice-based public-key encryptions (PKEs) and signature schemes. Further, Key Encapsulation Mechanisms (KEMs) are briefly explored.	In addition to in-depth computational problem issues, this work can be extended to include other challenges including attacks, vulnerabilities, algorithmic structures, and various comparative analysis of KEMs performances and challenges.

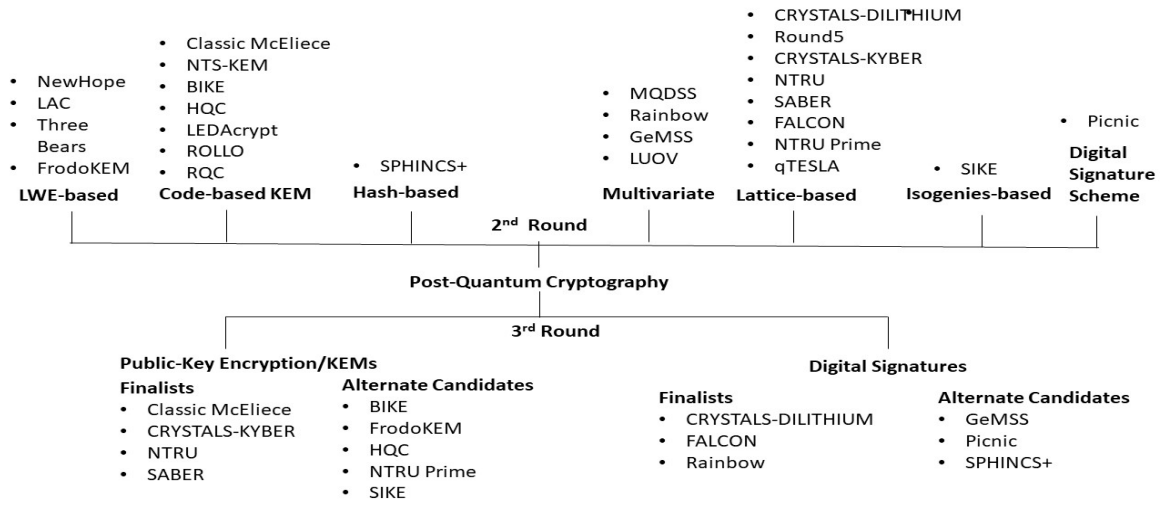

FIGURE 15. NTRU's 2nd and 3rd rounds of post-quantum cryptography.

c: KABATIANSKII et al.'s SCHEME

This is a digital signature scheme proposed in 1997 with four variants [207]. This scheme uses random error-correcting codes in the signature process. In [208], it is observed that this scheme is no more secure. Here, the condition to break the signature scheme is discussed. As a result, it is found that all three signature schemes proposed in the original work are not secure if at most 20 signatures are intercepted by an attacker. With this interception, an attacker will be able to recover the private key. In [208], recommendations are made to improve this scheme as well. The improved version has the provision to apply the multi-time signature formula. This makes the approach more secure compare to the original form.

d: ZHENG et al.'s SCHEME

In [209], this code-based ring signature scheme is proposed. This approach is an extended version of the McEliece-based digital signature scheme discussed by Courtois *et al.* [206]. In [206], it is observed that the McEliece-based digital signature scheme is having a large key size and signing cost. However, signature length and verification costs are very small. Thus, Courtois *et al.*'s extension is not a major variation of the McEliece-based digital signature scheme. Melchor *et al.* [210] observed that Zheng *et al.*'s scheme is difficult to use in practice and slower compared to other approaches.

Likewise, various code-based cryptography schemes are proposed in recent times [206], [207], [209], [211], [212]. These schemes presently suffer from various attacks (like Overbeck attack, attacks over twisted Reed-Solomon codes, and attacks over twisted Gabidulin codes). Additionally, there are many structural weaknesses in the proposed approaches. For example, rank metric codes are highly susceptible to structural attacks, the unfeasible key size is a major challenge to secure post-quantum approaches, and structures designed cannot be uniformly applied to every code-based cryptography approach. Among others, syndrome decoding, low weight codewords, large weight ternary syndrome decoding, McEliece-Goppa syndrome decoding, rank-metric syndrome decoding, and syndrome decoding in various other metrics are important challenges to address in the future.

C. LATTICE-BASED CRYPTOSYSTEMS

As shown in figure 15, there are 8 candidates (CRYSTALS-DILITHIUM, Round5, CRYSTAL-KYBER, NTRU, SABER, FALCON, NTRU Prime, and qTESLA) in the lattice-based cryptosystem of NTRU's 2nd round. In the 3rd round, 2 finalists (CRYSTAL-KYBER and NTRU) and 1 alternate (NTRU Prime) lies in public-key encryption, and 2 (CRYSTALS-DILITHIUM, FALCON) lies in digital signature finalists. There are various recent studies conducted over lattice-based cryptosystem useful to various other technologies or areas. Few of these recent studies are discussed as follows.

- Ravi *et al.* [16] prepared an in-depth study over lattice-based cryptosystem. The important lattice-based cryptosystem that is discussed in this study includes two major classes: LWE/R-based schemes and NTRU-based schemes. This article has discussed the algorithms, scope, pros, and cons in detail.
- Qian *et al.* [230] applied a data aggregation scheme in residential networks for smart grids. In this approach, lattice-based homomorphic cryptography is applied for resisting the networks against quantum attacks. The data aggregation approach is an aggregate signature scheme, and it is proven to be more secure because of its properties in implementing the security aspects, including PQC. In this work, the cryptographic algorithms are designed to be lightweight so that they

can work in residential area networks and can give better performance. The proposed security model is lightweight, and it is measured with computational and communicational costs that occur during its implementation in the residential network. In terms of security, the proposed approach claims message consistency, user privacy, and strong against attacks.

- Lu and Zhang [219] discussed the computational problems, security issues, and research challenges in lattice-based cryptography primitives. In this work, the major application areas of lattice-based cryptosystem are found to be in key exchanges, public key encryptions, and signature schemes. This work presents the importance of the most promising lattice-based candidates. For example, Hyber, LAC, LWE-variants, and few others. In this work, general observations of lattice-based cryptosystem and associated primitives are briefly explored.
- Li *et al.* [229] proposed a lattice-based signature scheme. The proposed scheme is tried to be integrated with blockchain-enabled systems. In the proposed scheme uses bimodal Gaussian distribution to make it a more efficient and random oracle model to make it more secure. The proposed approach is simulated, and comparative analysis with RSA and ECC is drawn. Results show that an increase in signature size with an increase in security level is lesser compared to RSA and ECC approaches. This concludes that the stability of the proposed approach is higher compared to other approaches.
- Buell *et al.* [228] discussed the basics of lattice-based cryptosystem and focused on NTRU public-key encryption approach. Discussion over the failure of the RSA cryptosystem and adoption of lattice-based cryptosystem is proposed in this work. This work discusses the recent trends of the problem of short vectors in lattices.

Likewise, there are many lattice-based approaches proposed during recent times. These approaches fall largely in LWE/R-based Schemes (LPREncrypt PKE Scheme, and Noisy Diffie Hellman Key Exchange), Key Reuse in LWE/R-based Schemes, NTRU-based Schemes, or Use of Error-Correcting Codes in Lattice-based PKE/KEMs. The major challenges in lattice-based cryptosystems include (i) selecting the optimal parameters in lattice-based schemes that ensure protection against attacks and provide minimum distance between two moduli. This can ensure a secure lattice-based digital signature approach in the future, (ii) achieving an efficient and secure implementation of lattice-based schemes is important to address, (iii) exploring the algebraic structures that provide an ideal lattice with optimization to modulo arithmetic can provide faster execution to lattice-based schemes, and (iv) memory footprint, efficiency, security assistance and applicability of implementation to different applications are important challenges in this cryptosystem.

D. HASH-BASED CRYPTOSYSTEMS

In [213]–[217], various hash-based post-quantum cryptosystems are proposed. The major challenges in this cryptosystem are (i) large message digest value which makes this category not appropriate for resource-constraint devices or fast response required resourceful devices. The strongest mechanism in this category of the algorithm includes LMSS or MSS. In terms of digital signatures, hash-based cryptography is an alternative to quantum-proof cryptography that is primarily geared at verifying digital signatures. Despite the challenges that quantum assaults provide for hash-based encryption, digital signatures produced by these methods are not number theory issues and are protected from attacks that quantum computers use to overcome existing cryptography. For each new communication, new keys must be produced, and keys from past messages must be monitored to avoid key recycling. The major challenges in this type of cryptography include large signature size, large key size, and complex key generation process, and optimization of parameters associated with public key encryption or digital signature.

E. ISOGENY-BASED CRYPTOSYSTEMS

The major challenges identified in isogeny-based cryptosystem include [206], [208], [210], [219], [227]–[230]: (i) how to avoid fourth root attacks in isogeny walks and cryptanalysis processes, (ii) ensuring collision resistance or preimage resistance in the use of secure hash functions for graphs of supersingular isogenies, (iii) designing strong mechanisms that avoid generic (computational-based) and other (active or side channel) attacks, and (iv) designing software or libraries that improve isogeny-based approach's performance on resource-constrained devices. Many efforts are made to propose a supersingular isogeny-based cryptography approach having a small key size. This makes an isogeny-based system suitable to those applications that required limited bandwidth, especially in IoT environments.

F. MULTIVARIATE CRYPTOSYSTEM

In multivariate cryptosystem, the major challenges observed in recent study include: (i) public key size is large (tens of Kbytes). Thus, this cryptosystem is suitable for generic computers, but a smaller key size is expected to successfully implement over small devices having a scarcity of resources. In [231], small key size-based schemes are compared to identify the machine suitable for various available hardware. However, efforts need to be drawn to make it suitable for sensor or RFID devices. (ii) Presently, formal security proofs of multivariate public key schemes are not explored much. Thus, there is a need to focus on matching the theoretical results with experimental work, and (iii) The direct and structural forms of attacks (like rank and differential attacks) are yet required to be analyzed for multivariate cryptosystems. In addition to challenges, the multivariate approach provides various advantages, including [231]: (i) multivariate system provides fast execution compared to other post-quantum

cryptosystem approaches, (ii) multivariate system is more suitable to resource-constrained devices (like smart cards, sensors, or RFID devices) because of use of simple arithmetic operations in these schemes, and (iii) smaller digital signature size compared to other PQC approaches is another advantage that this scheme offer to all types of devices for fast execution.

VIII. QFA AND DRONES

Drones and their application can serve many functions, from surveillance to humanitarian aid. The study based on QFA focuses on studying a mathematical model based on quantum systems with finite memory; QFA's have outperformed the traditional counterparts, serving more straightforward techniques, offering relatively robust solutions to specific problems. The main three advantages offered by QFA are space efficiency in solving promise problems and language recognition. The quantum state of such automata is always finite-dimensional, helping to characterize the class of languages recognizable by QFAs. Some other results exploring the parallels between QFAs and Markov chains are also an added advantage. The two types of control systems as Discrete Event Systems and Continuous Variable Dynamic Systems can be studied, where drone applications can be explored to empower the measures of QFAs. The standard drone uses with QFA allows management to understand performance drivers in diagnostics.

