IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 April 2024, accepted 3 May 2024, date of publication 15 May 2024, date of current version 24 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3401162

RESEARCH ARTICLE

Quantum Computing Integrated Patterns for Real-Time Cryptography in Assorted Domains

SHALLY NAGPAL[1], SHIVANI GABA[1], ISHAN BUDHIRAJA[2], MEENAKSHI SHARMA[3], AKANSHA SINGH[2], KRISHNA KANT SINGH[4], S. S. AKSAR[5], MOHAMED ABOUHAWWASH[6], AND CELESTINE IWENDI[7], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Panipat Institute of Engineering and Technology, Panipat 132102, India
[2]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh 201310, India
[3]Department of Electronics and Communication Engineering, Inderprastha Engineering College, Ghaziabad, Uttar Pradesh 201010, India
[4]Delhi Technical Campus, Greater Noida, Uttar Pradesh 201306, India
[5]Department of Statistics and Operations Research, College of Science, King Saud University, Riyadh 11451, Saudi Arabia
[6]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura 35516, Egypt
[7]School of Creative Technologies, University of Bolton, BL3 5AB Bolton, U.K.

Corresponding author: Akansha Singh (akansha1.singh@bennett.edu.in)

This work was supported by King Saud University, Riyadh, Saudi Arabia, through the Researchers Supporting Project under Grant RSP2024R167.

ABSTRACT Quantum computers use quantum-mechanical phenomena for knowledge manipulation and depend on quantum bits or qubits. A qubit can be created in several different ways, and out of this, one way of creating a quantum state is by using superconductivity. They must be held very cold to work on these superconductive qubits for long periods. The key to information storage and manipulation is the skill of all computer systems. Current traditional computers handle single bits stored in binary states of 0 and 1 form. Every temperature factor inside the device may be updated; thus, quantum computers are more excellent than the vacuum of space at temperatures similar to absolute null. Consider how the dilution refrigerator of a quantum computer consisting of over 2000 components provides a cold atmosphere for the inside of the qubits. Researchers from all around the world today are using actual quantum processors for validating algorithms for different fields of operation. Yet quantum computation was a strictly speculative topic a couple of decades ago. Quantum cryptography, also known as quantum encoding, uses quantum mechanics principles to encrypt messages in a way nobody else reads. It benefits quantum states, along with its "theory of no transition," which means that it cannot be disrupted unknowingly. Quantum-improved AI calculations are especially applicable to the area. This work focuses on the implementation patterns of quantum computing in real-time cryptography so that the overall communication will be secured and integrity aware.

INDEX TERMS Quantum cryptography, real time cryptography, security, integrity in real world environment.

I. INTRODUCTION

In everyday use, quantum computers use ions or photons as qubits, the critical segment of quantum physics. The crucial part of creative problem solving is generating, controlling, or manipulating qubits for high-performance and multi-dimensional approaches. Superconductive circuits can be operated at temperatures as low as those seen in outer space, for example, at the low-temperature area for many companies such as IBM, Google, and Rigetti. IonQ researchers use ultra-high vacuum chambers to trap single atoms within electromagnetic fields. However, in each situation, it is meant

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

to be isolated differently. According to current technology, computers, current ones operate on 'pulses' (an electrical or optical stream of ones and zeros) [1], [2], [3].

The fundamentals of Quantum Computing include a more detailed overview of the fundamental principles of quantum computing. This will encompass a discussion on quantum bits (qubits), their unique properties, and the principles of superposition and entanglement that distinguish quantum computing from classical computing.

The introduction of quantum computing revolutionizes our understanding of computation, delving into the realm of quantum mechanics and offering unprecedented computational power and efficiency. Unlike classical computers that operate based on bits in binary states of 0 and 1, quantum computers leverage quantum bits or qubits, which can exist in multiple states simultaneously due to principles like superposition and entanglement. These unique properties enable quantum computers to solve complex problems exponentially faster than classical computers, making them particularly promising for a wide range of applications.

Quantum computing architectures encompass various models, from gate-model quantum computers utilizing quantum circuits and logic gates to adiabatic quantum computers and quantum annealers that tackle specific problem classes. Recent advancements in quantum computing, such as demonstrations of quantum supremacy, improvements in quantum error correction techniques, and scalability of qubit systems, highlight the rapid evolution of this field. Real-world applications, including quantum-enhanced optimization algorithms, simulations in material science, and breakthroughs in cryptography through algorithms like Shor's for integer factorization, underscore the practical relevance of quantum computing across diverse domains.

However, alongside these advancements come significant challenges. Qubit decoherence, arising from interactions with the environment, remains a critical hurdle in maintaining quantum coherence and executing error-free computations. Addressing these challenges requires advancements in fault-tolerant quantum computing and scalable quantum hardware, paving the way for practical implementation in various sectors.

The ongoing research endeavors aim to unlock the full potential of quantum computing, realizing fault-tolerant quantum computers, exploring new quantum algorithms for optimization and machine learning, and revolutionizing industries ranging from finance to healthcare. The integration of quantum computing with real-time cryptography opens new horizons for secure communication and data processing, with implications extending to smart cities, IoT, and beyond.

The Key Advancements in Quantum Computing on the fundamental principles incorporate the key advancements in quantum computing. This may include recent breakthroughs in quantum hardware, novel algorithms, and notable achievements in the practical implementation of quantum processors. Moreover, the practical implications of quantum computing in real-world applications.

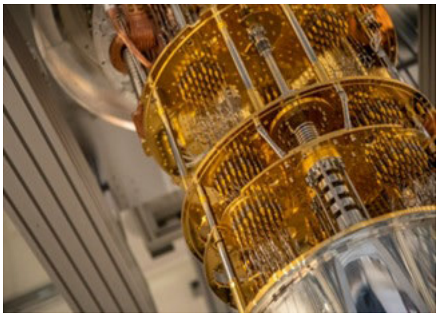


FIGURE 1. High performance quantum computers [26].

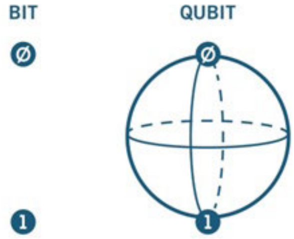


FIGURE 2. Bits and qubits in quantum computing [6].

Quantum registering may bring supersonic medication plan, in silico clinical preliminaries with virtual people reproduced 'live,' max control entire genetic sequencing and examination, the development of emergency clinics to the cloud, the accomplishment of prescient health, or the security of clinical information using quantum vulnerability and high-performance quantum computers are shown in Fig.1.

Qubits have specific strange quantum properties, meaning that a set of them can deliver much greater computing capacity with the interlocking, and therein the critical dimensions are required with high integrity [4], [5]. Qubits are the main aspects of quantum computing, and it's used in various implementations, including security, privacy, integrity, optimization factors, and many others, as shown in Fig.2.

Quantum computing makes use of quantum bits, or qubits, which can exist in several states concurrently because of the laws of superposition and entanglement. Traditional bits used in classical computing can only be 0 or 1. Real-time cryptography is the use of cryptographic techniques to ensure data security even during fast data transmission. These techniques must be able to encrypt and decrypt data quickly enough to meet real-time communication or processing demands. Integrated Patterns are well-established frameworks or methods for applying quantum computing concepts to a variety of industries, including telecommunications, healthcare, and finance, in order to streamline workflows or resolve challenging issues in a range of diverse fields.

A. OVERLAY AND SUPERPOSITION

Numerous combinations of 1 and 0 can simultaneously serve qubits. Superposition is called this potential to be

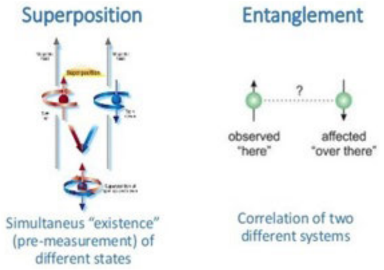

Superposition
Entanglement
observed "here"
?
affected "over there"
Simultaneus "existence" (pre-measurement) of different states
Correlation of two different systems

FIGURE 3. Superposition and entanglement in quantum computing [13].

TABLE 1. Classical vs quantum computing.

Parameters of comparison	Classical Computing	Quantum Computing
Information processing	Using Logic gates like AND, OR	Using quantum logic
Error rates	Classical computing has a less error rate	Quantum computing has a high error rate
States and Phases	Discrete	Continuous
Suitability	Classical computing is best suitable for the daily processing	Quantum computing is best appropriate for data analysis
Operations	Linear algebra	Boolean algebra

concurrently in different states. To overlay qubits, researchers use precise lasers or microwave beams to control them. This approach achieves a higher degree of accuracy with accuracy in the implementation patterns [7], [8].

The strength of quantum computers is critical, whereby elevating the computing power with doubling in a traditional device doubles the number of bits [6], [9], [10], [11], [12], [13], [14]. However, the combination of additional qubits in a quantum computer exponentially increases the numerical reduction capacity.

Superposition and Entanglement in Quantum Computing are shown in Fig.3. Quantum computers use intertwined qubits to work their magic through a quantum daisy chain [15], [16]. This is the reason why there are so many excited about their capacity for machines' ability to speed up calculations by specific quantum algorithms. It is the critical base of quantum systems with tremendous accuracy and minimum errors [4], [17].

B. DECOHERENCE AND DECOMPOSITION IN QUANTUM

Quantum computing integrates coherence and decoherence and is called the breakdown between qubits and their surrounding context. When two or more quantum particles are incredibly close, their properties may be uncertain or random. The minor vibration or temperature changes – called quantum-speak "noise" – may cause them to overlap until their task is performed correctly [18], [19]. This is why researchers are doing their best to shield qubits in supercooled fridges and vacuum rooms from the outside world. This cooling factor and the controlled temperature is integrated for performance in the implementation scenarios of quantum systems [20].

