IEEE Open Journal of the
Computer Society

Received 26 March 2024; accepted 2 May 2024. Date of publication 7 May 2024;
date of current version 20 May 2024. The review of this article was arranged by Associate Editor Z. Zheng.

Digital Object Identifier 10.1109/OJCS.2024.3397307

Generic Quantum Blockchain-Envisioned Security Framework for IoT Environment: Architecture, Security Benefits and Future Research

MOHAMMAD WAZID [1] (Senior Member, IEEE), ASHOK KUMAR DAS [2,3] (Senior Member, IEEE), AND YOUNGHO PARK [4] (Member, IEEE)

(Survey Paper)

[1]Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248002, India
[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India
[3]Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA 23435 USA
[4]School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea

CORRESPONDING AUTHORS: MOHAMMAD WAZID AND YOUNGHO PARK (e-mail: wazidkec2005@gmail.com; parkyh@knu.ac.kr).

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1I1A3058605.

ABSTRACT Quantum cryptography has the potential to secure the infrastructures that are vulnerable to various attacks, like classical attacks, including quantum-related attacks. Therefore, quantum cryptography seems to be a promising technology for the future secure online infrastructures and applications, like blockchain-based frameworks. In this article, we propose a generic quantum blockchain-envisioned security framework for an Internet of Things (IoT) environment. We then discuss some potential applications of the proposed framework. We also highlight the security advantages of quantum cryptography-based systems. We explain the working of blockchain, applications of blockchain, types of blockchain, the structure of blockchain, the structure of blockchain in a classical blockchain, and the structure of a block in a quantum blockchain context. Next, the adverse effects of quantum computing on the security of blockchain-based frameworks are highlighted. Furthermore, the comparisons of quantum cryptography-based security schemes, like quantum key distribution, quantum digital signature, and quantum hashing schemes, are provided. Finally, some future research directions related to the designed generic quantum blockchain-envisioned security framework for IoT are provided.

INDEX TERMS Quantum cryptography, quantum blockchain, Internet of Things, quantum key distribution, quantum digital signature, quantum hashing, security.

I. INTRODUCTION

Quantum computing is an interdisciplinary field that combines computer science, physics, and mathematics to tackle difficult problems more quickly than classical computers can. Quantum computing encompasses both the study of hardware and the creation of software. By taking advantage of quantum mechanical features like superposition and quantum interference, quantum computers are able to solve certain types of problems much more quickly than classical computers [1].

Blockchain is a type of shared database that keeps information in a different way than a traditional database does; rather than storing information in tables, blockchains store data in blocks that are cryptographically linked together with their hash values. In short, a distributed database or ledger that is shared among the nodes of a computer network is referred to as a blockchain [2]. A blockchain is capable of storing a variety of information, but the ledger function has proven to be its most useful application for handling transactions, i.e., Bitcoin.

Blockchain is decentralized, which means that no one person or group has authority over it; rather, the whole user base retains power collectively [3]. The data that is entered into a decentralized blockchain cannot be altered, which means that it cannot be deleted. When using Bitcoin, all transactions are permanently recorded and may be viewed by any interested party [4].

Cryptography is a way to turn the original data (i.e., plaintext) into some scrambled information, which is called the encrypted message or ciphertext. Due to such transformation of data, a user with the proper key (i.e., secret key) is only able to decrypt the message [5]. By extension, quantum cryptography is another way of encrypting the information. It transmits the data in a secure way with the help of principles of quantum mechanics [1]. The principles of quantum mechanics that underlie quantum cryptography are what makes it challenging. These include the following:

i) The constituent parts of the universe, known as particles, are intrinsically ambiguous and can coexist in a number of different locations or states at the same time.
ii) Photons are capable of randomly manifesting themselves in two distinct quantum states.
iii) It is not possible to measure a quantum attribute without causing some kind of change or disturbance.
iv) Although it is possible to clone some quantum features of a particle, this is not yet possible for the entire particle.
v) The operation of quantum cryptography is influenced in some way by each of these propositions.