QFA theory can be applied to small devices like drones. Quantum superposition is faster compared to probabilistic superposition. Likewise, quantum shows many properties that give advantages over classical finite automata and can be preferred for small devices like drones. Quantum dynamics must be reversible, however, which may put computational constraints on machines having a scarcity of memory. Drones have a scarcity of resources. QFA is not yet explored for drones. However, finite state automata have shown various advantages to drones. For example, Hoffmann *et al.* [232] discussed the use case of drone control. Drone control feature is required in single drone movement for applications (like aid in disaster recovery, sanitization, medicine transfer) or multi-drone activity for collision avoidance. Drone states can be defined with automata network encoding, and the drone's controlled and exogenous states can be defined. Figure 16 shows an example of a finite-state machine for quantum drone-based patrolling and data communication. This way, an in-depth analysis of drone states can be determined, and drone movements can be controlled. For example, the formation of the finite state machine for multiple UAVs to solve an assigned task is shown in figure 17. Zhou *et al.* [233] discussed the problem of solving the formation of multiple UAV's using finite state automata. The steps followed for multiple UAV movement in finite machine are described as follows:

1. Models considered during UAV formation are free to fly M_1, creating the initial formation M_2, retaining the formation M_2, update the formation M_4, avoid formation M_5.
2. Based on the UAV formation in Step 1, updating the situation between the states of the two UAV's is determined. UAV's initial command for formation is named as C_1; constraints are satisfied by the formation is named as C_2, the existence of an obstacle within a range is defined as C_3, No obstacle existence within a range is denoted as C_4, a UAV joins the formation is denoted as C_5, a UAV leaves the formation is named as C_6, UAV's start a combined task is defined as C_7, UAV's end a combined task is defined as C_8, the command for destroying formation is denoted as C_9.

Small size QFA is also possible. Small-sized QFA exhibit periodic behaviors [234], making quantum computing and paradigm better than classical devices. Thus, this may be good for resource constraint devices like drones. Bianchi *et al.* [234] studied Bertoni's statistical framework for the synthesis of small QFA. Further, efforts are made to improve the size of QFA by varying the modules. Additionally, the solution to promise problems on different QFA is important for resource-constrained devices. This is because of a significant reduction in the number of states as compared to classical finite automata. Hoffmann *et al.* [232] also discussed one case study of human-robot collaboration. This study helps determine the state of a machine or robot and how humans can efficiently control it. Similarly, work can be extended to study the importance of the promise problem in QFA and drones for reducing the states and achieving maximum efficiency in operations. There are three types of QFA that are widely discussed in recent studies. This includes (i) One-way QFA, (ii) Two-way QFA, and (iii) Enhanced QFA. The quantum interactive proof systems correlate with algebra and QFA models such as 1-way QFAs. Latvian QFAs can be hit on to the market and the needs with drone applications in terms of several parameters such as computational power, closure properties, comparison, and inclusive relation with the models used in QFAs.

IX. CHALLENGES, LIMITATIONS, AND DISCUSSIONS

This section discusses the important research challenges, limitations, and findings in quantum computing or related studies. Details are discussed as follows [235]–[246].

A. RESEARCH CHALLENGES

Although the quantum area is not new, there is a wide scope of improvements in quantum associated applications, systems and

- *Lack of Efficient Devices:* Universal quantum computer devices from IBM, Google, and Intel appear genuine. However, there is typically a lower number of qubits available for usage due to error correction. So, nowadays, even an average laptop can use software tools to simulate the functioning of 30–40 qubits, as shown by an ordinary laptop.
- *Quantum Computing and Healthcare:* Quantum computing and storage facility may be a repository for Big Data analytics in the healthcare industry. Data

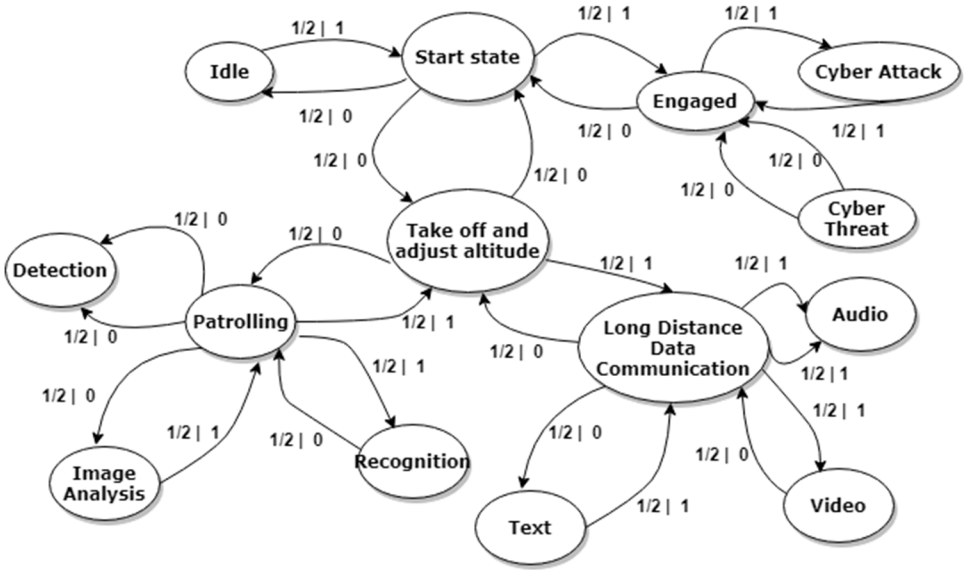

FIGURE 16. An example of finite-state machine for quantum drone-based patrolling and data communication.

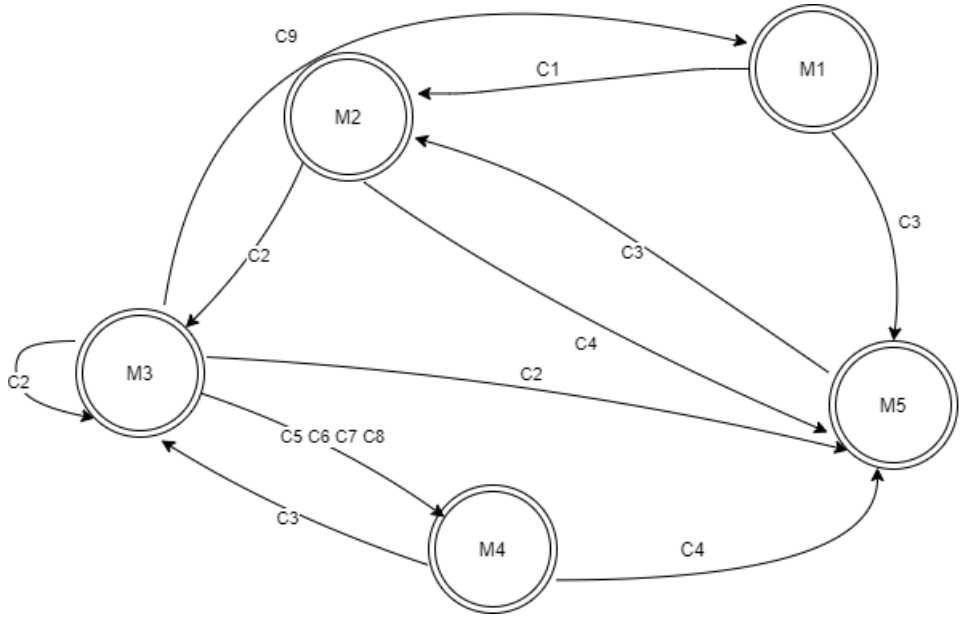

FIGURE 17. State diagram representation of finite state automata.

is distributed widely across the healthcare industry, making it easier to extract data from. It is worth doing because of the fundamental units of Quantum computing in removing the heterogeneity or variety problem in Big data.

- Gate error, relaxation, dephasing, readout error, and crosstalk are all examples of disturbances and defects that may occur in quantum computers in the contemporary age of quantum computing. Aside from that, they offer a limited number of qubits that are connected in a certain way.
- *Input and correlation cost:* Quantum algorithms may be useful for processing data but are rarely advantageous for reading data. The reading of the input in certain instances drives the cost of quantum algorithms. This needs further investigation. Further, quantum algorithms are needed to be explored for correlating inputs to outputs. In recent observations, quantum computing is found to be costly in this machine learning-integrated scenarios, i.e., learning the solution from quantum algorithm as a bit string makes QML inefficient.

- *Variation in performance:* The performance of quantum algorithms varies with domain and application. In certain scenarios, heuristic approaches or post-quantum mechanisms are found to be better. Thus, there is a need to mark quantum algorithms before claiming them to be the most efficient approach.
- *Improvement in Quantum Entanglement:* Recently, many studies realizes the importance of quantum entanglement in different applications. Likewise, simulations for quantum entanglement have proposed improvements in various factors like coupling, sustainability, and returned fields. However, this work needs to be extended in many other quantum entanglement improvement directions like pure states, ensembles, improving density metrics, and non-local or steerable states.
- *Cost Issues:* Quantum devices are costly as compared to classical devices. For example, efforts are performed to lower the cost of a cryogenic refrigerator [243].
- *Quantum radar issues:* In quantum radars, there are many issues, including minimization of signal losses due to wires, design, material, diameter and length of wires, the architecture of signal flow, total cost reduction, optimal cooling units, and associated parameters, novel designs requiring low temperature-based operating conditions, cryogenic dilution refrigerators usage and improving transit power are few issues need to be handled.
- *Lack of hybrid quantum-classical algorithms:* There is a lack of hybrid classical-quantum algorithms. Such algorithms are capable of executing the critical part over quantum computers and another bulky part over classical computers. This progression can make error-free computational feasibilities. Thus, it would be easier to handle the computational tasks with the present conditions of a noisy quantum computing environment.
- *Lack of large-scale quantum computing:* To solve complex challenges, a quantum computer is expected in nearby future. Large scale computing is possible through various means, including efficient hardware (i.e., physical implementation), more qubit design computer, distributed topologies, algorithm optimization with less storage, MLor deep quantum learning, and quantum logic gates and circuits, variations in the type of qubits, and efficient electronic design for qubits.
- *Scope of new solutions:* Quantum computing has the potential to provide environment-friendly technologies and solutions. Solutions like new energy and power system with heat, water, and wind would be interesting to investigate. Thus, it has wide research scope to explore.

B. LIMITATIONS

This section explores the major limitations in studied areas. Details are presented as follows.

- The present quantum computing has the limitation of representing one classical result in output irrespective of the qubit property of holding multiple values. This property indicates that the output will be probabilistic rather than deterministic. Here, if the desired outcome is not achieved, then multiple and repeated runs must be executed.
- The decoherence issue caused by vibrations, temperature variation, electromagnetic waves' nature, and other environment interaction destroys the quantum properties. Thus, the presently designed quantum computers are not expected to return correct results. The existing hardware to maintain coherence is not sufficient. Thus, there is a need to design and manufacture hardware that supports large-scale computations.
- The present quantum or classical computers are affected by various sources of errors. There are no QEC schemes that consume a large number of qubits for error correction. There is a need for such algorithms that handle storage, logic, and computational facilities efficiently by reducing the complexity of their execution.
- The present quantum computers have 65-qubit availability, and efforts are in progress to make 1121-qubit computers by 2023 [244]. Thus, the present quantum computers have very limited quantum bits support, which is not sufficient to perform heavy computational tasks.
- There is a lack of optimization algorithms and other algorithms that perform meaningful tasks. Without these algorithms, it would be difficult to perform useful tasks in a noisy environment. Thus, there is a need to overcome this limitation.