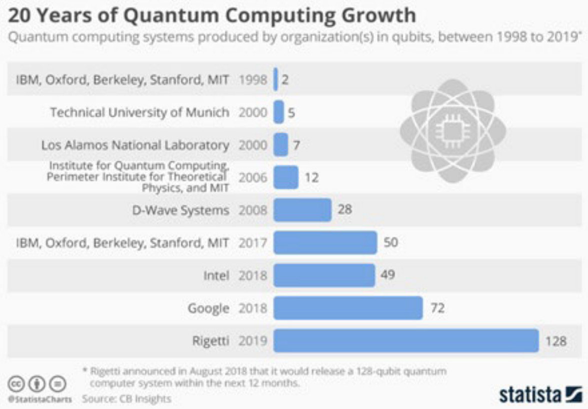


FIGURE 4. Research Analytics by Statista [14].

However, noise also leads several mistakes to slipping into equations, despite their attempts. Any of them can be compensated by intelligent quantum algorithms, which can help incorporate more qubits. However, developing a single, extremely stable "logical" qubit will likely require thousands of stable qubits [21], [22], [23]. This envisages a quantum computer's computing ability for assorted phases and layers of implementations [24].

The numbers of bits are required to be controlled with tremendous accuracy and maximum throughput, and that is where a mathematical equation can be carried out, which is clearly beyond even the powerful supercomputer's grasp [25], [26]. The number of qubits to do this is still uncertain because researchers continue to discover new algorithms to improve the efficiency of conventional machines, and supercomputer software is improving [27].

There is much discussion in the field of science about how important this landmark is to be achieved. Companies are now beginning to test quantum computers from companies such as IBM, Rigetti, and D-Wave, a Canadian company, instead of waiting before the dominance is announced and is implemented by corporate giants to massive implementation levels for social and corporate segments and growth of quantum Computing by Statista is shown in Fig.4.

C. QUANTUM ALGORITHMS VS. CLASSICAL ALGORITHMS IN CRYPTOGRAPHY

In this section, we delve into the fundamental differences between quantum algorithms and classical algorithms in the realm of cryptography, elucidating how their distinct features impact their working mechanisms.

1) QUANTUM ALGORITHM BASICS

1) Quantum Bits (Qubits):One of the foundational disparities lies in the representation of information. While classical algorithms operate with classical bits, which can exist in a state of 0 or 1, quantum algorithms leverage quantum bits or qubits. Qubits, due to the principles of superposition and entanglement, can exist

in multiple states simultaneously, enabling quantum algorithms to perform parallel computations in a way classical algorithms cannot.

2) Quantum Parallelism: Quantum algorithms harness quantum parallelism to process a multitude of possibilities simultaneously. Classical algorithms, on the other hand, process each possibility sequentially. This inherent parallelism grants quantum algorithms a potential advantage in certain computational tasks.
3) Quantum Cryptographic Algorithms:
   - Shor's Algorithm for Integer Factorization: A prominent example of the quantum advantage in cryptography is Shor's algorithm. This quantum algorithm efficiently factors large integers exponentially faster than the best-known classical algorithms. The security of widely-used cryptographic schemes, such as RSA, relies on the difficulty of factoring large numbers. Shor's algorithm introduces a quantum speedup that poses a threat to the classical security assumptions underpinning such schemes.
   - Grover's Algorithm for Search: Grover's algorithm showcases another facet of quantum superiority by providing a quadratic speedup in unstructured search problems. In the context of cryptography, this algorithm can be applied to search a database or an unsorted list, reducing the search time significantly compared to classical search algorithms.
4) Quantum Key Distribution (QKD):
   - Quantum Entanglement in QKD: Quantum Key Distribution (QKD) is a cryptographic protocol that utilizes the principles of quantum mechanics to secure communication channels. Unlike classical key distribution methods, QKD leverages quantum entanglement to establish a shared secret key between two parties. The security of the key is guaranteed by the principles of quantum mechanics, making it resistant to eavesdropping attempts.
   - No-Cloning Theorem: The No-Cloning Theorem, a fundamental principle of quantum mechanics, states that an arbitrary unknown quantum state cannot be cloned perfectly. This theorem is exploited in quantum cryptography to detect any attempt to intercept or clone quantum keys. Classical key distribution systems do not benefit from this inherent quantum protection.
5) Post-Quantum Cryptography:
   - Quantum Threats to Classical Cryptography: The advent of quantum computing introduces new challenges to classical cryptographic systems. Algorithms such as Shor's can potentially break widely-used public-key cryptosystems. As a response, the field of post-quantum cryptography is actively exploring cryptographic schemes that resist quantum attacks, ensuring the continued security of communication in a post-quantum era.
6) Quantum Cryptographic Protocols:
   - Quantum Coin Protocols: Quantum cryptographic protocols, such as quantum coin disputes, illustrate the unique challenges and advantages presented by quantum communication. These protocols leverage the properties of quantum mechanics to establish secure and tamper-evident communication channels between untrusted participants.
7) Challenges and Opportunities:
   - Quantum Errors and Noise: Quantum algorithms face challenges such as errors and noise due to the delicate nature of quantum states. Implementing error-correction techniques becomes crucial to maintain the integrity of quantum cryptographic systems. Classical algorithms, not subject to quantum noise, do not face this particular challenge.

In conclusion, quantum algorithms in cryptography harness the principles of quantum mechanics to perform computations and establish secure communication channels in ways that classical algorithms cannot replicate. The parallelism that qubits provide, the effectiveness with which they solve particular issues, and the distinctive characteristics of quantum cryptography highlight the transformative potential of quantum technologies in the field of information security.

II. USE CASES OF QUANTUM COMPUTING

Quantum encryption is the knowledge of using quantum mechanical properties to carry out encryption activities. Quantum encryption is the best-known example of a quantum key distribution that provides an informatively safe approach to the critical exchange problem [28]. The benefit of quantum cryptography is that the completion using conventional (non-quantum) communication only of different cryptographic activities can be proved or supposedly unlikely. For instance, data encoded in a quantum state cannot be copied. The quantum condition is modified as you try to decipher the coded data by collapsing the wave function (no-cloning theorem). This can track the number of main deliveries eavesdropping [29]. In the data-protection chain, cryptography is the most potent component. However, stakeholders cannot believe that encryption keys remain forever stable. The topic of quantum cryptography encompasses various cryptographic practices and protocols. The following discusses some of the more significant applications and protocols [5], [31].

Quantum key distribution (QKD) is the most often used for situations where a third party cannot uncover the key even though Person-1 and Person-2 may exchange information. If a third party wants to think about the key to be found, there would be inconsistencies between Person-1 and Person-2. Using traditional methods, the key is then usually used for secure communications. For example, for symmetric cryptography, the exchanged key may be used [32], [33].

FIGURE 5. IBM quantum computer [30].

It was shown mathematically that, unlike standard key distribution, Quantum Key Distribution (QKD) would not restrict the eavesdropping of an adversary. It is commonly known as "unconditional security and protection aspects"; however, different laws of quantum mechanics are needed, i.e., Person-1 should be able to authenticate him, and Person-2 should be unable to impersonate him [19], [21], [22].

Although QKD does look good, the prospect of successfully implementing it is challenging. This is attributable to the inadequate distance between primary and secondary power plants. The new and continuing investigation results have just widened the boundaries. Two-field QKD (TF-QD) approach could theoretically solve the scaling out of a failure channel in the twinning flow method and demonstrate that its covert function, known as the PLOB, was no longer present at 340 km of optical fiber; in reality, it surpassed it at 200 km before hitting the loss-scaling of its non-repeating primary capability. They were unable to follow up. The analysis indicates that "550-kilometer standard fiber," still the default for modern communications, can get optimal performance. Though TF-QD tends to increase local network bandwidth, the Sending-Not-Sending (SNS) Version yields impressive overall speed over long distances.

III. QUANTUM ENCRYPTION AND SECURITY PERSPECTIVES

The parties involved do not trust each other in mistrustful cryptography. For example, Person-1 and Person-2 join private entries to carry out the calculation. They work together [34], [35]. But Person-1 has no faith in Person-2, and Person-2 has no trust in Alice [36]. So, a stable cryptographic job demands that Person-1 can promise that Person-2 has not cheated after the calculation has been completed and that Person-2 is therefore specific that Person-1 has not fooled. For example, commitments and stable calculations, including other cases of coin flipping and forgetful transfer, work in mistrusted cryptography. The key distribution is not in the field of mistrustful encryption [37]. The wary quantum cryptography uses quantum systems to examine the area of manipulative cryptography and can be integrated to track the communication and sniffing attempts [38].

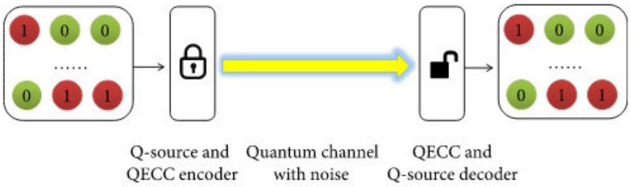

1
0
0
......
0
1
1
1
0
0
......
0
1
1
Q-source and QECC encoder
Quantum channel with noise
QECC and Q-source decoder

FIGURE 6. Quantum based secured communication.

Protocols not only use quantum mechanics but may provide total security if it also utilizes special relativity. To name a few, Mayers each provided "confirmed proof" instances of unconditionally secure quantum bit involvement. This is the process: After lo and Chau reached the perfect quantum gold, they had no chance of bringing more bricks to the mission. Lo has proven that one out of two ignorant transfers and the other two would still be unsafe. I'm working my way down the list, writing the following are the following: However, Kent has shown these "relativistic" and "primitive" protocols to be somewhat conservative.