C. IMPORTANT DISCUSSIONS

Quantum areas for evolving day by day. Kop [247] identified 6 key application areas of quantum technology. This includes quantum computing, communication, sensing, simulation, science, and AI. Quantum computing is itself a big domain. It incorporates various other concepts, including qubit implementations, gates, circuits, algorithms, interfaces, and software components. In [247], the important aspects, directions, application areas, and principles are discussed in detail. Further, the importance of quantum concepts, their relation to lack of international policy, inaction, and consensus and risks in various sectors are explored. Here, it is strongly emphasized that quantum technology is playing and will continue to plan an important role for entrepreneurs, scientists, programmers, and governments, provided this technology should ensure ethical guidelines. In a real-world scenario, quantum is having importance and applications in various areas, including finance, chemistry, traffic engineering, space exploration, cryptography, environment-friendly solutions, cloud computing, distributed navigation and coordination, and many more [247]. Among these, quantum drones, satellites, and networks can be popularly

used for mission planning and scheduling, distributed navigations and coordination, object detection, environment cleaning, quantum internet, and space exploration. In another attempt, Liu *et al.* [8] discussed the first approach in designing mobile entanglement distribution using drones. This approach is designed to work in all weather conditions. This multi-weather system is flexible and cost-effective in QKD teleportation, repeaters, and other areas. The quantum-based technologies can integrate existing infrastructure with long-distance connectivity and are helpful for space, air, and underwater technologies and networks. Ball *et al.* [248] discussed the importance of software tools in quantum control solutions. Real-time experiments-based observations are identified for reducing the error and noise and improving the performance of the quantum computer. In conclusion, various recent studies have opted for the design, development, and implementation of quantum-based software and hardware for different applications. Among these applications, space-based computing and network is an important area. Increasing the capabilities of quantum associated software and hardware can improve the technical capability in space as well, which has already shown its importance to various areas.

X. CONCLUSION AND FUTURE DIRECTIONS

This work has reviewed the recent studies over quantum drones, satellites, attacks, architectures, algorithms, and quantum and PQC aspects. Further, this work addresses the recent research directions, challenges, limitations, and futuristic aspects in these areas. As quantum computing and associated aspects are expected to hold tremendous potential in nearby times, this work will be useful to explore the various directions in the quantum area. Thus, this work describes various research directions, challenges, and futuristic aspects of quantum drones, architectures, algorithms, satellites, IoDs, a constellation of satellites, long-distance communication, attacks over quantum networks and communication, and PQC aspects. It has been observed that the area of quantum computing is not new, but there exist various concepts like a quantum drone, satellites, networks, and communication that are still in an infant stage.

A. FUTURE DIRECTIONS

This work can be extended in various directions. Details are presented as follows.

- *In-depth hybrid algorithm analysis:* The present survey starts with taxonomy and covers the major issues in different domains. However, a specific topic like a hybrid algorithm (i.e., algorithms that partially run over quantum computers and partially over hybrid computers) can be taken up for in-depth study. Here, an analysis of the hybrid algorithm, its importance, and comparative analysis would be interesting to explore in the future.
- *Simulating network behaviors:* quantum drones, quantum satellites, a constellation of quantum satellites, internet of quantum drones, and related areas are recently designed and developed. There are a large set of applications associated with this area. This includes environment cleaning, carbon dioxide and hydrogen control, clean technology, modeling energy systems (such as heat, water, and wind), the internet of planetary things, and many more. Most of these concepts may take time to develop. Thus, simulation software could be designed, developed, or explored that helps in advancing quantum-related applications or domains.
- *Quantum cybersecurity, attacks, and warfare:* As discussed earlier, quantum networks may have multiple systems like radars, underwater drones, satellites, magnetometers, chemical detectors, transmitters, and receivers. A study of these systems and their properties would be useful to explore for identifying and handling associated challenges. In these systems and their networks, the chances of cyberattacks cannot be neglected. Thus, areas like quantum cybersecurity, attacks, and warfare can be explored to have prior knowledge and designing the countermeasures.
- *Quantum material and electronic developments:* quantum matters like oxide-based quantum matter, electronic and magnetic structures, and transistors play an important role in major information and communication technologies. Thus, work can be extended to explore the feasibility of similar materials and their importance in designing new quantum directions.
- *Detailed study over numerical or statistical methods:* This work can be extended to explore numerical and statistical methods used to predict quantum machine properties. For example, numerical methods for determining arbitrary quantum spin model behavior would be interesting to explore.
- *Quantum Computing for Trajectory Planning and UAVs:* In [249]–[251], quantum computing is associated with UAVs, their trajectory planning, and their applications in real life. In [249] quantum-inspired reinforcement learning algorithm is proposed. In this algorithm, selection policy and reinforcement strategies are proposed to improve the results. Here, quantum computation theory is used. Likewise, this work can be extended to apply different quantum finite automata for analyzing the steps and optimizing the results.
- *Blind Quantum Computation:* Quantum infrastructure can keep the privacy of resources in addition to fast processing. In blind quantum computation, input, computation function, and output are hidden from the computer. In recent studies, various efforts are made to propose frameworks and algorithms for blind quantum computations. However, its real advantages to applications are yet to be explored in detail, which help solve considerable challenges to quantum clouds. Thus there is a need to examine quantum clouds, blind quantum computations for clouds, and their usages to real-time applications.

REFERENCES

[1] S. P. Jordan and Y.-K. Liu, "Quantum cryptanalysis: Shor, grover, and beyond," *IEEE Secur. Privacy*, vol. 16, no. 5, pp. 14–21, Sep. 2018, doi: 10.1109/MSP.2018.3761719.

[2] P.-L. Cayrel and M. Meziani, "Post-quantum cryptography: Code-based signatures," in *Advances in Computer Science and Information Technology* (Lecture Notes in Computer Science), vol. 6059. Berlin, Germany: Springer, 2010, pp. 82–99, 2010, doi: 10.1007/978-3-642-13577-4_8.

[3] F. Canisius, S. Wang, H. Croft, S. G. Leblanc, H. A. J. Russell, J. Chen, and R. Wang, "A UAV-based sensor system for measuring land surface albedo: Tested over a boreal peatland ecosystem," *Drones*, vol. 3, no. 1, p. 27, Mar. 2019, doi: 10.3390/DRONES3010027.

[4] D. Hambling. (Oct. 2016). *Quantum Film Sensor Stops Delivery Drones Crashing Into Things*. Accessed: May 3, 2021. [Online]. Available: https://www.newscientist.com/article/2108958-quantum-film-sensor-stops-delivery-drones-crashing-into-things/#ixzz6tjiOcuJW

[5] A. D. Hill, J. Chapman, K. Herndon, C. Chopp, D. J. Gauthier, and P. Kwiat, "Drone-based quantum key distribution," *Urbana*, vol. 51, pp. 61801–63003, Sep. 2017.

[6] F. Khoshnoud, M. B. Quadrelli, I. I. Esat, and D. Robinson, "Quantum cooperative robotics and autonomy," 2020, *arXiv:2008.12230*. [Online]. Available: http://arxiv.org/abs/2008.12230

[7] E. Cartlidge. *Quantum Sensors: A Revolution in the Offing|Optics & Photonics News*. Accessed: Jul. 14, 2021. [Online]. Available: https://www.osa-opn.org/home/articles/volume_30/september_2019/features/quantum_sensors_a_revolution_in_the_offing/

[8] H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, J. Guo, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Y.-X. Gong, Z. Xie, and S.-N. Zhu, "Drone-based entanglement distribution towards mobile quantum networks," *Nat. Sci. Rev.*, vol. 7, no. 5, pp. 921–928, May 2020, doi: 10.1093/nsr/nwz227.

[9] M. Irving. (Jan. 2021). *Quantum Communication Network Goes Long With Help of Drones*. Accessed: May 5, 2021. [Online]. Available: https://newatlas.com/telecommunications/quantum-communication-network-drones/

[10] J. F. Bobier, P. Gerbert, J. Burchardt, and A. Gourevitch. (Jan. 2020). *A Quantum Advantage in Fighting Climate Change*. Accessed: May 5, 2021. [Online]. Available: https://www.bcg.com/en-in/publications/2020/quantum-advantage-fighting-climate-change

[11] B. Song, K. Li, D. Orellana-Martín, and M. J. Pérez-Jiménez, "A survey of nature-inspired computing: Membrane computing," *ACM Comput. Surv.*, vol. 54, no. 1, p. 31, Feb. 2021, doi: 10.1145/3431234.

[12] F. Yan, A. M. Iliyasu, and S. E. Venegas-Andraca, "A survey of quantum image representations," *Quantum Inf. Process.*, vol. 15, no. 1, pp. 1–35, Dec. 2015, doi: 10.1007/S11128-015-1195-6.

[13] Discover QGIS. (Jul. 30, 2016). *QGIS Development Team*. Accessed: May 6, 2021. [Online]. Available: http://www.qgis.org/en/site/about/features.html

[14] J. D. Renwick, L. J. Klein, and H. F. Hamann, "Drone-based reconstruction for 3D geospatial data processing," in *Proc. IEEE 3rd World Forum Internet Things*, Feb. 2016, pp. 729–734, doi: 10.1109/WF-IOT.2016.7845501.

[15] M. Schirber, "Quantum drones take flight," *Physics*, vol. 14, p. 7, Jan. 2021, doi: 10.1103/PHYSICS.14.7.

[16] P. Ravi, J. Howe, A. Chattopadhyay, and S. Bhasin, "Lattice-based key-sharing schemes," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–39, Apr. 2021, doi: 10.1145/3422178.

[17] T. A. Shaikh and R. Ali, "Quantum computing in big data analytics: A survey," in *Proc. IEEE Int. Conf. Comput. Inf. Technol. (CIT)*, Dec. 2016, pp. 112–115, doi: 10.1109/CIT.2016.79.

[18] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," *Comput. Sci. Rev.*, vol. 31, pp. 51–71, Feb. 2019, doi: 10.1016/J.COSREV.2018.11.002.

[19] M. M. Savchuk and A. V. Fesenko, "Quantum computing: Survey and analysis," *Cybern. Syst. Anal.*, vol. 55, no. 1, pp. 10–21, Jan. 2019.

[20] C. C. McGeoch, R. Harris, S. P. Reinhardt, and P. I. Bunyk, "Practical annealing-based quantum computing," *Computer*, vol. 52, no. 6, pp. 38–46, Jun. 2019, doi: 10.1109/MC.2019.2908836.

[21] Y. Li, M. Tian, G. Liu, C. Peng, and L. Jiao, "Quantum optimization and quantum learning: A survey," *IEEE Access*, vol. 8, pp. 23568–23593, 2020, doi: 10.1109/ACCESS.2020.2970105.