A. QUANTUM COMPUTING AND REAL TIME CRYPTOGRAPHY

Contrary to the distribution of quantum keys, quantum coins are a protocol between two participants that have no confidence in each other. Participants can interact and share information through qubits. Via a quantum channel, Person-1 and Person-2 are not confident of each other, so everyone wants the other to lie. More work, therefore, needs to be done to ensure that neither Person-1 nor Person-2 will achieve a significant advantage over the others to generate a desirable result. The power to manipulate a particular outcome is called a bias, and protocols that reduce a deceptive player's bias are developed [39], [40]. Stealing is otherwise known, as shown in Fig. 6. Regarding quantum communication protocols, including the quantum coin reversion, significant safety benefits have been demonstrated over traditional communication, but in practice, they are difficult to achieve [41]. Manipulation and tampering happen when a player tries to manipulate a specific outcome or increases its likelihood [28], [31]. For example, Person-1 could cheat by arguing that Person-2 wrongly guessed her initial foundation when he correctly thought, but Person-1 will have to create a new string of qubits that exactly matches what Person-2 calculated on the other side of the table. Her probability of producing a similar qubit will decline exponentially, and if Person-2 notes a misunderstanding, he will know that she lied. Person-1 can also create a chain of photons with a combination of states, but Person-2 can see that her chain partly (but not entirely) correlates with the two sides of the table and knows that she is tricked in the process. An intrinsic defect of existing quantum devices still exists. Errors and lost qubits can impact the measures of Person-2 and lead to gaps in

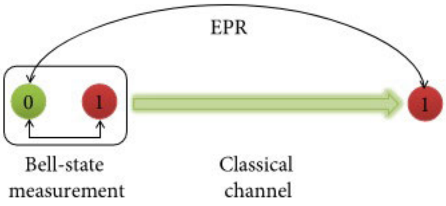


FIGURE 7. Quantum based channel.

the measuring table of Bob. Significant calculation losses would impair the capacity of Person-2 in a step to validate the qubit sequence of Person-1 [42]. It is possible to have the Einstein-Podolsky-Rosen (EPR) paradox, that's certain. Two photons in anisotropic; two, polarized, for as long as they are measured the same way, are in an EPR pair [33], [37]. A Person could do this. Person-1 could transmit one photon to Person-2 and save Person-2's bits. Meanwhile, Person-2 will be determining her EPR photon pairs on the other side of the room and establishing an ideal relation to the other table. She never knew that she was breaking the rules as long as that did all well. It will take quantum-based technology that does not currently exist, which, in reality, is impossible. To be effective, Person-1 should be able to store and count nearly all the photons effectively, as shown in Fig. 7. This may be because all missing photons count as nulls in the series. The overall communications using such an approach are highly monitored and can be tracked.

Quantum coin disputes are typically seen in situations where mistrust is involved. To build a reward program, you have to measure a benefit that Person-1 can't alter, and recipients won't know about it until Person-1 has the chance to comment about it. It cannot be changed. Such strategies are often used in cryptography.

It has been integrated that an absolute-safety protocol can be constructed from a pledge and a quantum tube [36]. At the same time, simultaneously, Kilian developed a slight touch, on the other hand, had an obscure distribution method that allowed almost any computing device to be transported safely (so-called secure multiparty computation). Let's clear it up and say that we are unsure about the wording because we are only aware of the gist of the definition of the concept) Let's clarify that we are aware only of the gist of the concept. One can conduct multiparty computation given dedication and a quantum channel (it does not necessarily have to be physical). Researchers cannot make any claims about 'possibility,' which means you can lose defense of the study results [40], [43].

Consequently, it has been shown that protocols for the early stages of quantum engagement are invalid. Mayers showed that no unconditionally stable quantum protocol is possible: the only kind of attack that a computationally limited attacker might launch is a running botnet. Even if Mayers can be successfully applied under conditions that are considerably weaker than sufficient for multi-card computation, there remains the probability of quantum protocols (and, thus, multiparty protocols). Below is an example of how quantum communication can be used to develop engagement protocols. The movement in, November 2013 introduces "conditional encryption," first seen internationally. The current scenarios are learning a new approach called "perfectly unconditional hiding," recently proposed by Yadav et al. constructions without the use of error-correcting subsystems (CTE) (BQSM) [2], [16], [21], [44], [45], [46]. This model postulates that the quantity of data an adversary can store has a known upper limit, the Q limit. However, constrained is not by the sum of classical (i., non-quantum) data they can keep. As the actual knowledge (as represented by a quantum memory of Qubit opposition) is deceptive, the proof is often calculated, or inconsistent competition between researchers allows a large amount of evidence to be measured by dishonest individuals.

Damä, Fehr, and Schaffner suggested that BQSM procedures were never meant to help the would-be engineers to save quantitative data for everybody. At least, it is possible to perform these tasks using today's state-of-the-the-the-art technology protocol implementations minor. The correspondence of creativity is only more significant than the constraint set of the adversary only knows one thing: Everything that has ever been written.

It provides an advantage to the BCNOS algorithm by assuming that the quantum memory of the competition opponents is weak. In the current day and age, single-qubit storage is challenging. This depends on the exact protocol.) By delaying the protocol, more time is allowed to be spent in the quantum storage cycle. According to the Wehner, Schaffner, and Terhal containment noises, the BQSM is implicated [24], [39]. Rather than limit the physical scale of his memory, an adversary can make incomplete use of available quantum devices of varying sizes. Sound canals are unavoidable due to the constant uncertainty at the quantum level Primitives are returned with sufficiently high noise levels as in the BQSM, and it is a model about noisy storage models [9].

Similar findings can be obtained in the classic setting if the opponent can record a bond to the quantity of definitive (non-quantum) data. The report was released. However, it has been shown that the honest parties still need to use a lot of memorandum in this model (especially the square root of the opponent's memory).

B. QUANTUM ENCRYPTION DEPENDING ON POSITION

Quantifying quantitative positioning aims to use a player's geographical location as its (only) credential. You want, for instance, to send a message to a player in a particular position to ensure it can only be read if the recipient party is in that same position [47], [48]. A player, Alice, needs to persuade the (honest) verifiers in the simple task of verifying the location that she's in a given place. Checking positions using classical protocols against colluded opposing opponents (those who govern all functions except the claimed location of the prover) was shown by Gao et al. Schemes are possible under different conditions on the opponents [10].

In 2002, Kent researched his position-based quantum systems, referred to as "quantum tagging" today. At the end of 2006, a U.S. patent was granted. The verge of a scientific breakthrough in using quantum effects for location checking appeared in the literature in 2010. The research of the Council of Europe (Council of Europe study) noted that the survey shows black people don't know how to give or receive instructions for gifts the same way that white people do [49], [50]. Thus other protocols to guarantee this are still refuted. In 2011, Buhrman et al. reported that using a large quantity of quantum entanglement had been unable to consistently provide the result (they use a double exponential number of EPRs, the number of qubits in which the honest player works). This result proves that the theory is wrong, but it does not invalidate the hypothesis of highly efficient quantum storage [11]. This pushed Beigi and König to develop new position authentication protocols. Lastly, they proved that an opponent is still robust under a certain amount of control by showing that their vulnerabilities remain linear, assuming their protocols still have a linear number of connected edges. Systematic checks are possible because time and energy by quantum effects are not addressed. Notice that the position study in quantum cryptography also discusses a more complex version of port-based teleportation called qubit teleportation [51].

C. QUANTUM COMPUTING AND REAL-TIME CRYPTOGRAPHY: A UNIFIED MODEL

In this section, we aim to elucidate the synergy between quantum computing and real-time cryptography, providing a comprehensive understanding of their collective functionality.

1) QUANTUM COIN PROTOCOLS FOR UNTRUSTED PARTICIPANTS

The introduction of quantum coins as a protocol between untrusted participants necessitates an exploration of the dynamics between Person-1 and Person-2. Through the use of qubits and a quantum channel, both individuals navigate a scenario where mutual distrust prevails. Protocols are introduced to mitigate biases, preventing any participant from gaining a significant advantage. Quantum coin disputes, often arising in mistrustful situations, involve strategies that measure benefits resistant to alteration by Person-1, aligning with principles employed in cryptography.

2) CHALLENGES IN QUANTUM COMMUNICATION PROTOCOLS

While quantum communication protocols, including quantum coin protocols, demonstrate significant safety benefits over traditional communication, practical challenges exist. Manipulation and tampering, where a player attempts to influence outcomes or increase their likelihood, pose threats. We delve into scenarios where Person-1 may attempt deception but faces challenges due to exponential declines in probability, photon chain correlations, and the intrinsic defects in existing quantum devices.

3) QUANTUM COIN DISPUTES AND CRYPTOGRAPHIC STRATEGIES

Quantum coin disputes are particularly relevant in situations involving mistrust [52]. The section highlights the use of cryptographic strategies to establish a reward program where the benefits are resistant to manipulation. The integration of absolute-safety protocols using pledges and quantum channels is explored, emphasizing the potential for secure multiparty computation.

4) CHALLENGES AND OPPORTUNITIES IN QUANTUM PROTOCOLS

Mayers' work on unconditionally stable quantum protocols is discussed, emphasizing the limitations of such protocols under computationally limited attacks. The introduction of conditional encryption and the exploration of "perfectly unconditional hiding" present current scenarios and advancements, including considerations of quantum memory constraints and potential dishonest practices.

5) QUANTUM MEMORY CONSIDERATIONS AND NOISE LEVELS

We delve into the challenges posed by quantum memory considerations and the implications of noise levels in protocols [53]. The BCNOS algorithm and its advantage over adversaries with weak quantum memory are discussed. Considerations of noise levels in storage models, such as the BQSM, highlight the unavoidable nature of sound canals and their impact on quantum storage.

6) IMPLICATIONS FOR REAL-TIME MODELS

The collective insights from quantum computing and real-time cryptography are then synthesized to discuss their implications for real-time models. We elaborate on how quantum protocols and cryptographic strategies collectively contribute to enhancing the security and efficiency of real-time communication.

IV. INNOVATIONS FOR REAL-WORLD APPLICABILITY

This section aims to augment our model study by incorporating innovations adapted for real-world applications. While our exploration of quantum computing and cryptography applications across diverse sectors is comprehensive, we recognize the importance of aligning our research with current developments and practical considerations.

A. PRACTICAL IMPLEMENTATION STRATEGIES

- This aspect focuses on bridging the gap between theoretical concepts and practical deployment of quantum computing and cryptography. It involves addressing challenges related to hardware limitations, scalability issues, and ensuring compatibility and interoperability with existing systems. Practical implementation strategies delve into the technical aspects of integrating quantum technologies into real-world scenarios, considering factors such as resource constraints, performance optimization, and system stability.

B. ADVANCES IN QUANTUM KEY DISTRIBUTION (QKD)

- Quantum Key Distribution (QKD) is a critical component of quantum-safe cryptography, and recent advancements in this field have significantly enhanced the security of cryptographic communication. This innovation emphasizes the exploration of cutting-edge QKD techniques that improve the generation and distribution of cryptographic keys in real-time scenarios. By incorporating these advances, our study remains at the forefront of ensuring secure communication channels in quantum computing environments.

C. QUANTUM-SAFE CRYPTOGRAPHY STANDARDS

- As quantum computing poses a potential threat to traditional cryptographic systems, there is a pressing need for developing quantum-safe cryptography standards and protocols. This innovation involves investigating the latest developments in cryptographic techniques that are resilient against quantum attacks. By staying updated on evolving standards, our research provides insights into implementing robust cryptographic systems capable of withstanding quantum threats in practical applications.

D. QUANTUM CLOUD COMPUTING INTEGRATION

- Cloud computing has become integral to modern IT infrastructures, and the integration of quantum computing with cloud platforms presents both opportunities and challenges. This innovation explores how quantum algorithms can be deployed and managed within cloud environments to leverage scalable resources and distributed computing capabilities. Understanding the benefits and challenges of quantum cloud computing is crucial for deploying quantum applications in real-world scenarios effectively.

E. CROSS-DISCIPLINARY APPLICATIONS

- Quantum computing and cryptography have transformative potential across various domains beyond traditional IT and cybersecurity [54]. This innovation highlights the diverse applications of quantum technologies in sectors such as healthcare, finance, logistics, and more. By showcasing cross-disciplinary applications, our study demonstrates the broad spectrum of real-world scenarios where quantum solutions can offer significant advancements and improvements.

F. QUANTUM ERROR CORRECTION CONSIDERATIONS

- Quantum systems are inherently susceptible to errors due to environmental factors and quantum decoherence. Quantum error correction techniques play a vital role in mitigating these errors and improving the reliability of quantum computations. This innovation focuses on discussing current state-of-the-art error correction methods and their applicability in real-world quantum computing scenarios. Addressing error correction challenges is essential for ensuring the practical viability of quantum computing technologies.

G. CONSIDERATIONS FOR QUANTUM CRYPTOGRAPHY ADOPTION

- Adopting quantum-safe cryptographic methods involves more than just technical aspects. This innovation explores practical considerations such as integration with existing communication infrastructure, user acceptance, regulatory compliance, and overall feasibility. Understanding the challenges and opportunities associated with quantum cryptography adoption is crucial for successful implementation and deployment in real-world communication systems.

These refined innovations collectively contribute to making our study more relevant, practical, and aligned with the current landscape of quantum computing and cryptography in real-world applications. By addressing these key areas, we aim to provide valuable insights and guidance for researchers, practitioners, and decision-makers navigating the complexities of quantum technologies.

V. PRACTICAL SIGNIFICANCE AND REAL-WORLD IMPLICATIONS

The practical significance of our research is further underscored by incorporating case studies and examples from various domains. These real-world illustrations not only validate the relevance of our research but also highlight its potential impact in diverse contexts.

For instance, consider the application of quantum computing in optimizing supply chain logistics. By leveraging quantum algorithms for route optimization and inventory management, companies can significantly reduce costs and improve efficiency. Case studies showcasing such implementations provide tangible evidence of how quantum computing can revolutionize traditional processes.

In the healthcare sector, quantum computing holds promise for accelerating drug discovery and personalized medicine. Quantum simulations can model complex molecular interactions, leading to the development of novel pharmaceuticals and treatment strategies. Real-life examples of successful drug discovery initiatives powered by quantum computing emphasize its transformative potential in advancing healthcare outcomes.

Furthermore, in the finance industry, quantum computing can revolutionize risk analysis, portfolio optimization, and fraud detection. By analyzing vast datasets and performing complex calculations at unprecedented speeds, quantum computers can provide valuable insights for making informed financial decisions. Case studies highlighting quantum-enhanced financial analytics demonstrate the practical benefits of integrating quantum technologies in the finance sector.

Additionally, the integration of quantum computing with cryptography opens new frontiers in cybersecurity.

Quantum-safe encryption algorithms protect sensitive data from quantum threats, ensuring secure communication channels in an era of advancing technologies. Examples of quantum-resistant cryptographic protocols in action showcase the critical role of quantum computing in safeguarding digital information.

These case studies and examples collectively emphasize the potential consequences and real-world applications of our research. They provide concrete evidence of how quantum computing can drive innovation, improve efficiency, enhance security, and ultimately impact various sectors in meaningful ways. By showcasing these practical implications, our research contributes to bridging the gap between theoretical concepts and practical implementations, paving the way for a quantum-powered future across diverse domains.

The case studies can be elaborated in different subsections which are discussed below:

A. IN-DEPTH CASE STUDIES

The case studies serve as tangible examples, showcasing how quantum computing integrated patterns can be applied to address specific challenges in real-world scenarios. By delving deeper into these examples, we aim to highlight the versatility and adaptability of our proposed patterns.

B. QUANTIFIABLE IMPACT

By discussing measurable outcomes, efficiency improvements, and advancements in security achieved through the integration of quantum computing into real-time cryptography, we aim to provide a clearer picture of the tangible benefits of our work.

C. INDUSTRY-SPECIFIC CONSEQUENCES

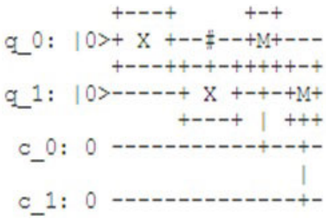
Recognizing the diverse nature of our case studies, we explicitly highlight the consequences and implications of our research within different industries. Tailoring our discussions to industry-specific contexts underscores the versatility of Quantum Computing Integrated Patterns, emphasizing how they can be adapted to address unique challenges within various sectors.

D. FUTURE SCENARIOS AND TRENDS

Anticipating the evolving technological landscape, we incorporate discussions on future scenarios and emerging trends. By exploring how our research might shape or respond to changing dynamics, we position our work as not only relevant in the present but also forward-thinking and adaptable to future challenges.

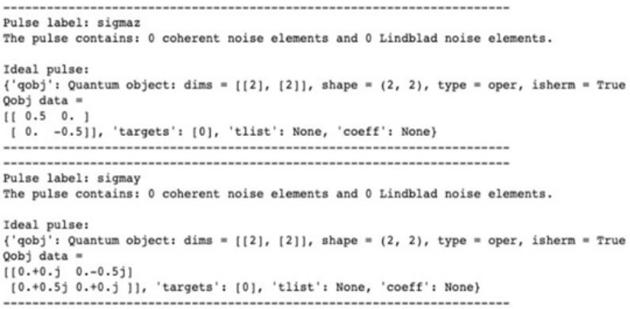
E. USER PERSPECTIVES

Including perspectives from potential end-users or stakeholders enriches our discussion on the practical significance and consequences of implementing Quantum Computing Integrated Patterns. By incorporating user viewpoints, we provide a more holistic understanding of how our research can be perceived, adopted, and adapted in real-world contexts.



```
        +----+    +-+
q_0: |0>+ X +--‡--+M+---
        +---++-+-+++++-+
q_1: |0>-----+ X +-+-+M+
             +---+ | +++
 c_0: 0 -----------+--+-
                      |
 c_1: 0 --------------+-
```

FIGURE 8. Quantum programming and circuit formation.



```
------------------------------------------------------------------------
Pulse label: sigmaz
The pulse contains: 0 coherent noise elements and 0 Lindblad noise elements.

Ideal pulse:
{'qobj': Quantum object: dims = [[2], [2]], shape = (2, 2), type = oper, isherm = True
Qobj data =
[[ 0.5  0. ]
 [ 0.  -0.5]], 'targets': [0], 'tlist': None, 'coeff': None}
------------------------------------------------------------------------
------------------------------------------------------------------------
Pulse label: sigmay
The pulse contains: 0 coherent noise elements and 0 Lindblad noise elements.

Ideal pulse:
{'qobj': Quantum object: dims = [[2], [2]], shape = (2, 2), type = oper, isherm = True
Qobj data =
[[0.+0.j  0.-0.5j]
 [0.+0.5j 0.+0.j ]], 'targets': [0], 'tlist': None, 'coeff': None}
------------------------------------------------------------------------
```

FIGURE 9. Log generation in quantum cryptography.