[22] S. B. Ramezani, A. Sommers, H. K. Manchukonda, S. Rahimi, and A. Amirlatifi, "Machine learning algorithms in quantum computing: A survey," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2020, pp. 1–8, doi: 10.1109/IJCNN48605.2020.9207714.

[23] D. J. Egger, C. Gambella, J. Marecek, S. McFaddin, M. Mevissen, R. Raymond, A. Simonetto, S. Woerner, and E. Yndurain, "Quantum computing for finance: State of the art and future prospects," *IEEE Trans. Quantum Eng.*, vol. 1, 2020, Art. no. 3101724, doi: 10.1109/TQE.2020.3030314.

[24] T. M. Fernandez-Carames, "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6457–6480, Jul. 2020, doi: 10.1109/JIOT.2019.2958788.

[25] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020, doi: 10.1109/ACCESS.2020.2968985.

[26] A. A. Saki, M. Alam, K. Phalak, A. Suresh, R. O. Topaloglu, and S. Ghosh, "A survey and tutorial on security and resilience of quantum computing," 2021, *arXiv:2106.06081*. [Online]. Available: http://arxiv.org/abs/2106.06081

[27] A. P. Jianwei, "Space science activities in China quantum science satellite," *Chin. J. Space Sci.*, vol. 34, no. 5, pp. 547–549, 2014.

[28] M. Mastriani, S. S. Iyengar, and L. Kumar, "Satellite quantum communication protocol regardless of the weather," *Opt. Quantum Electron.*, vol. 53, no. 4, pp. 1–14, Mar. 2021, doi: 10.1007/S11082-021-02829-8.

[29] M. Krelina, "Quantum warfare: Definitions, overview and challenges," 2021, *arXiv:2103.12548*. [Online]. Available: http://arxiv.org/abs/2103.12548

[30] S. A. Wolf, "Overview of the status of quantum science and technology and recommendations for the DoD," Inst. Defense Analyses, New York, NY, USA, Tech. Rep. HQ0034-14-D-0001, 2019.

[31] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," *Rev. Mod. Phys.*, vol. 89, no. 3, p. 35002, 2017.

[32] Y. Shih, "Quantum imaging," in *IEEE J. Sel. Topics Quantum Electron.*, vol. 13, no. 4, pp. 1016–1030, Jul./Aug. 2007, doi: 10.1109/JSTQE.2007.902724.

[33] S. El Gaily and S. Imre, "Constrained quantum optimization algorithm," in *Proc. 20th Int. Symp. Infoteh-Jahorina*, Mar. 2021, pp. 1–6, doi: 10.1109/INFOTEH51037.2021.9400679.

[34] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, pp. 195–202, Sep. 2017.

[35] Y.-B. Sheng and L. Zhou, "Distributed secure quantum machine learning," *Sci. Bull.*, vol. 62, no. 14, pp. 1025–1029, 2017.

[36] C. Q. Choi. (Jun. 2019). *World's First Quantum Drone for Impenetrable Air-to-Ground Data Links Takes Off*. Accessed: Jun. 25, 2021. [Online]. Available: https://spectrum.ieee.org/tech-talk/computing/networks/quantum-drone

[37] D. Huang, Y. Zhao, T. Yang, S. Rahman, X. Yu, X. He, and J. Zhang, "Quantum key distribution over double-layer quantum satellite networks," *IEEE Access*, vol. 8, pp. 16087–16098, 2020, doi: 10.1109/ACCESS.2020.2966683.

[38] M. Raska, "China's quantum satellite experiments: Strategic and military implications," Nanyang Technol. Univ., Singapore, Tech. Rep.223, 2016.

[39] A. Mashatan and D. Heintzman, "The complex path to quantum resistance," *Queue*, vol. 19, no. 2, pp. 65–92, Apr. 2021, doi: 10.1145/3466132.3466779.

[40] J. Wang, X. Wang, R. Gao, C. Lei, W. Feng, N. Ge, S. Jin, and T. Q. S. Quek, "Physical layer security for UAV communications in 5G and beyond networks," 2021, *arXiv:2105.11332*. [Online]. Available: http://arxiv.org/abs/2105.11332

[41] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: A survey," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33–52, Jan. 2020, doi: 10.1109/JIOT.2019.2943900.

[42] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019, doi: 10.1109/JIOT.2019.2927379.

[43] N. Pathak, A. Mukherjee, and S. Misra, "AerialBlocks: Blockchain-enabled UAV virtualization for industrial IoT," *IEEE Internet Things Mag.*, vol. 4, no. 1, pp. 72–77, Mar. 2021, doi: 10.1109/iotm.0011.1900093.

[44] P. K. Sharma and D. I. Kim, "Secure 3D mobile UAV relaying for hybrid satellite-terrestrial networks," *IEEE Trans. Wireless Commun.*, vol. 19, no. 4, pp. 2770–2784, Apr. 2020, doi: 10.1109/TWC.2020.2968296.
[45] S. Yan, X. Wang, Z. Li, B. Li, and Z. Fei, "Cooperative jamming for physical layer security in hybrid satellite terrestrial relay networks," *China Commun.*, vol. 16, no. 12, pp. 154–164, Dec. 2019, doi: 10.23919/JCC.2019.12.012.
[46] C. Abellan and V. Pruneri, "The future of cybersecurity is quantum," *IEEE Spectr.*, vol. 55, no. 7, pp. 30–35, Jul. 2018, doi: 10.1109/MSPEC.2018.8389185.
[47] F. Daum, "Quantum radar cost and practical issues," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 35, no. 11, pp. 8–20, Nov. 2020, doi: 10.1109/MAES.2020.2982755.
[48] C. Fang, "The simulation and analysis of quantum radar cross section for three-dimensional convex targets," *IEEE Photon. J.*, vol. 10, no. 1, Feb. 2018, Art. no. 7500308, doi: 10.1109/JPHOT.2017.2780981.
[49] A. Salmanogli and D. Gokcen, "Entanglement sustainability improvement using optoelectronic converter in quantum radar (interferometric object-sensing)," *IEEE Sensors J.*, vol. 21, no. 7, pp. 9054–9062, Apr. 2021, doi: 10.1109/JSEN.2021.3052256.
[50] Q. Zhang, F. Xu, L. Li, N.-L. Liu, and J.-W. Pan, "Quantum information research in China," *Quantum Sci. Technol.*, vol. 4, no. 4, Nov. 2019, Art. no. 040503, doi: 10.1088/2058-9565/AB4BEA.
[51] A. V. Navaneeth and M. R. Dileep, "A study and analysis of applications of classical computing and quantum computing: A survey," in *ICT Analysis and Applications* (Lecture Notes in Networks and Systems), vol. 154. Singapore: Springer, 2021, pp. 235–246, doi: 10.1007/978-981-15-8354-4_25.
[52] (Apr. 2018). *Quantum Algorithm Implementations for Beginners*. Accessed: Jul. 14, 2021. [Online]. Available: https://arxiv.org/abs/1804.03719v2
[53] M. F. Riedel, D. Binosi, R. Thew, and T. Calarco, "The European quantum technologies flagship programme," *Quantum Sci. Technol.*, vol. 2, no. 3, Jun. 2017, Art. no. 030501, doi: 10.1088/2058-9565/AA6ACA.
[54] *Quantum Algorithm Zoo*. Accessed: Sep. 9, 2021. [Online]. Available: http://quantum.algorithmzoo.org/
[55] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020, doi: 10.1364/AOP.361502.
[56] B. P. Williams, J. M. Lukens, N. A. Peters, B. Qi, and W. P. Grice, "Quantum secret sharing with polarization-entangled photon pairs," *Phys. Rev. A, Gen. Phys.*, vol. 99, no. 6, Jun. 2019, Art. no. 062311.
[57] J. M. Arrazola and N. Lütkenhaus, "Quantum communication with coherent states and linear optics," *Phys. Rev. A, Gen. Phys.*, vol. 90, no. 4, Oct. 2014, Art. no. 042335.
[58] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," *Proc. 50th Annu. Symp. Found. Comput. Sci.*, Oct. 2009, pp. 517–526.
[59] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, pp. 45–53, Mar. 2010.
[60] D. P. DiVincenzo, "The physical implementation of quantum computation," *Fortschritte Phys.*, vol. 48, nos. 9–11, pp. 771–783, Feb. 2000, doi: 10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E.
[61] A. M. Steane, "Quantum computer architecture for fast entropy extraction," *Quantum Inf. Comput.*, vol. 2, p. 297, Apr. 2002. [Online]. Available: http://dl.acm.org/citation.cfm?id=2011480
[62] A. M. Steane, "How to build a 300 bit, 1 giga-operation quantum computer," *Quantum Inf. Comput.*, vol. 7, no. 3, pp. 171–183, Mar. 2007. [Online]. Available: http://dl.acm.org/citation.cfm?id=2011718
[63] T. P. Spiller, W. J. Munro, S. D. Barrett, and P. Kok, "An introduction to quantum information processing: Applications and realizations," *Contemp. Phys.*, vol. 46, no. 6, pp. 407–436, Nov. 2005, doi: 10.1080/00107510500293261.
[64] R. V. Meter and M. Oskin, "Architectural implications of quantum computing technologies," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 2, no. 1, pp. 31–63, Jan. 2006, doi: 10.1145/1126257.1126259.
[65] N. C. Jones, R. V. Meter, G. A. Fowler, L. P. McMahon, J. Kim, D. T. Ladd, and Y. Yamamoto, "Layered architecture for quantum computing," *Phys. Rev. X*, vol. 2, no. 3, 2012, Art. no. 031007, doi: 10.1103/PhysRevX.2.031007.
[66] H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, Y. Niu, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Z. Xie, Y.-X. Gong, and S.-N. Zhu, "Drone-based all-weather entanglement distribution," *Nat. Sci. Rev.*, vol. 7, no. 5, pp. 921–928, 2020. [Online]. Available: https://arxiv.org/abs/1905.09527v1
[67] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum internet: Networking challenges in distributed quantum computing," *IEEE Netw.*, vol. 34, no. 1, pp. 137–143, Jan. 2020.
[68] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.
[69] *Quantum Safe Cryptography and Security An introduction, Benefits, Enablers and Challenges*, European Telecommunications Standards Institute, Sophia Antipolis, France, Jun. 2015. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf
[70] European Telecommunications Standards Institute. (Mar. 2017). *Quantum-Safe Cryptography; Quantum-Safe Threat Assessment*. [Online]. Available: https://www.etsi.org/deliver/etsi_gr/QSC/001_099/004/01.01.01_60/gr_QSC004v010101p.pdf
[71] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.
[72] *Internet Security Threat Report*, Symantec, Tempe, AZ, USA, 2016.
[73] A. P. Bhatt and A. Sharma, "Quantum cryptography for Internet of Things security," *J. Electron. Sci. Technol.*, vol. 17, no. 3, pp. 213–220, 2019.
[74] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 4, pp. 912–925, Apr. 2018.
[75] A. Shi, H. Guan, and W. Zhang, "Efficient diabatic quantum algorithm in number factorization," *Phys. Lett. A*, vol. 384, no. 28, Oct. 2020, Art. no. 126745, doi: 10.1016/j.physleta.2020.126745.
[76] M. Abd Elaziz, D. Mohammadi, D. Oliva, and K. Salimifard, "Quantum marine predators algorithm for addressing multilevel image segmentation," *Appl. Soft Comput.*, vol. 4, Jun. 2021, Art. no. 107598, doi: 10.1016/j.asoc.2021.107598.
[77] A. Hosoyamada, Y. Sasaki, S. Tani, and K. Xagawa, "Quantum algorithm for the multicollision problem," *Theor. Comput. Sci.*, vol. 842, pp. 100–117, Nov. 2020.
[78] M. Mojrian and S. A. Mirroshandel, "A novel extractive multi-document text summarization system using quantum-inspired genetic algorithm: MTSQIGA," *Expert Syst. Appl.*, vol. 171, Jun. 2021, Art. no. 114555.
[79] Y. Wang and C. Wei, "Design optimization of office building envelope based on quantum genetic algorithm for energy conservation," *J. Building Eng.*, vol. 35, Mar. 2021, Art. no. 102048, doi: 10.1016/j.jobe.2020.102048.
[80] A. Kaveh, M. Kamalinejad, K. Biabani Hamedani, and H. Arzani, "Quantum teaching-learning-based optimization algorithm for sizing optimization of skeletal structures with discrete variables," *Structures*, vol. 32, pp. 1798–1819, Aug. 2021, doi: 10.1016/j.istruc.2021.03.046.
[81] C. Ding, T.-Y. Bao, and H.-L. Huang, "Quantum-inspired support vector machine," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Jun. 10, 2021, doi: 10.1109/TNNLS.2021.3084467.
[82] L. Braine, D. J. Egger, J. Glick, and S. Woerner, "Quantum algorithms for mixed binary optimization applied to transaction settlement," *IEEE Trans. Quantum Eng.*, vol. 2, 2021, Art. no. 3101208, doi: 10.1109/TQE.2021.3063635.
[83] Y. Kang and J. Heo, "Quantum minimum searching algorithm and circuit implementation," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2020, pp. 214–219, doi: 10.1109/ICTC49870.2020.9289455.
[84] T. Satoh, Y. Ohkura, and R. Van Meter, "Subdivided phase oracle for NISQ search algorithms," *IEEE Trans. Quantum Eng.*, vol. 1, 2020, Art. no. 3100815, doi: 10.1109/TQE.2020.3012068.
[85] S. Mondal, M. R. Laskar, and A. K. Dutta, "ML criterion based signal detection of a MIMO-OFDM system using quantum and semi-quantum assisted modified DHA/BBHT search algorithm," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1688–1698, Feb. 2021, doi: 10.1109/TVT.2021.3055537.
[86] V. Bhatia and K. R. Ramkumar, "An efficient quantum computing technique for cracking RSA using Shor's algorithm," in *Proc. IEEE 5th Int. Conf. Comput. Commun. Autom. (ICCCA)*, Oct. 2020, pp. 89–94, doi: 10.1109/ICCCA49541.2020.9250806.
[87] D. Chivilikhin, A. Samarin, V. Ulyantsev, I. Iorsh, A. R. Oganov, and O. Kyriienko, "MoG-VQE: Multiobjective genetic variational quantum eigensolver," 2020, *arXiv:2007.04424*. [Online]. Available: http://arxiv.org/abs/2007.04424