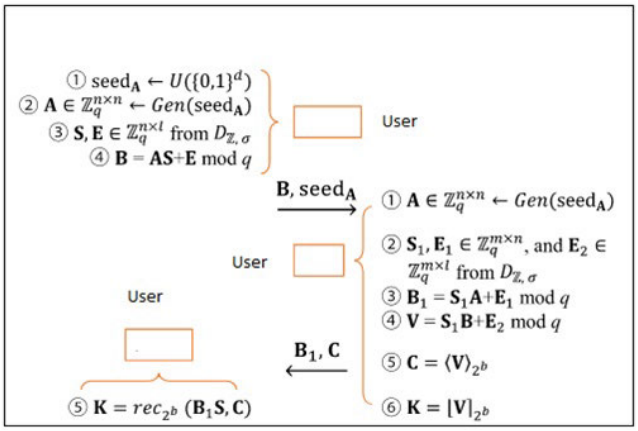

① $\mathrm{seed}_{\mathbf{A}} \leftarrow U(\{0,1\}^d)$
② $\mathbf{A} \in \mathbb{Z}_q^{n\times n} \leftarrow Gen(\mathrm{seed}_{\mathbf{A}})$
③ $\mathbf{S}, \mathbf{E} \in \mathbb{Z}_q^{n\times l}$ from $D_{\mathbb{Z},\sigma}$
④ $\mathbf{B} = \mathbf{AS}+\mathbf{E} \bmod q$
User
$\mathbf{B}, \mathrm{seed}_{\mathbf{A}}$
① $\mathbf{A} \in \mathbb{Z}_q^{n\times n} \leftarrow Gen(\mathrm{seed}_{\mathbf{A}})$
User
② $\mathbf{S}_1, \mathbf{E}_1 \in \mathbb{Z}_q^{m\times n}$, and $\mathbf{E}_2 \in \mathbb{Z}_q^{m\times l}$ from $D_{\mathbb{Z},\sigma}$
User
③ $\mathbf{B}_1 = \mathbf{S}_1\mathbf{A}+\mathbf{E}_1 \bmod q$
④ $\mathbf{V} = \mathbf{S}_1\mathbf{B}+\mathbf{E}_2 \bmod q$
$\mathbf{B}_1, \mathbf{C}$
⑤ $\mathbf{C} = \langle \mathbf{V} \rangle_{2^b}$
⑤ $\mathbf{K} = rec_{2^b}\,(\mathbf{B}_1\mathbf{S}, \mathbf{C})$
⑥ $\mathbf{K} = \lfloor \mathbf{V} \rceil_{2^b}$

FIGURE 10. Implementation pattern.

VI. IMPLEMENTATION PATTERNS

The implementation frameworks for quantum computing are in development; still, Python is one of the high-performance programming platforms that can be used for quantum-based real-time cryptography. Any fiber-optic cable may be an example of a quantum communication medium through which we can transmit individual photons (particles of light). Photons are called polarization and may be one of two states. Photons are called polarization. We can use this qubit, as shown in Fig. 8, Fig.9, and Fig 10.

The accompanying Table 1 portrays the security boundary dissected on simulation with grouped methodologies, including old-style crypto-sign and quantum-based unique security with successful security [47], [55]. The conventional method of crypto-signals incorporates the vital trade with old-style hash generation; however, it is powerless and ineffective for real-time situations. The execution examples of

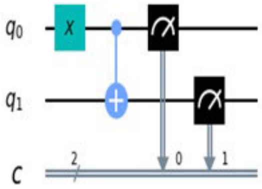


FIGURE 11. Algorithm and implementation patterns quantum cryptography.

TABLE 2. Evaluation patterns quantum analytics.

Crypto-Signal Based Approach	Quantum Based Security Integration
78	96
82	96
73	94
83	92
86	96
89	96
70	96
72	89
83	92
83	89
84	93
81	97
83	96
70	92
78	96

quantum-based security are utilizing ongoing key generation and having its record in the unique history that depends on the center advancements of quantum. Quantum Cryptography Performance Analytics is shown in Fig. 11.

The Table 3 provides a comparative analysis of the performance metrics across different application domains for the quantum cryptographic patterns discussed in our paper. The metrics include Quantum Bit Error Rate (QBER), key generation rate, computational overhead, and the estimated security level. QBER, a crucial metric, is presented as a percentage, representing the ratio of the number of qubits that are erroneously received to the total number of qubits sent during the quantum key distribution (QKD) process. Lower QBER percentages indicate a more robust and error-resistant quantum cryptographic implementation. Key generation rate is measured in kilobits per second (Kbps), providing insight into the speed at which secure keys can be generated, which is vital for real-time applications. Computational overhead, measured in milliseconds (ms), reflects the extra time required to perform cryptographic operations, impacting the overall system efficiency. Finally, the security level gives a qualitative assessment of the cryptographic strength particular to each domain. This detailed evaluation assists in highlighting the efficacy and practicality of the integrated quantum computing patterns within varied real-time cryptographic scenarios.

A. INTEGRATION OF BASE ADAPTIVE COMMUNICATION

The present chapter describes the performance comparison between existing and proposed techniques and is divided into three sections. The first describes the working of the current base adaptive communication technique, followed by another area that deals with the working of proposed genetic and quantum improved communication [56], [57]. The section focuses on the performance comparison between the existing base adaptive transmission and proposed genetic and quantum improved encoding.

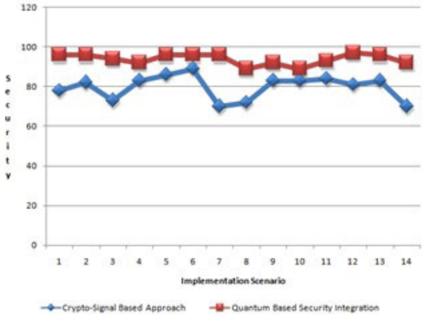


FIGURE 12. Quantum cryptography performance analytics.

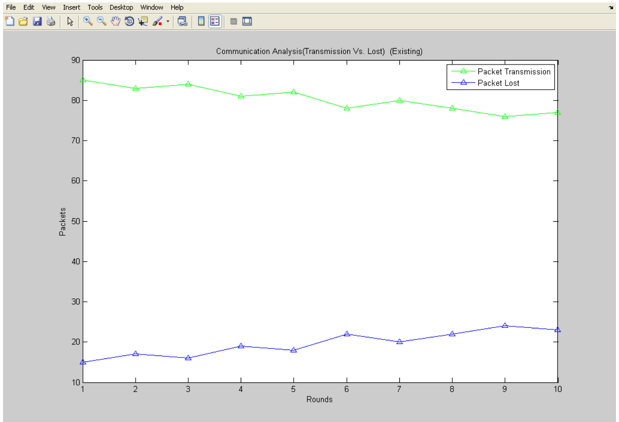


FIGURE 13. Packet communication analysis (classical approach).

The plot shows the communication analysis in the existing approach, as shown in Fig. 12. The base adaptive communication method represents the packet transmission versus packet loss.

B. INTEGRATION OF QUANTUM ENCODING FOR ELEVATION OF OUTCOMES AND PERFORMANCE

The outcomes and plot represent the communication analysis of the proposed genetic and quantum encoding communication. It shows the packet lost versus packet transmitted in the proposed approach.

C. INTEGRATION OF BASE ADAPTIVE COMMUNICATION

The present chapter describes the performance comparison between existing and proposed techniques and is divided into three sections. The first describes the working of the current base adaptive communication technique, followed by another area that deals with the working of proposed genetic and quantum improved communication [58], [59].

TABLE 3. Performance evaluation of quantum cryptographic patterns.

Domain	QBER (%)	Key Generation Rate (Kbps)	Computational Overhead (ms)	Security Level
Financial Transactions	0.8	500	12	High
Health Data Exchange	1.2	450	15	High
E-commerce	0.9	480	10	Medium
Government Data	0.7	520	20	Very High
Personal Communications	1.0	460	8	Medium

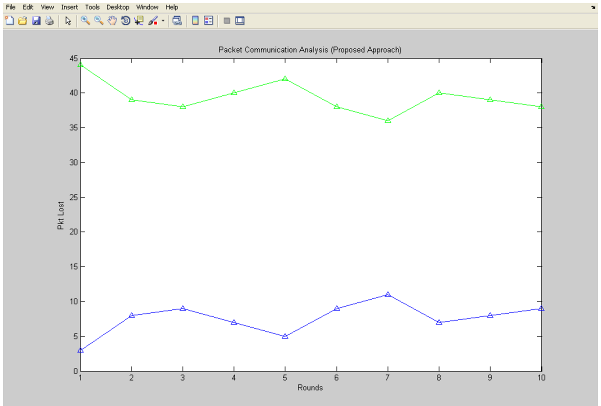

File Edit View Insert Tools Desktop Window Help
Packet Communication Analysis (Proposed Approach)
Pkt Lost
0
5
10
15
20
25
30
35
40
45
1
2
3
4
5
6
7
8
9
10
Rounds

FIGURE 14. Integration of quantum algorithm.

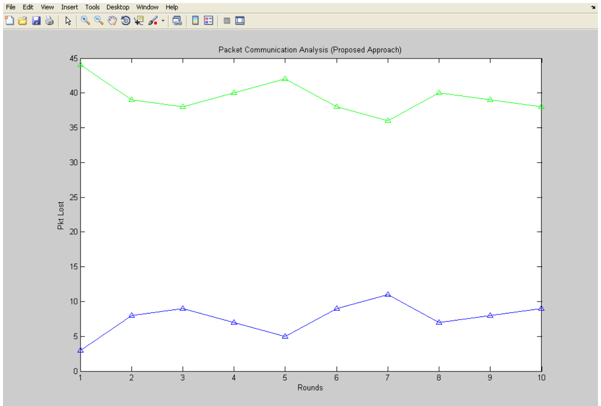

File Edit View Insert Tools Desktop Window Help
Packet Communication Analysis (Proposed Approach)
Pkt Lost
0
5
10
15
20
25
30
35
40
45
1
2
3
4
5
6
7
8
9
10
Rounds

FIGURE 15. Integration of quantum algorithm.

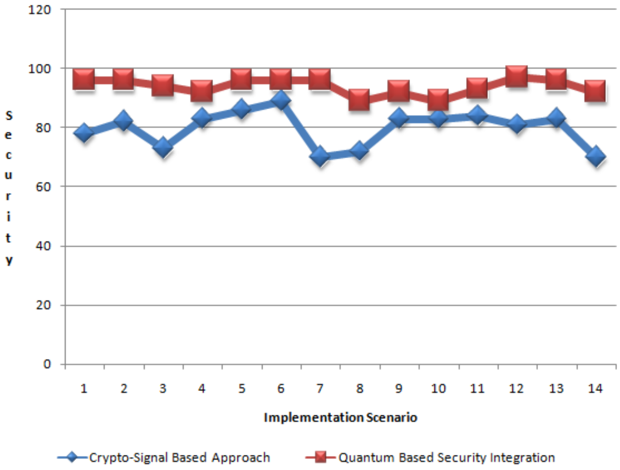


FIGURE 16. Quantum cryptography performance analytics.

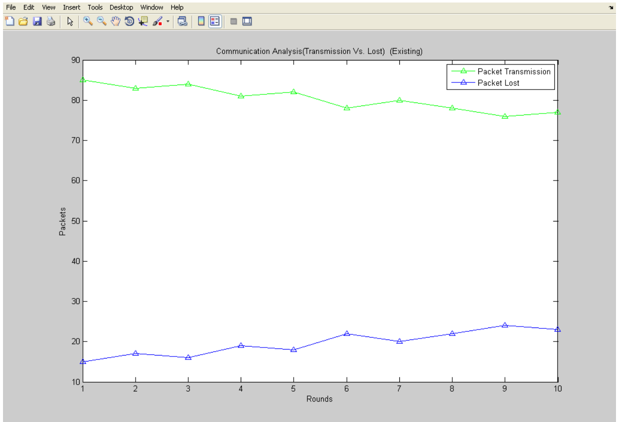

File Edit View Insert Tools Desktop Window Help
Communication Analysis(Transmission Vs. Lost) (Existing)
Packet Transmission
Packet Lost
Packets
10
20
30
40
50
60
70
80
90
1
2
3
4
5
6
7
8
9
10
Rounds

FIGURE 17. Packet communication analysis (classical approach).

The section focuses on the performance comparison between the existing base adaptive transmission and proposed genetic and quantum improved encoding.

The plot shows the communication analysis in the existing approach, as shown in Fig. 12. The base adaptive communication method represents the packet transmission versus packet loss.

D. INTEGRATION OF QUANTUM ENCODING FOR ELEVATION OF OUTCOMES AND PERFORMANCE

The outcomes and plot represent the communication analysis of the proposed genetic and quantum encoding communication. It shows the packet lost versus packet transmitted in the proposed approach.

Here the results show the relative examination in ways of packet communication. The x-axis indicates the number of rounds, and the y-axis shows the bundle correspondence. The green line addresses the amount of packet communication in the event of the proposed approach. The outcomes show that the technique has further developed packet communication over the network. The observations taken for the packet loss in case of existing and proposed work are shown here in the tabular outcomes [60]. The results represent the communication analysis between the current and proposed approaches. It shows that the overall packet transferred in the proposed is better than the existing approach, as shown in Fig. 13.

Here the figure shows the comparative investigation as far as packet loss. Here x-axis indicates the number of

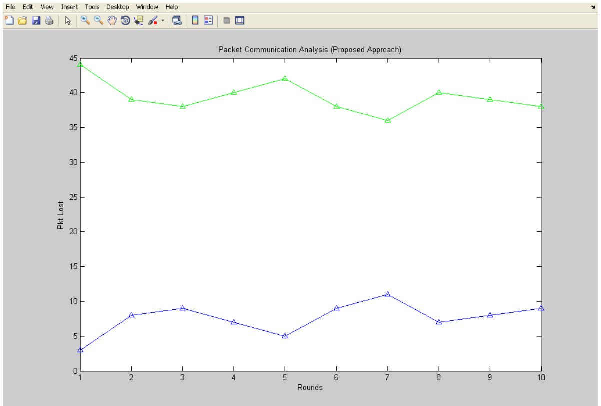


FIGURE 18. Integration of quantum algorithm.

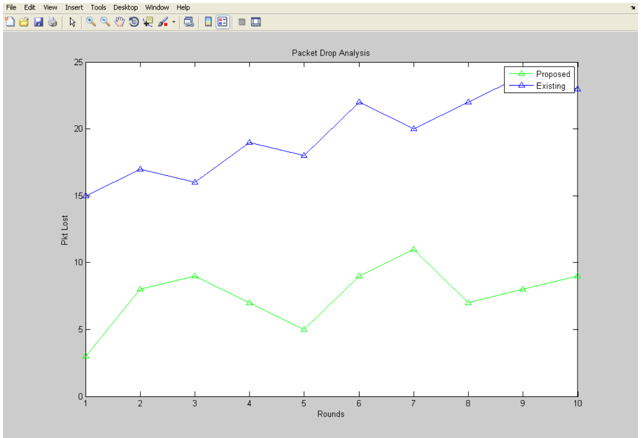


FIGURE 19. Packet loss analysis (comparative).

TABLE 4. Packet loss analysis.

No. of packets transmit	Packet Transmit/Packet Lost (In Existing)	Packet transmit/packet lost (Proposed)
34	28/6	30/4
46	35/11	40/6
60	47/13	50/10

rounds, and the y pivot offers the packet communication. The green line here addresses the amount of packet loss if the proposed approach should occur. The outcomes show that the strategy has diminished the packet loss over the organization. The perceptions assumed for the packet loss in the event of existing and proposed work are displayed in the accompanying table.

Here Table 2 shows the packet loss that occurs in existing and proposed approaches. The mobility in the network is here defined at the node level, and the nodes perform the switching between the regional coverage. The figure shows that the communication loss is continuously high in the case of the existing approach.

With the implementation of the quantum computing-based toolkits in Python, the overall security and integrity in the communication are elevated, and secured communication takes place. In constructing quantum key distribution protocols, quantum cryptography has been primarily established so far. Sadly, for many users (large networks), the need for setup and the manipulation of many pair-secret keys makes symmetrical cryptosystems with keys distributed through the quantum key distribution unaffordable (“key-management problem”). It does not solely deal with cryptographic operations and is much more important in everyday use. The secured protocols use the quantum-like approach to key distribution, which employs three stages of classical algorithms to perform its three communication phases.

E. IMPLEMENTATION HURDLES

The hurdles arises in an implementation of this technique are as follows:

- The use of encryption and blockchain technology to improve privacy and security in decentralized systems.
- Research into post-quantum cryptography methods to provide long-term security against changing risks.
- Adoption of machine learning techniques for privacy preservation that train models on sensitive data using cryptographic techniques without jeopardizing the privacy of individuals.

VII. CONCLUSION

Quantum computing is a kind of implementation that needs much verisimilitude soon for various applications of social and corporate domains. The single most exciting applications of quantum computers are the ability to model molecules for real-world applications. Many corporate segments, including Daimler and Volkswagen, use quantum computers to find innovative and improved ways of increasing the energy efficiency of electric vehicle (battery) models. They are also tested to be used for their potential in novel pharmaceuticals. The machines can quickly crunch through many possibilities because they’re made to crunch rapidly to solve optimization problems. In other words, for example, Airbus uses these as measurements of the most fuel-efficient route and altitude. Volkswagen has developed a route planning service that calculates the perfect ways for buses and taxis to minimize congestion. Many of the researchers in the field so far still expect that computers can assist in the development of artificial intelligence. Quantum computers will not likely realize their full potential for a long time. On the other hand, though, new computing networks are expected to meet their pledge, whole industries can be changed, and the entire world economy can be benefited. Quantum computing is not limited to cryptography but can be integrated for cloud applications, wireless implementations, smart cities, the Internet of Things (IoT), grid systems, and many others where a higher degree of performance and accuracy is required.

REFERENCES

[1] J. Domingo-Ferrer, S. Ricci, and J. Soria-Comas, ''A methodology to compare anonymization methods regarding their risk-utility trade-off,'' in *Modeling Decisions for Artificial Intelligence* (Lecture Notes in Computer Science). Cham, Switzerland: Springer, 2017, pp. 132–143.

[2] A. Aggarwal, S. Gaba, J. Kumar, and S. Nagpal, ''Blockchain and autonomous vehicles: Architecture, security and challenges,'' in *Proc. 5th Int. Conf. Comput. Intell. Commun. Technol. (CCICT)*, Jul. 2022, pp. 332–338.

[3] S. Gaba, S. Nagpal, and A. Aggarwal, ''A comparative study of convolutional neural networks for plant phenology recognition,'' in *Advanced Sensing in Image Processing and IoT*. Boca Raton, FL, USA: CRC Press, 2022, pp. 109–136.

[4] T. Fuhr and P. Paillier, ''Decryptable searchable encryption,'' in *Provable Security* (Lecture Notes in Computer Science). . Berlin, Germany: Springer, 2007, pp. 228–236.

[5] K.-A. Shim, ''A survey of public-key cryptographic primitives in wireless sensor networks,'' *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 577–601, 1st Quart., 2016.

[6] *Quantum Computing Developments Chart*. Accessed: May 6, 2019. [Online]. Available: https://www.statista.com/chart/17896/quantum-computing-developments/

[7] S. Gaba, S. Nagpal, A. Aggarwal, R. Kumar, and S. Kumar, ''An analysis of Internet of Things (IoT) malwares and detection based on static and dynamic techniques,'' in *Proc. 7th Int. Conf. Parallel, Distrib. Grid Comput. (PDGC)*, Nov. 2022, pp. 24–29.

[8] P. Singh, G. Bathla, D. Panwar, A. Aggarwal, and S. Gaba, ''Performance evaluation of genetic algorithm and flower pollination algorithm for scheduling tasks in cloud computing,'' in *Proc. Int. Conf. Signal Process. Integr. Netw.* Singapore: Springer, 2022, pp. 139–154.

[9] V. Srinivasan, J. Stankovic, and K. Whitehouse, ''Protecting your daily in-home activity information from a wireless snooping attack,'' in *Proc. 10th Int. Conf. Ubiquitous Comput.*, 2008, pp. 202–211.

[10] X. Gao, B. Firner, S. Sugrim, V. Kaiser-Pendergrast, Y. Yang, and J. Lindqvist, ''Elastic pathing: Your speed is enough to track you,'' in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, Sep. 2014, pp. 975–986.