[88] J. Guan, Q. Wang, and M. Ying, "An HHL-based algorithm for computing hitting probabilities of quantum random walks," *Quantum Phys.*, vol. 121, no. 5, pp. 395–408, Sep. 2020, doi: 10.26421/QIC21.5-6-4.

[89] W. Easttom, "Quantum Computing and Cryptography," in *Modern Cryptography*. Cham, Switzerland: Springer, 2021, pp. 385–390, doi: 10.1007/978-3-030-63115-4_19.

[90] S. K. Liao, W. Cai, W. Liu, L. Zhang, Y. Li, J. Ren, J. Yin, Q. Shen, and Y. Cao, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, Sep. 2017.

[91] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, p. 10504, Jan. 2007.

[92] S. Liao, J. Lin, J. Ren, W. Liu, J. Qiang, J. Yin, Y. Li, Q. Shen, L. Zhang, X. Liang, and H. Yong, "Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab," *Chin. Phys. Lett.*, vol. 34, no. 9, p. 90302, 2017.

[93] S. A. Hamiltona, "Overview of NASA's national space quantum laboratory program," in *Proc. IAC*, Oct. 2019, pp. 1–12.

[94] *China Launches World's First Quantum Communications Satellite Into Space*. Accessed: Jul. 14, 2021. [Online]. Available: https://www.spaceflightinsider.com/space-flight-news/china-launches-world-first-quantum-communications-satellite/

[95] G. W. Hein, "Status, perspectives and trends of satellite navigation," *Satell. Navigat.*, vol. 1, no. 1, pp. 1–12, Dec. 2020.

[96] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, and Z. Wang, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, 2011.

[97] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, "An entanglement-based wavelength-multiplexed quantum communication network," *Nature*, vol. 564, no. 7735, pp. 225–228, Dec. 2018.

[98] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, X.-D. Cai, P. Xu, G.-S. Pan, J.-J. Jia, Y.-M. Huang, H. Yin, J.-Y. Wang, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," *Nature*, vol. 488, no. 7410, pp. 185–188, Aug. 2012.

[99] N. C. Coops, T. R. H. Goodbody, and L. Cao, "Four steps to extend drone use in research," *Nature*, vol. 572, no. 7770, pp. 433–435, Aug. 2019.

[100] M. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones: A review," *Progr. Aerosp. Sci.*, vol. 91, pp. 99–131, May 2017.

[101] *Airbus Zephyr*. Accessed: Jun. 9, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Airbus_Zephyr

[102] (Jun. 9, 2021). *Drones Could Help Create a Quantum Internet*. [Online]. Available: https://www.sciencenews.org/article/physics-drones-could-help-create-quantum-internet

[103] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.

[104] *Esa Moon Village Project Webpage*. Accessed: Nov. 22, 2019. [Online]. Available: https://www.esa.int/AboutUs/MinisterialCouncil2016/MoonVillage

[105] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, "Satellite communications in the new space era: A survey and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 70–109, 1st Quart., 2021.

[106] (Nov. 2017). *Quantum Technologies in Space Intermediate Strategic Report for ESA and National Space Agencies*. Accessed: Jul. 14, 2021. [Online]. Available: https://www.cosmos.esa.int/documents/1866264/3219248/BassiA_QT_In_Space_-_White_Paper.pdf/6f50e4bc-9fac-8f72-0ec0-f8e030adc499?t=1565184619333

[107] O. Kodheli, A. Guidotti, and A. Vanelli-Coralli, "Integration of satellites in 5G through LEO constellations," in *Proc. IEEE Global Commun. Conf.*, Dec. 2017, pp. 1–6.

[108] C. A. Hofmann and A. Knopp, "Direct access to satellites: An internet of remote things technology," in *Proc. IEEE 2nd 5G World Forum (5GWF)*, Sep. 2019, pp. 578–583.

[109] E. Lagunas, S. K. Sharma, S. Maleki, S. Chatzinotas, and B. Ottersten, "Resource allocation for cognitive satellite communications with incumbent terrestrial networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 1, no. 3, pp. 305–317, Sep. 2015.

[110] L. Bacsardi, "Using quantum computing algorithms in future satellite communication," *Acta Astronautica*, vol. 57, nos. 2–8, pp. 224–229, Jul. 2005.

[111] L. Bacsardi and S. Imre, "Analyzing the quantum based satellite communications," *Procedia Comput. Sci.*, vol. 7, pp. 256–257, Jan. 2011.

[112] S. Khatri, A. J. Brady, R. A. Desporte, M. P. Bart, and J. P. Dowling, "Spooky action at a global distance: Analysis of space-based entanglement distribution for the quantum internet," *NPJ Quantum Inf.*, vol. 7, no. 1, Dec. 2021, Art. no. 4, doi: 10.1038/s41534-020-00327-5.

[113] *Quantum Science Satellite*. Accessed: Jul. 14, 2021. [Online]. Available: https://spaceflight101.com/spacecraft/quantum-science-satellite/

[114] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, and A. Zeilinger, "Experimental verification of the feasibility of a quantum channel between space and Earth," *New J. Phys.*, vol. 10, no. 3, p. 33038, 2008.

[115] N. Gigov, "Quantum key distribution data post-processing with limited resources: Towards satellite-based quantum communication," Univ. Waterloo, Waterloo, ON, Canada, Tech. Rep. 10012/7244, 2013.

[116] E. F. Dumitrescu, A. J. McCaskey, G. Hagen, G. R. Jansen, T. D. Morris, T. Papenbrock, R. C. Pooser, D. J. Dean, and P. Lougovski, "Cloud quantum computing of an atomic nucleus," *Phys. Rev. Lett.*, vol. 120, no. 21, May 2018, Art. no. 210501.

[117] G. Färnkranz, "The quantum digital future," in *The Quantum Internet*. Cham, Switzerland: Springer, 2020, pp. 1–81.

[118] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini, "Quantum internet-applications, functionalities, enabling technologies, challenges, and research directions," 2021, *arXiv:2101.04427*. [Online]. Available: https://arxiv.org/abs/2101.04427

[119] K. Sharma and X. Wang, "Toward massive machine type communications in ultra-dense cellular IoT networks: Current issues and machine learning-assisted solutions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 426–471, 1st Quart., 2019.

[120] W. Y. B. Lim, J. Huang, Z. Xiong, J. Kang, D. Niyato, X.-S. Hua, C. Leung, and C. Miao, "Towards federated learning in UAV-enabled Internet of Vehicles: A multi-dimensional contract-matching approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5140–5154, Aug. 2021, doi: 10.1109/TITS.2021.3056341.

[121] Y. Sun, S. Yi, and F. Hou, "Unmanned aerial vehicle methods makes species composition monitoring easier in grasslands," *Ecol. Ind.*, vol. 95, pp. 825–830, Dec. 2018, doi: 10.1016/j.ecolind.2018.08.042.

[122] X. Sun and N. Ansari, "Jointly optimizing drone-mounted base station placement and user association in heterogeneous networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6, doi: 10.1109/ICC.2018.8422377.

[123] G. Acampora, "Quantum machine intelligence," *Quantum Mach. Intell.*, vol. 1, pp. 1–3, May 2019, doi: 10.1007/s42484-019-00006-5.

[124] R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys.*, vol. 21, nos. 6–7, pp. 467–488, 1982, doi: 10.1007/BF02650179.

[125] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, and R. Biswas, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.

[126] H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48572–48634, 2019, doi: 10.1109/ACCESS.2019.2909530.

[127] A. Conrad, S. Isaac, R. Cochran, D. Sanchez-Rosales, B. Wilens, A. Gutha, T. Rezaei, D. J. Gauthier, and P. Kwiat, "Drone-based quantum key distribution," *Proc. SPIE*, vol. 11678, May 2021, Art. no. 116780X, doi: 10.1117/12.2582376.

[128] A. Perdomo-Ortiz, M. Benedetti, J. Realpe-Gomez, and R. Biswas, "Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers," *Quantum Sci. Technol.*, vol. 3, no. 3, 2018, Art. no. 030502, doi: 10.1088/2058-9565/aab859.

[129] M. Schuld, I. Sinayskiy, and F. Petruccione, "An introduction to quantum machine learning," *Contemp. Phys.*, vol. 56, no. 2, pp. 172–185, 2015, doi: 10.1080/00107514.2014.964942.

[130] M. Pande and P. Mulay, "Bibliometric survey of quantum machine learning," *Sci. Technol. Libraries*, vol. 39, no. 4, pp. 369–382, 2020, doi: 10.1080/0194262X.2020.1776193.

[131] V. Dunjko, J. M. Taylor, and H. J. Briegel, "Quantum-enhanced machine learning," *Phys. Rev. Lett.* 117, Sep. 2016, Art. no. 130501, doi: 10.1103/PhysRevLett.117.130501.

[132] D. Ristè, M. P. da Silva, C. A. Ryan, A. W. Cross, A. D. Córcoles, J. A. Smolin, J. M. Gambetta, J. M. Chow, and B. R. Johnson, "Demonstration of quantum advantage in machine learning," *NPJ Quantum Inf.*, vol. 3, no. 1, pp. 1–5, Dec. 2017.
[133] M. Benedetti, J. Realpe-Gomez, and A. Perdomo-Ortiz, "Quantum-assisted Helmholtz machines: A quantum-classical deep learning framework for industrial datasets in near-term devices," *Quantum Sci. Technol.*, vol. 3, no. 3, 2018, Art. no. 034007, doi: 10.1088/2058-9565/aabd98.
[134] U. Alvarez-Rodriguez, L. Lamata, P. Escandell-Montero, J. D. Martín-Guerrero, and E. Solano, "Supervised quantum learning without measurements," *Sci. Rep.*, vol. 7, no. 1, Dec. 2017, Art. no. 13645, doi: 10.1038/s41598-017-13378-0.
[135] A. Kerenidis and A. Prakash, "Quantum recommendation systems," in *Proc. 8th Innov. Theor. Comput. Sci. Conf. (ITCS)*, 2017, pp. 1–21.
[136] L. Lamata, "Basic protocols in quantum reinforcement learning with superconducting circuits," *Sci. Rep.*, vol. 7, no. 1, Dec. 2017, Art. no. 1609.
[137] S. Y.-C. Chen and S. Yoo, "Federated quantum machine learning," *Entropy*, vol. 23, no. 4, p. 460, Apr. 2021, doi: 10.3390/e23040460.
[138] A. Giusti, J. Guzzi, D. C. Ciresan, F.-L. He, J. P. Rodriguez, F. Fontana, M. Faessler, C. Forster, J. Schmidhuber, G. D. Caro, D. Scaramuzza, and L. M. Gambardella, "A machine learning approach to visual perception of forest trails for mobile robots," *IEEE Robot. Autom. Lett.*, vol. 1, no. 2, pp. 661–667, Jul. 2016, doi: 10.1109/LRA.2015.2509024.
[139] M. Bejiga, A. Zeggada, A. Nouffidj, and F. Melgani, "A convolutional neural network approach for assisting avalanche search and rescue operations with UAV imagery," *Remote Sens.*, vol. 9, no. 2, p. 100, Jan. 2017, doi: 10.3390/rs9020100.
[140] M. Barbeau, "Recognizing drone swarm activities: Classical versus quantum machine learning," *Digitale Welt*, vol. 3, no. 4, pp. 45–50, Oct. 2019, doi: 10.1007/s42354-019-0212-9.
[141] S.-J. Hong, Y. Han, S.-Y. Kim, A.-Y. Lee, and G. Kim, "Application of deep-learning methods to bird detection using unmanned aerial vehicle imagery," *Sensors*, vol. 19, no. 7, p. 1651, Apr. 2019, doi: 10.3390/s19071651.
[142] A. Carrio, C. Sampedro, A. Rodriguez-Ramos, and P. Campoy, "A review of deep learning methods and applications for unmanned aerial vehicles," *J. Sensors*, vol. 2017, Aug. 2017, Art. no. 3296874, doi: 10.1155/2017/3296874.
[143] L. Shan, R. Miura, T. Kagawa, F. Ono, H.-B. Li, and F. Kojima, "Machine learning-based field data analysis and modeling for drone communications," *IEEE Access*, vol. 7, pp. 79127–79135, 2019, doi: 10.1109/ACCESS.2019.2922544.
[144] P. V. Klaine, J. P. B. Nadas, R. D. Souza, and M. A. Imran, "Distributed drone base station positioning for emergency cellular networks using reinforcement learning," *Cogn. Comput.*, vol. 10, pp. 790–804, May 2018, doi: 10.1007/s12559-018-9559-8.
[145] W. Wang and H.-K. Lo, "Machine learning for optimal parameter prediction in quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 100, no. 6, Dec. 2019, Art. no. 062334, doi: 10.1103/PhysRevA.100.062334.
[146] M. Chen, M. Mozaffari, W. Saad, C. Yin, M. Debbah, and C. S. Hong, "Caching in the sky: Proactive deployment of cache-enabled unmanned aerial vehicles for optimized quality-of-experience," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 5, pp. 1046–1061, May 2017, doi: 10.1109/JSAC.2017.2680898.
[147] V. Dunjko and H. J. Briegel, "Machine learning & artificial intelligence in the quantum domain: A review of recent progress," *Rep. Prog. Phys.*, vol. 81, no. 7, p. 74001, 2018, doi: 10.1088/1361-6633/aab406.
[148] V. Moret-Bonillo, "Can artificial intelligence benefit from quantum computing?" *Prog. Artif. Intell.*, vol. 3, no. 2, pp. 89–105, Mar. 2015, doi: 10.1007/s13748-014-0059-0.
[149] J. Sun, J. Tang, and S. Lao, "Collision avoidance for cooperative UAVs with optimized artificial potential field algorithm," *IEEE Access*, vol. 5, pp. 18382–18390, 2017, doi: 10.1109/ACCESS.2017.2746752.
[150] A. Islam, T. Rahim, M. Masuduzzaman, and S. Y. Shin, "A blockchain-based artificial intelligence-empowered contagious pandemic situation supervision scheme using Internet of Drone Things," *IEEE Wireless Commun.*, early access, Apr. 20, 2021, doi: 10.1109/MWC.001.2000429.
[151] H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, J. Guo, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Y.-X. Gong, Z. Xie, and S.-N. Zhu, "Optical-relayed entanglement distribution using drones as mobile nodes," *Phys. Rev. Lett.*, vol. 126, no. 2, Jan. 2021, Art. no. 20503.
[152] R. Gupta, A. Kumari, and S. Tanwar, "Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, Jan. 2021, Art. no. e4176, doi: 10.1002/ett.4176.
[153] *How Quantum Computers Will Revolutionise Artificial Intelligence, Machine Learning and Bid Data*. Accessed: Aug. 9, 2021. [Online]. Available: https://bernardmarr.com/how-quantum-computers-will-revolutionise-artificial-intelligence-machine-learning-and-big-data/
[154] C. Dilmegani. *Quantum Artificial Intelligence in 2021: In-Depth Guide*. Accessed: Aug. 9, 2021. [Online]. Available: https://research.aimultiple.com/quantum-ai/
[155] *AI Applications of Quantum Computing*. Accessed: Aug. 9, 2021. [Online]. Available: https://www.uts.edu.au/research-and-teaching/our-research/centre-quantum-software-and-information/qsi-research/qsi-research-programs/ai-applications-quantum-computing
[156] M. Möller and C. Vuik, "On the impact of quantum computing technology on future developments in high-performance scientific computing," *Ethics Inf. Technol.*, vol. 19, no. 4, pp. 253–269, Dec. 2017, doi: 10.1007/s10676-017-9438-0.
[157] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, pp. 195–202, Sep. 2017, doi: 10.1038/nature23474.
[158] Y. Levine, D. Yakira, N. Cohen, and A. Shashua, "Deep learning and quantum entanglement: Fundamental connections with implications to network design," 2017, *arXiv:1704.01552*. [Online]. Available: http://arxiv.org/abs/1704.01552
[159] S. Y. Yan, *Quantum Attacks on Public-Key Cryptosystems*, vol. 9781441977229. USA: Springer, 2013.
[160] S. Y. Yan, "Quantum attacks on IFP-based cryptosystems," in *Quantum Attacks Public-Key Cryptosystems*. Boston, MA, USA: Springer, 2013, pp. 31–91.
[161] L. Chen, L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on post-quantum cryptography," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 8105, 2016, doi: 10.6028/NIST.IR.8105.
[162] K. K. Soni and A. Rasool, "Cryptographic attack possibilities over RSA algorithm through classical and quantum computation," in *Proc. Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Dec. 2018, pp. 11–15, doi: 10.1109/ICSSIT.2018.8748675.
[163] J. Suo, L. Wang, S. Yang, W. Zheng, and J. Zhang, "Quantum algorithms for typical hard problems: A perspective of cryptanalysis," *Quantum Inf. Process.*, vol. 19, no. 6, p. 178, Jun. 2020, doi: 10.1007/s11128-020-02673-x.
[164] M. Bozzio, A. Cavaillès, E. Diamanti, A. Kent, and D. Pitalúa-García, "Multi-photon and side-channel attacks in mistrustful quantum cryptography," 2021, *arXiv:2103.06970*. [Online]. Available: http://arxiv.org/abs/2103.06970
[165] A. M. Childs and G. Ivanyos, "Quantum computation of discrete logarithms in semigroups," *J. Math. Cryptol.*, vol. 8, no. 4, pp. 405–416, Jan. 2014, doi: 10.1515/jmc-2013-0038.
[166] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter. *Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms*. Accessed: Jun. 6, 2021. [Online]. Available: https://eprint.iacr.org/2017/598.pdf
[167] X. Bonnetain, A. Hosoyamada, M. Naya-Plasencia, Y. Sasaki, and A. Schrottenloher, "Quantum attacks without superposition queries: The offline Simon's algorithm," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 11921. Cham, Switzerland: Springer, Dec. 2019, pp. 552–583, doi: 10.1007/978-3-030-34578-5_20.
[168] P. Wang, S. Tian, Z. Sun, and N. Xie, "Quantum algorithms for hash preimage attacks," *Quantum Eng.*, vol. 2, no. 2, p. e36, Jun. 2020, doi: 10.1002/que2.36.
[169] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *Quantum Inf. Comput.*, vol. 3, no. 4, pp. 317–344, Jan. 2003. Accessed: Jul. 05, 2021. [Online]. Available: http://arxiv.org/abs/quant-ph/0301141
[170] *NSA Surveillance, Edward Snowden and the End of Privacy: A Real-Time Account of the Biggest Leaks in US History*. Accessed: Jun. 5, 2021. [Online]. Available: https://ultraculture.org/blog/2017/04/24/nsa-surveillance-edward-snowden/
[171] *Analyzing Quantum Insert Attacks—Infosec Resources*. Accessed: Jun. 6, 2021. [Online]. Available: https://resources.infosecinstitute.com/topic/analyzing-quantum-insert-attacks/
[172] A. Prasad and K. Kaushik, "Digital signatures," in *Emerging Security Algorithms and Techniques*, K. Kaushik, Ed. Boca Raton, FL, USA: Taylor & Francis, 2019, pp. 249–272.