[11] *Quantum computing developments*. [Online]. Available: https://www2.itif.org/2018-tech-explainer-quantum-computing.pdf

[12] *Future With Quantum Computers*. [Online]. Available: https://www.c-sharpcorner.com/article/future-with-quantum-computers/

[13] (2021). *IBM Promises 100x Faster Quantum Computing*. [Online]. Available: https://www.extremetech.com/computing/319759-ibm-promises-100x-faster-quantum-computing-in-2021

[14] *Creating the Heart of a Quantum Computer: Developing Qubits*. [Online]. Available: https://www.energy.gov/science/articles/creating-heart-quantum-computer-developing-qubits

[15] S. Gaba, S. Nagpal, A. Aggarwal, S. Kumar, and P. Singh, ''A modified approach for accuracy enhancement in intruder detection with optimally certain features,'' in *Mobile Radio Communications and 5G Networks*. Springer, 2023, pp. 149–157.

[16] S. Gaba, I. Buddhiraja, V. Kumar, and A. Makkar, ''Federated learning based secured computational offloading in cyber-physical IoST systems,'' in *Proc. Int. Conf. Recent Trends Image Process. Pattern Recognit.* Switzerland: Springer, 2022, pp. 344–355.

[17] S. Gaba, D. Kumar, S. Nagpal, and A. Aggarwal, ''A quick analysis on cyber physical systems for sustainable development,'' *Grenze Int. J. Eng. Technol. (GIJET)*, vol. 8, no. 1, pp. 621–627, 2022.

[18] P. Consul, I. Budhiraja, D. Garg, and A. Bindle, ''Power allocation scheme based on DRL for CF massive MIMO network with UAV,'' in *Innovations in Information and Communication Technologies*. Singapore: Springer, 2022, pp. 33–43.

[19] A. Aggarwal, S. Gaba, S. Chawla, and A. Arya, ''Recognition of alphanumeric patterns using backpropagation algorithm for design and implementation with ANN,'' *Int. J. Secur. Privacy Pervasive Comput.*, vol. 14, no. 1, pp. 1–11, Feb. 2022.

[20] H. Sharma, I. Budhiraja, P. Consul, N. Kumar, D. Garg, L. Zhao, and L. Liu, ''Federated learning based energy efficient scheme for MEC with NOMA underlaying UAV,'' in *Proc. 5th Int. ACM Mobicom Workshop Drone Assist. Wireless Commun. 5G Beyond*, Oct. 2022, pp. 73–78.

[21] S. Gaba, A. Aggarwal, and S. Nagpal, ''Role of machine learning for ad hoc networks,'' in *Cloud and IoT-Based Vehicular Ad Hoc Networks*, 2021, pp. 269–291.

[22] A. Aggarwal, S. Gaba, S. Nagpal, and B. Vig, ''Bio-inspired routing in VANET,'' in *Cloud and IoT-Based Vehicular Ad Hoc Networks*, 2021, pp. 199–220.

[23] A. Aggarwal, S. Gaba, S. Nagpal, and A. Arya, ''A comparative analysis among task scheduling for grouped and ungrouped grid application,'' in *Proc. NITTTR*, 2021, pp. 1–5.

[24] I. Budhiraja, D. Garg, N. Kumar, and R. Sharma, ''A comprehensive review on variants of SARS-CoVs-2: Challenges, solutions and open issues,'' *Comput. Commun.*, vol. 197, pp. 34–51, Jan. 2023.

[25] N. Joshi, I. Budhiraja, D. Garg, S. Garg, B. J. Choi, and M. Alrashoud, ''Deep reinforcement learning based rate enhancement scheme for RIS assisted mobile users underlaying UAV,'' *Alexandria Eng. J.*, vol. 91, pp. 1–11, Mar. 2024.

[26] I. Budhiraja, D. Garg, R. Singh, S. Garg, B. J. Choi, and M. Alrashoud, ''SWIPT and uplink NOMA approach for self energy recycling in full-duplex enabled D2D network,'' *Alexandria Eng. J.*, vol. 90, pp. 208–215, Mar. 2024.

[27] L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, and S. Ricci, ''A privacy-enhancing framework for Internet of Things services,'' in *Proc. Int. Conf. Netw. Syst. Secur.*, 2019, pp. 77–97.

[28] A. Verma, P. Bhattacharya, I. Budhiraja, A. K. Gupta, and S. Tanwar, ''Fusion of federated learning and 6G in Internet-of-Medical-Things: Architecture, case study and emerging directions,'' in *Futuristic Trends in Networks and Computing Technologies*. Singapore: Springer, 2022, pp. 229–242.

[29] M. A. Mustafa, S. Cleemput, A. Aly, and A. Abidin, ''A secure and privacy-preserving protocol for smart metering operational data collection,'' *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6481–6490, Nov. 2019.

[30] A. Sharma, S. Gaba, S. Singla, S. Kumar, C. Saxena, and R. Srivastava, ''A genetic improved quantum cryptography model to optimize network communication,'' in *Proc. ICRTCIS*, 2019, pp. 47–54.

[31] P. Consul, I. Budhiraja, R. Chaudhary, and N. Kumar, ''Security reassessing in UAV-assisted cyber-physical systems based on federated learning,'' in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2022, pp. 61–65.

[32] K. S. Roy and H. K. Kalita, ''A survey on post-quantum cryptography for constrained devices,'' *Int. J. Appl. Eng. Res.*, vol. 14, no. 11, pp. 2608–2615, 2019.

[33] A. Barnawi, I. Budhiraja, K. Kumar, N. Kumar, B. Alzahrani, A. Almansour, and A. Noor, ''A comprehensive review on landmine detection using deep learning techniques in 5G environment: Open issues and challenges,'' *Neural Comput. Appl.*, vol. 34, no. 24, pp. 21657–21676, Dec. 2022.

[34] S. Nagpal, A. Aggarwal, and S. Gaba, ''Privacy and security issues in vehicular ad hoc networks with preventive mechanisms,'' in *Proc. Int. Conf. Intell. Cyber-Phys. Syst.*, 2021, pp. 317–329.

[35] S. Gaba, A. Aggarwal, S. Nagpal, D. Kumar, and P. Singh, ''A forecast of coronary heart disease using proficient machine learning algorithms,'' in *Proc. 6th Int. Conf. Image Inf. Process.*, 2021, pp. 517–522.

[36] P. Consul, I. Budhiraja, R. Chaudhary, and D. Garg, ''FLBCPS: Federated learning based secured computation offloading in blockchain-assisted cyber-physical systems,'' in *Proc. IEEE/ACM 15th Int. Conf. Utility Cloud Comput. (UCC)*, Dec. 2022, pp. 412–417.

[37] R. Nijhawan, M. Juneja, N. Kaur, A. Yadav, and I. Budhiraja, ''Automated deep learning based approach for albinism detection,'' in *Proc. Int. Conf. Recent Trends Image Process. Pattern Recognit.* Switzerland: Springer, 2022, pp. 272–281.

[38] J. Hajny, P. Dzurenda, and L. Malina, ''Attribute-based credentials with cryptographic collusion prevention,'' *Secur. Commun. Netw.*, vol. 8, no. 18, pp. 3836–3846, Dec. 2015.

[39] H. Khan, I. Budhiraja, S. A. Wahaj, M. Z. Alam, S. T. Siddiqui, and M. I. Alam, ''IoT and blockchain integration challenges,'' in *Proc. IEEE Int. Conf. Current Develop. Eng. Technol. (CCET)*, Dec. 2022, pp. 1–5.

[40] P. Rani, V. Kumar, I. Budhiraja, A. Rathi, and S. Kukreja, ''Deploying electronic voting system use-case on Ethereum public blockchain,'' in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2022, pp. 1–6.

[41] A. Ben-David, N. Nisan, and B. Pinkas, ''FairplayMP: A system for secure multi-party computation,'' in *Proc. 15th ACM Conf. Comput. Commun. Secur.*, 2008, pp. 257–266.

[42] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, ''Smart grid metering networks: A survey on security, privacy and open research issues,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2886–2927, 3rd Quart., 2019.

[43] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 7, pp. 1735–1744, Jul. 2014.

[44] A. Yadav, S. Gaba, H. Khan, I. Budhiraja, A. Singh, and K. K. Singh, "ETMA: Efficient transformer-based multilevel attention framework for multimodal fake news detection," *IEEE Trans. Computat. Social Syst.*, early access, Mar. 20, 2023, doi: 10.1109/TCSS.2023.3255242.

[45] S. Gaba, I. Budhiraja, V. Kumar, S. Garg, G. Kaddoum, and M. M. Hassan, "A federated calibration scheme for convolutional neural networks: Models, applications and challenges," *Comput. Commun.*, vol. 192, pp. 144–162, Aug. 2022.

[46] S. Gaba, I. Budhiraja, A. Makkar, and D. Garg, "Machine learning for detecting security attacks on blockchain using software defined networking," in *Proc. IEEE Int. Conf. Commun. Workshops*, May 2022, pp. 260–264.

[47] S. Singh, A. Bhardwaj, I. Budhiraja, U. Gupta, and I. Gupta, "Cloud-based architecture for effective surveillance and diagnosis of COVID-19," in *Convergence of Cloud With AI for Big Data Analytics: Foundations and Innovation*. Hoboken, NJ, USA: Wiley, 2023, pp. 69–88

[48] A. Bhardwaj, U. Gupta, I. Budhiraja, and R. Chaudhary, "Container-based migration technique for fog computing architecture," in *Proc. Int. Conf. Advancement Technol. (ICONAT)*, Jan. 2023, pp. 1–6.

[49] M. Singh, G. S. Aujla, A. Singh, N. Kumar, and S. Garg, "Deep-learning-based blockchain framework for secure software-defined industrial networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 606–616, Jan. 2021.

[50] U. Demirbaga and G. S. Aujla, "RootPath: Root cause and critical path analysis to ensure sustainable and resilient consumer-centric big data processing under fault scenarios," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1493–1500, Feb. 2024.