[173] C. Simon, "Towards a global quantum network," *Nature Photon.*, vol. 11, no. 11, pp. 678–680, Oct. 2017, doi: 10.1038/s41566-017-0032-0.
[174] C. Liorni, H. Kampermann, and D. Bruß, "Quantum repeaters in space," *New J. Phys.*, vol. 23, no. 5, May 2021, Art. no. 053021, doi: 10.1088/1367-2630/abfa63.
[175] S. Das, M. Saifur Rahman, and M. Alam Majumdar, "Design of a quantum-repeater using quantum-circuits and benchmarking its performance on an IBM quantum-computer," 2020, *arXiv:2009.04584*. [Online]. Available: http://arxiv.org/abs/2009.04584
[176] *Quantum Safe Cryptography and Security*. Accessed: Jun. 6, 2021. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf
[177] P. Wright, C. White, R. C. Parker, J. Pegon, M. Menchetti, J. Pearse, A. Bahrami, A. Moroz, A. Wonfor, R. V. Penty, and T. P. Spiller, "5G network slicing with QKD and quantum-safe security," *J. Opt. Commun. Netw.*, vol. 13, no. 3, pp. 33–40, Mar. 2021, doi: 10.1364/JOCN.413918.
[178] P. Wallden and E. Kashefi, "Cyber security in the quantum era," *Commun. ACM*, vol. 62, no. 4, pp. 120–129, Apr. 2019, doi: 10.1145/3241037.
[179] H. Crawford and S. Atkin. *Quantum Authentication: Current and Future Research Directions*. Accessed: Jun. 6, 2021. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
[180] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," in *Proc. Amer. Assoc. Phys. Teachers*, 2002, pp. 558–559.
[181] S. N. Sivanandam and S. N. Deepa, "Genetic algorithms," in *Introduction to Genetic Algorithms*. Berlin, Germany: Springer-Verlag, 2008, pp. 15–37.
[182] K. H Han and J. H. Kim, "Quantum inspired evolutionary algorithm for a class of combinatorial optimization," *IEEE Trans. Evol. Comput.*, vol. 6, no. 6, pp. 580–593, Dec. 2002.
[183] K. H. Han, K. H. Park, and C. H. Lee, "Parallel quantum-inspired genetic algorithm for combinatorial optimization problem," in *Proc. Congr. Evol. Comput.*, Seoul, South Korea, 2001, pp. 1422–1429.
[184] K. H. Han and J. H Kim, "Genetic quantum algorithm and its application to combinatorial optimization problem," in *Proc. Congr. Evol. Comput.*, vol. 2, 2000, pp. 1354–1360.
[185] Y. Lv and N. Liu, "Application of quantum genetic algorithm on finding minimal reduct," in *Proc. IEEE Int. Conf. Granular Comput.*, May 2007, pp. 722–728.
[186] S. Mousavi, F. Afghah, J. D. Ashdown, and K. Turck, "Use of a quantum genetic algorithm for coalition formation in large-scale UAV networks," *Ad Hoc Netw.*, vol. 87, pp. 26–36, May 2019.
[187] S. P. Ketchpel, "Coalition formation among autonomous agents," in *Proc. Eur. Workshop Modelling Autonomous Agents Multi-Agent World*. Berlin, Germany: Springer, 1993, pp. 73–88.
[188] A. Razi, F. Afghah, and J. Chakareski, "Optimal measurement policy for predicting UAV network topology," in *Proc. 51st Asilomar Conf. Signals, Syst., Comput.*, 2017, pp. 1374–1378.
[189] A. Rovira-Sugranes and A. Razi, "Predictive routing for dynamic uav networks," in *Proc. Int. Conf. Wireless Space Extreme Environ.*, Oct. 2017, pp. 43–47.
[190] J. Contreras, M. Klush, and J. Yen, "Multi-agent coalition formation in power transmission planning: A bilateral Shapley value approach," in *Proc. AIPS*, 1998, pp. 19–26.
[191] J. Yu, Y. Shi, D. Tang, H. Liu, and L. Tian, "Optimizing sequential diagnostic strategy for large-scale engineering systems using a quantum-inspired genetic algorithm: A comparative study," *Appl. Soft Comput.*, vol. 85, Dec. 2019, Art. no. 105802.
[192] A. Layeb, "A hybrid quantum inspired harmony search algorithm for 0–1 optimization problems," *J. Comput. Appl. Math.*, vol. 253, pp. 14–25, Dec. 2013.
[193] D. D. Karaboga and B. Basturk, "A powerful and efficient algorithm for numerical function optimization: Artificial bee colony (ABC) algorithm," *J. Global Optim.*, vol. 39, no. 3, pp. 459–471, Apr. 2007.
[194] S. Das, A. Mukhopadhyay, A. Roy, A. Abraham, and B. K. Panigrahi, "Exploratory power of the harmony search algorithm: Analysis and improvements for global numerical optimization," *IEEE Trans. Syst., Man, Cybern. B. Cybern.*, vol. 41, no. 1, pp. 89–106, Feb. 2011.
[195] D. Zou, L. Gao, S. Li, J. Wu, and X. Wang, "A novel global harmony search algorithm for task assignment problem," *J. Syst. Softw.*, vol. 83, no. 10, pp. 1678–1688, Oct. 2010.
[196] M. Jaberipour and E. Khorram, "Two improved harmony search algorithms for solving engineering optimization problems," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 11, pp. 3316–3331, Nov. 2010.
[197] Y. Rizk and M. Awad, "A quantum genetic algorithm for pickup and delivery problems with coalition formation," *Procedia Comput. Sci.*, vol. 159, pp. 261–270, 2019.
[198] J. Gu, X. Gu, andM. Gu, "A novel parallel quantum genetic algorithm for stochastic job shop scheduling," *J. Math. Anal. Appl.*, vol. 355, no. 1, pp. 63–81, Jul. 2009.
[199] D. Konar, K. Sharma, V. Sarogi, and S. Bhattacharyya, "A multi-objective quantum-inspired genetic algorithm (Mo-QIGA) for real-time tasks scheduling in multiprocessor environment," *Procedia Comput. Sci.*, vol. 131, pp. 591–599, Jan. 2018.
[200] H. Xing, X. Liu, X. Jin, L. Bai, and Y. Ji, "A multi-granularity evolution based quantum genetic algorithm for QoS multicast routing problem in WDM networks," *Comput. Commun.*, vol. 32, no. 2, pp. 386–393, Feb. 2009.
[201] Z. A. El M. Dahi, C. Mezioud, and A. Draa, "A quantum-inspired genetic algorithm for solving the antenna positioning problem," *Swarm Evol. Comput.*, vol. 31, pp. 24–63, Dec. 2016.
[202] A. Narayanan and M. Moore, "Quantum-inspired genetic algorithm," in *Proc. Int. Conf. Evol. Comput.*, May 1996, pp. 41–46.
[203] M. Bhatia, S. K. Sood, and S. Kaur, "Quantum-based predictive fog scheduler for IoT applications," *Comput. Ind.*, vol. 111, pp. 51–67, Oct. 2019.
[204] R. J. McEliece, "A public-key cryptosystem based on algebraic," *Coding Thv*, vol. 4244, pp. 114–116, Apr. 1978.
[205] Y. X. Li, R. H. Deng, and X. M. Wang, "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 271–273, Jan. 1994.
[206] N. T. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2001, pp. 157–174.
[207] G. Kabatianskii, E. Krouk, and B. Smeets, "A digital signature scheme based on random error-correcting codes," in *Proc. Int. Conf. Cryptogr. Coding*, 1997, pp. 161–167.
[208] P.-L. Cayrel, A. Otmani, and D. Vergnaud, "On kabatianskii-krouk-smeets signatures," in *Proc. Int. Workshop Arithmetic Finite Fields*, 2007, pp. 237–251.
[209] D. Zheng, X. Li, and K. Chen, "Code-based ring signature scheme," *Int. J. Netw. Secur.*, vol. 5, no. 2, pp. 154–157, 2007.
[210] C. A. Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie, "A new efficient threshold ring signature scheme based on coding theory," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4833–4842, Jul. 2011, doi: 10.1109/TIT.2011.2145950.
[211] L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava, R. Matulevicius, A.-A.-O. Affia, M. Laurent, N. H. Sultan, and Q. Tang, "Post-quantum era privacy protection for intelligent infrastructures," *IEEE Access*, vol. 9, pp. 36038–36077, 2021.
[212] E. Jömeri, "Code-based cryptography," M.S. thesis, School Sci., Aalto Univ., Espoo, Finland, 2020.
[213] V. B. Y. Kumar, N. Gupta, A. Chattopadhyay, M. Kasper, C. Kraus, and R. Niederhagen, "Post-quantum secure boot," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2020, pp. 1582–1585.
[214] L. A. L. Pérez, L. J. M. Arrieta, F. S. H. Mendoza, L. A. L. Servín, and E. S. Acevedo, "Public hash signature for mobile network devices," *Ingeniería Investigación y Tecnología*, vol. 20, no. 2, pp. 1–10, Apr. 2019.
[215] K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto, and T. Schroeter, "Blockchained post-quantum signatures," in *Proc. IEEE Int. Conf. Internet Things*, Jul. 2018, pp. 1196–1203.
[216] D. Butin, J. Walde, and J. Buchmann, "Post-quantum authentication in OpenSSL with hash-based signatures," in *Proc. 10th Int. Conf. Mobile Comput. Ubiquitous Netw. (ICMU)*, Oct. 2017, pp. 1–6.
[217] O. Potii, Y. Gorbenko, and K. Isirova, "Post quantum hash based digital signatures comparative analysis. Features of their implementation and using in public key infrastructure," in *Proc. 4th Int. Sci.-Practical Conf. Problems Infocommun.*, Oct. 2017, pp. 105–109.
[218] Z. Wang, D. Tang, H. Yang, and F. Li, "A public key encryption scheme based on a new variant of LWE with small cipher size," *J. Syst. Archit.*, vol. 117, Aug. 2021, Art. no. 102165.
[219] X. Lu and J. Zhang, "Lattice-based PKE/KEM," *Natl. Sci. Rev.*, vol. 4, May 2021, Art. no. nwab090.
[220] M. Bisheh-Niasar, R. Azarderakhsh, and M. Mozaffari-Kermani, "High-speed NTT-based polynomial multiplication accelerator for CRYSTALS-kyber post-quantum cryptography," Cryptol. ePrint Arch., Santa Barbara, CA, USA, Tech. Rep. 563, 2021.

[221] G. Mazzola, K. Liang, and H. Chen. (2021). *Investigation on NIST Post-Quantum Lattice-Based Encryption Schemes*. Accessed: Jul. 9, 2021. [Online]. Available: https://repository.tudelft.nl/islandora/object/uuid:57f7922f-93ad-4411-b6c2-9c5a8a5a845e
[222] N. Raviv, B. Langton, and I. Tamo, "Multivariate public key cryptosystem from sidon spaces," *Public Key Cryptogr.*, vol. 1, pp. 242–265, Jun. 2021.
[223] S. Dai, "Quantum cryptanalysis on a multivariate cryptosystem based on clipped Hopfield neural network," *IEEE Trans. Neural Netw. Learn. Syst.*, early access, Mar. 1, 2021, doi: 10.1109/TNNLS.2021.3059434.
[224] M. Øygarden, D. Smith-tone, and J. Verbel, "On the effect of projection on rank attacks in multivariate cryptography," in *Proc. IACR*, 2021, pp. 1–16.
[225] N. Kundu, S. K. Debnath, D. Mishra, and T. Choudhury, "Post-quantum digital signature scheme based on multivariate cubic problem," *J. Inf. Secur. Appl.*, vol. 53, Aug. 2020, Art. no. 102512.
[226] A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem, "GeMSS: A great multivariate short signature," UPMC-Paris Sorbonne Univ., Paris, France, Tech. Rep., 2017.
[227] H. Onuki and T. Moriya, "Radical isogenies on Montgomery curves," in *Proc. ICAR*, 2021, pp. 1–22.
[228] D. Buell, "Lattice-based cryptography and NTRU," in *Fundamentals Cryptography*. Cham, Switzerland: Springer, 2021, pp. 205–221.
[229] C. Li, Y. Tian, X. Chen, and J. Li, "An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems," *Inf. Sci.*, vol. 546, pp. 253–264, Feb. 2021.
[230] J. Qian, Z. Cao, M. Lu, X. Chen, J. Shen, and J. Liu, "The secure lattice-based data aggregation scheme in residential networks for smart grid," *IEEE Internet Things J.*, early access, Jun. 17, 2021, doi: 10.1109/JIOT.2021.3090270.
[231] J. Ding and A. Petzoldt, "Current state of multivariate cryptography," *IEEE Secur. Privacy*, vol. 15, no. 4, pp. 28–36, 2017, doi: 10.1109/MSP.2017.3151328.
[232] J. Hoffmann, H. Hermanns, M. Klauck, M. Steinmetz, E. Karpas, and D. Magazzeni, "Let's learn their language? A case for planning with automata-network languages from model checking," in *Proc. AAAI Conf. Artif. Intell.*, 2020, vol. 34, no. 9, pp. 13569–13575.
[233] S.-L. Zhou, Y.-H. Kang, H.-D. Dai, and Z. Chao, "Multi-UAVs formation autonomous control method based on RQPSO-FSM-DMPC," *Math. Problems Eng.*, vol. 2016, Sep. 2016, Art. no. 4878962.
[234] M. P. Bianchi, C. Mereghetti, and B. Palano, "Quantum finite automata: Advances on Bertoni's ideas," *Theor. Comput. Sci.*, vol. 664, pp. 39–53, Feb. 2017.
[235] M. Finiasz and N. Sendrier, "Security bounds for the design of code-based cryptosystems," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2009, pp. 88–105.
[236] Ö. Dagdelen, M. Fischlin, and T. Gagliardoni, "The fiat–shamir transformation in a quantum world," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2013, pp. 62–81.
[237] P. S. Barreto, S. Gueron, T. Güneysu, R. Misoczki, and E. Persichetti, "CAKE: Code-based algorithm for key encapsulation," in *Proc. IMA Int. Conf. Cryptogr. Coding*, 2017, pp. 207–226.
[238] R. Behnia, "Efficient post-quantum and compact cryptographic constructions for the Internet of Things," Ph.D. dissertation, Dept. Comput. Sci. Eng., College Eng., Univ. South Florida, Tampa, FL, USA, 2021.
[239] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for internet of drones for smart city surveillance," *J. Syst. Archit.*, vol. 115, May 2021, Art. no. 101955.
[240] R. El Bansarkhani and R. Misoczki, "G-Merkle: A hash-based group signature scheme from standard assumptions," in *Proc. Int. Conf. Post-Quantum Cryptogr.*, 2018, pp. 441–463.
[241] A. Nitaj, *Quantum and Post Quantum Cryptography*. Princeton, NJ, USA: Citeseer, 2021.
[242] A. Metelmann, "A superconducting qubit that protects itself," *Physics*, vol. 14, p. 25, Feb. 2021.
[243] S. Krinner, S. Storz, P. Kurpiers, P. Magnard, J. Heinsoo, R. Keller, J. Lütolf, C. Eichler, and A. Wallraff, "Engineering cryogenic setups for 100-qubit scale superconducting circuit systems," *EPJ Quantum Technol.*, vol. 6, no. 1, Dec. 2019, Art. no. 2.
[244] A. Cho. (Sep. 2020). *IBM Promises 1000-Qubit Quantum Computer Milestone-by 2023*. Accessed: Jun. 26, 2021. [Online]. Available: https://www.sciencemag.org/news/2020/09/ibm-promises-1000-qubit-quantum-computer-milestone-2023
[245] S. Pakin and P. Coles, *The Problem with Quantum Computers*. New York, NY, USA: Scientific American, 2019. Accessed: Jun. 26, 2021. [Online]. Available: https://blogs.scientificamerican.com/observations/the-problem-with-quantum-computers/
[246] A. Cintas-Canto, "Efficient hardware constructions for error detection of post-quantum cryptographic schemes," Univ. South Florida, Tampa, FL, USA, Tech. Rep., 2021. [Online]. Available: https://scholarcommons.usf.edu/etd/8750
[247] M. Kop, *Establishing a Legal-Ethical Framework for Quantum Technology*. Yale Law School, Yale Journal of Law & Technology, Yale Univ., New Haven, CT, USA, 2021.
[248] H. Ball, M. Biercuk, A. Carvalho, J. Chen, M. Hush, L. De Castro, and L. Li, "Software tools for quantum control: Improving quantum computer performance through noise and error suppression," *Quantum Sci. Technol.*, pp. 1–56, Jan. 2021.
[249] Y. Li, A. H. Aghvami, and D. Dong, "Intelligent trajectory planning in UAV-mounted wireless networks: A quantum-inspired reinforcement learning perspective," *IEEE Wireless Commun. Lett.*, early access, Jun. 16, 2021, doi: 10.1109/LWC.2021.3089876.
[250] Y. Li, A. Hamid Aghvami, and Y. Deng, "Joint resource block and beamforming optimization for cellular-connected UAV networks: A hybrid D3QN-DDPG approach," 2021, *arXiv:2102.13222*. [Online]. Available: http://arxiv.org/abs/2102.13222
[251] S. Perkins. (Mar. 2016). *Tiny Gravity Sensor Could Detect Drug Tunnels, Mineral Deposits*. Accessed: May 3, 2021. [Online]. Available: https://www.sciencemag.org/news/2016/03/tiny-gravity-sensor-could-detect-drug-tunnels-mineral-deposits

ADARSH KUMAR received the master's degree (M.Tech.) in software engineering from Thapar University, Patiala, Punjab, India, and the Ph.D. degree from Jaypee Institute of Information Technology University, Noida, Uttar Pardesh, India. He held a postdoctoral position with the Software Research Institute, Athlone Institute of Technology, Ireland. From 2005 to 2016, he has been associated with the Department of Computer Science Engineering and Information Technology, Jaypee Institute of Information Technology, where he worked as an Assistant Professor. He is currently an Associate Professor with the School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India. He has many research papers in reputed journals, conferences, and workshops. He participated in one European Union H2020 Sponsored Research Project and he is executing two research projects sponsored from UPES SEED Division and one sponsored from Lancaster University. His main research interests include cybersecurity, cryptography, network security, and *ad-hoc* networks.

SURBHI BHATIA received the bachelor's degree in information technology, in 2010, the master's degree in technology from Amity University, in 2012, and the Ph.D. degree in computer science and engineering from Banasthali Vidyapith, India. She is currently an Assistant Professor with the Department of Information Systems, College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia. She has rich eight years of teaching and academic experience. She has published many research papers in reputed journals and conferences in high indexing databases and has patents, granted from USA, Australia, and India. Her research interests include machine learning, sentiment analysis, and information retrieval. She has authored two books and edited seven books from Springer, Wiley, and Elsevier. She has completed two funded research projects from the Deanship of Scientific Research, King Faisal University and Ministry of Education, Saudi Arabia. She has earned the Professional Management Professional Certification from PMI, USA. She has delivered talks as a keynote speaker in IEEE conferences and in faculty development programs. She is serving as a guest editor for special issues in reputed journals. She is the Editorial Board Member in the *International Journal of Hybrid Intelligence* (Inderscience Publishers) and *SN Applied Sciences* (Springer).

KESHAV KAUSHIK received the B.Tech. degree in computer science and engineering from the University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak, and the M.Tech. degree in information technology from the YMCA University of Science and Technology, Faridabad, Haryana. He is currently pursuing the Ph.D. degree in cybersecurity and forensics. He is an Assistant Professor with the Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India. He is an experienced educator with over six years of teaching and research experience in the area of cybersecurity, the Internet of Things, and blockchain technology. He has published several research papers in international journals and has presented at reputed international conferences. His research interests include blockchain technology, cybersecurity, and the Internet of Things.

S. MANJULA GANDHI received the master's degree in computer applications from the University of Madras, the post master's degree (M.S. By Research), and the Ph.D. degree from Anna University. She is currently working as an Associate Professor with the Department of Computing, Coimbatore Institute of Technology, India. She has 20 years of teaching experience in multi discipline specialization of computer science. Her research interests include quantum computing, quantum graph theory algorithms, quantum arithmetic circuits, and quantum machine learning. She has worked on projects as a part of IBM Advocate Mentorship Program, and playing the role of a Translation Lead for translating Qiskit textbook to Tamil language. She has guided nearly 200 PG projects and has 25 publications in various journals and conferences. She has received Qiskit Advocate Advanced Certification from IBM Quantum, in September 2020. She has received the Distinguished Alumni Award from Maitreyi College, University of Delhi, in April 2021.

S. GAYATHRI DEVI received the bachelor's, master's, and M.Phil. degrees and the Ph.D. degree in multicast routing protocols in mobile *ad-hoc* networks from Bharathiar University. She is currently an Assistant Professor with the Faculty of Data Science, Coimbatore Institute of Technology (CIT), India. She published a number of articles in preferred journals and chapter in a book. She has participated in a range of workshops and summer schools, including IBM Quantum Global Summer School, in 2020 and 2021. She also presented various academic as well as research-based papers at several national and international conferences.

DIEGO A. DE J. PACHECO has 18 years' experience in industry and ten years' experience in academy duties as a Professor, the Head of the Department of Production Engineering and the Department of Industrial Engineering Management, and the Dean of the Department of Mechanical Engineering and Academic Manager. His primary areas of research interests include industry 4.0/5.0, digitalization, and innovation. He has over 190 scientific articles published in peer-reviewed journals and conferences. He serves as a Revisor and an Editor for top-ranking journals, including IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, *IJPR*, *IJPPM*, *JCLP*, *IJLSS*, and others.

ARWA MASHAT received the Ph.D. degree in instructional design and technology from Old Dominion University, USA. She is currently an Assistant Professor with the Information System Department, Faculty of Computing and Information Technology, King Abdulaziz University, Rabigh, Saudi Arabia. Her research interests include eye tracking, education technology, online learning, and the Internet of Things.