[51] A. Aggarwal, S. Gaba, and M. Mittal, "A comparative investigation of consensus algorithms in collaboration with IoT and blockchain," in *Transforming Cybersecurity Solutions Using Blockchain*. Singapore: Springer, 2021, pp. 115–140.

[52] B. A. Taha, A. J. Addie, A. J. Haider, V. Chaudhary, R. Apsari, A. Kaushik, and N. Arsad, "Exploring trends and opportunities in quantum-enhanced advanced photonic illumination technologies," *Adv. Quantum Technol.*, vol. 7, no. 3, Mar. 2024, Art. no. 2300414.

[53] D. Shin, "Modern quantum information and the impact of quantum computing on cryptography," *Bull. Amer. Phys. Soc.*, Mar. 2024.

[54] S. Cherbal, A. Zier, S. Hebal, L. Louail, and B. Annane, "Security in Internet of Things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing," *J. Supercomput.*, vol. 80, no. 3, pp. 3738–3816, Feb. 2024.

[55] A. M. Aslam, R. Chaudhary, A. Bhardwaj, I. Budhiraja, N. Kumar, and S. Zeadally, "Metaverse for 6G and beyond: The next revolution and deployment challenges," *IEEE Internet Things Mag.*, vol. 6, no. 1, pp. 32–39, Mar. 2023.

[56] V. Vishnoi, P. Consul, I. Budhiraja, S. Gupta, and N. Kumar, "Deep reinforcement learning based energy consumption minimization for intelligent reflecting surfaces assisted D2D users underlaying UAV network," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, May 2023, pp. 1–6.

[57] V. Vishnoi, I. Budhiraja, S. Gupta, and N. Kumar, "A deep reinforcement learning scheme for sum rate and fairness maximization among D2D pairs underlaying cellular network with NOMA," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13506–13522, Oct. 2023.

[58] A. Barnawi, S. Gaba, A. Alphy, A. Jabbari, I. Budhiraja, V. Kumar, and N. Kumar, "A systematic analysis of deep learning methods and potential attacks in Internet-of-Things surfaces," *Neural Comput. Appl.*, vol. 35, no. 25, pp. 18293–18308, Sep. 2023.

[59] H. Sharma, N. Kumar, I. Budhiraja, and A. Barnawi, "Secrecy rate maximization in THz-aided heterogeneous networks: A deep reinforcement learning approach," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13490–13505, Oct. 2023.

[60] S. Gaba, H. Khan, K. J. Almalki, A. Jabbari, I. Budhiraja, V. Kumar, A. Singh, K. K. Singh, S. S. Askar, and M. Abouhawwash, "Holochain: An agent-centric distributed hash table security in smart IoT applications," *IEEE Access*, vol. 11, pp. 81205–81223, 2023.

SHALLY NAGPAL received the Ph.D. degree in computer science engineering from the Maharishi Markandeshwar Engineering College. She is currently an Assistant Professor with the Emerging Department, Panipat Institute of Engineering and Technology, Panipat, Haryana, India. She teaches with the Department of Computer Science and Engineering. She has presented and published abundant papers and chapters in national/international conferences and journals. Her research interests include big data, cloud computing, machine learning, AI, and cyber attacks. She has organized and attended numerous of workshops, FDPs, and conferences on national/international platforms.

SHIVANI GABA received the B.Tech. and M.Tech. degrees from Kurukshetra University, in 2015 and 2017, respectively. She is currently a Research Scholar with the School of Computer Science and Engineering, Bennett University, Greater Noida, and also an Assistant Professor with Panipat Institute of Engineering and Technology, Panipat, Haryana. She is an Educator, a Researcher, and a Philanthropist. She is a Microsoft Technology Associate (MTA) and a Microsoft Office Specialist (MOS) Certified. She has presented and published abundant papers and chapters in national/international conferences and journals. Her research interests include AI, blockchain, deep learning, and cyber attacks.

ISHAN BUDHIRAJA received the B.Tech. degree in electronics and communication engineering from Uttar Pradesh Technical University, Lucknow, India, in 2008, the M.Tech. degree in electronics and communication engineering from Maharshi Dayanand University, Rohtak, Haryana, in 2012, and the Ph.D. degree in computer science engineering from the Thapar Institute of Engineering and Technology, Patiala, India, in 2021. Some of his research findings are published in top-cited journals, such as IEEE Transactions on Industrial Informatics, IEEE Transactions on Vehicular Technology, IEEE Transactions on Mobile Computing, IEEE Internet of Things Journal, *IEEE Wireless Communications Magazine*, and IEEE Systems Journal, and various international top-tiered conferences, such as IEEE GLOBECOM, IEEE ICC, IEEE WCMC, ACM, and IEEE Infocom. He was a Research Associate on the project Energy Management of Smart Home using cloud infrastructure-a utility perspective, funded by CSIR, New Delhi, India. His research interests include device-to-device communications, the Internet of Things, non-orthogonal multiple access, femtocells, deep reinforcement learning, and microstrip patch antenna.

MEENAKSHI SHARMA received the B.E. degree from Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, in 1996, and the M.Tech. degree in communication systems and the Ph.D. degree in microwave engineering. She is currently a Professor and the Head of the Department of Electronics and Communication Engineering, Inderprastha Engineering College, Ghaziabad. Besides this, she is the Dean Student, a Welfare, and the Coordinator of Internal Quality Assurance Cell, IPEC. She has more than 26 years of teaching and one year of industrial experience to her credit. She is the Founder Faculty of IPEC and has been working with IPEC since past 23 years in various capacities. She has published a good number of research articles with journals of repute, including SCI publications. She has authored a book titled "*Electronics Engineering Made Easy*" with Cengage Learning (formerly Thomson Press) under technological university series. She has one granted patent and six published patents to her credit. She has been a resource person for various workshops and faculty development programs. She has also convened numerous national level conferences and seminars. Her research interests include microwave filter, antenna design, the IoT, and digital circuit design. She is a Life Member of IETE, New Delhi. She has chaired many international and national conferences.

AKANSHA SINGH received the B.Tech., M.Tech., and Ph.D. degrees in computer science, and the Ph.D. degree in image processing and machine learning from IIT Roorkee. She is currently a Professor with the School of Computer Science and Engineering, Bennett University, Greater Noida, India. She has also undertaken government funded project as the Principal Investigator. Her research interests include image processing, remote sensing, the IoT, and machine learning. She served as an associate editor and the guest editor for several journals.

KRISHNA KANT SINGH received the B.Tech., M.Tech., M.S., and Ph.D. degrees in image processing and machine learning from IIT Roorkee. He is currently the Director of Delhi Technical Campus, Greater Noida, India, bringing a wealth of teaching and research experience to his role. His scholarly output is remarkable, having authored over 140 research articles in esteemed Scopus and SCIE indexed journals, along with 25 technical books, showcasing his profound impact on the field. He is an Associate Editor of IEEE Access and many other journals of high repute. He also served as the Guest Editor for *Open Computer Science*, *Wireless Personal Communications*, *Complex and Intelligent Systems*, and many other journals. Additionally, his involvement in the Editorial Board of *Applied Computing and Geosciences* (Elsevier) highlights his significant contributions to academia and research.

S. S. AKSAR received the B.Sc. degree in mathematics and the M.Sc. degree in applied mathematics from Mansoura University, Egypt, in 1998 and 2004, respectively, and the Ph.D. degree in operation research from Cranfield University, U.K., in 2011. He has been an Associate Professor with Mansoura University, since 2016. He joined King Saud University, in 2012, where he is currently with the Department of Statistics and Operation Research, as a Professor. His research interests include game theory and its applications that include mathematical economy, dynamical systems, and network analysis.

MOHAMED ABOUHAWWASH received the B.Sc. and M.Sc. degrees in statistics and computer science from Mansoura University, Mansoura, Egypt, in 2005 and 2011, respectively, and the joint Ph.D. degree in statistics and computer science from Michigan State University, East Lansing, MI, USA, and Mansoura University, in 2015. In 2018, he was a Visiting Scholar with the Department of Mathematics and Statistics, Faculty of Science, Thompson Rivers University, Kamloops, BC, Canada. He is currently with Michigan State University. He is also an Associate Professor with the Department of Mathematics, Faculty of Science, Mansoura University. His current research interests include evolutionary algorithms, machine learning, image reconstruction, and mathematical optimization. He was a recipient of the best master's and Ph.D. thesis awards from Mansoura University in 2012 and 2018, respectively.

CELESTINE IWENDI (Senior Member, IEEE) received the Ph.D. degree in electronics engineering. A highly motivated Researcher and a Teacher with emphasis on communication, hands-on experience, and willing-to-learn, and a 23 years technical expertise. He has developed operational, maintenance, and testing procedures for electronic products, components, equipment, and systems; provided technical support and instruction to staff and customers regarding equipment standards, assisting with specific, and difficult in-service engineering; inspected electronic and communication equipment, instruments, products, and systems to ensure conformance to specifications, safety standards, and regulations. He is currently a Wireless Sensor Network Chief Evangelist, AI, ML, and the IoT Expert, and a Designer. He is a Reader (Professor) with the University of Bolton, U.K. He is a Visiting Professor with five universities. He is also the IEEE University of Bolton, the Student Branch Counselor, and the former Board Member of IEEE Sweden Section; and a fellow of The Higher Education Academy, U.K., and the Institute of Management Consultants to add to his teaching, managerial and professional experiences. He is an Ambassador in the prestigious Manchester Conference Ambassador Program and an IEEE Humanitarian Philanthropist. He received the prestigious recognition of the Royal Academy of Engineering through the Exceptional Talent Scheme, acknowledging his substantial contributions to artificial intelligence and its medical applications. Additionally, he takes pride in his three-year inclusion in Elsevier's publication, featuring the World's Top 2% Influential Scientists. He is an IEEE Brand Ambassador. He was a past ACM Distinguished Speaker, a Seasoned Lecturer, and a Chartered Engineer.