The concept of quantum blockchain can be conceptualized as a decentralized, encrypted, and dispersed database that is underpinned by quantum computation and the notion of quantum information [6]. After being added to the quantum blockchain, the information cannot be changed in an unauthorized manner after that point. It is secured against quantum attacks as well as classical attacks [7], [8].

The concept of the Internet of Things (IoT) refers to a network of tangible entities, commonly referred to as “things,” which are equipped with sensors, software, and other tools and technological components. These elements enable the items to establish connections and facilitate the exchange of data with other devices and systems over the Internet [9]. These gadgets, also referred to as smart objects, encompass a wide range of technologies, including but not limited to smart home equipment such as smart AC controllers, wearables like smartwatches, and RFID-enabled apparel, as well as more intricate industrial machinery and transportation systems. The IoT is utilized in several sectors, including smart residences that facilitate the remote management of gadgets and health monitoring, as well as industrial IoT, which enhances machinery maintenance and supply chain optimization [10], [11]. The IoT plays a significant role in the healthcare sector by facilitating remote patient monitoring and enhancing medication adherence. Similarly, in the context of smart cities, IoT technology contributes to effective traffic management and enables comprehensive environmental monitoring. Within the realm of agriculture, the IoT plays a vital role in enabling precision farming techniques and facilitating the tracking of livestock. Similarly, in the retail sector, IoT technology accelerates inventory management processes and enhances the overall customer experience [12]. The IoT has shown to be advantageous for the energy sector through the implementation of smart grid technology. Additionally, the transportation industry has experienced a significant transformation due to the integration of fleet management systems and the emergence of autonomous cars. Moreover, the IoT assumes a pivotal function in the realm of environmental monitoring, weather forecasting, and animal tracking, thereby making significant contributions to the field of disaster management. Simultaneously, wearables and personal devices such as fitness trackers and smart clothes provide individuals with individualized data and enhanced convenience. These applications exemplify the extensive influence of the IoT on contemporary culture and the business sector [9], [13].

A. *POST-QUANTUM* VERSUS *QUANTUM BLOCKCHAINS*

1) POST-QUANTUM BLOCKCHAIN

Lattice-based post-quantum cryptography plays a crucial role in preparing blockchain technology for the quantum computing age due to its efficiency and straightforward implementation [14]. Alongside, hash-based signatures have gained traction for their simplicity, such as the use of hash trees, and enhanced security features. However, research also delves into code-based, multi-variate, and isogeny-based cryptographic methods, recognizing that the balance between security levels and key sizes may vary across different applications. Furthermore, there has been a notable surge in research focused on leveraging post-quantum cryptography to enhance privacy, leading to significant advancements in post-quantum zero-knowledge proofs (ZKPs). Although the widespread application of post-quantum cryptography remains in its nascent stages, there is a growing interest among researchers to identify the quantum-resistance needs of decentralized applications and to develop post-quantum blockchain frameworks for IoT and other relevant use cases.

2) QUANTUM BLOCKCHAIN

Quantum cryptography plays a pivotal role in enhancing the security and privacy of blockchain systems through the unique capabilities of quantum mechanics. Key techniques in quantum cryptography, such as Quantum Key Distribution (QKD), quantum signatures, quantum teleportation, and quantum bit commitment, are integral to quantum blockchains. QKD, in particular, serves as the essential foundation for key exchange and authentication within these systems.

The design of quantum blockchains can follow two main approaches: integrating quantum and classical systems to create hybrid quantum-classical blockchains, and developing entirely quantum-based systems, known as fully quantum blockchains. While fully quantum blockchains promise unmatched security against all currently known Cyber threats, their practical deployment is hindered by the current scarcity of quantum computing resources.

3) COMPARISON BETWEEN POST-QUANTUM AND QUANTUM BLOCKCHAINS

Post-quantum blockchains incorporate cryptographic algorithms into classical blockchain technology to safeguard against potential quantum attacks. These systems maintain compatibility with current blockchain infrastructure and are relatively easier to implement and adopt, preserving existing performance levels. However, they do not fully harness the potential of quantum technologies, and their security relies on unproven cryptographic algorithms since post-quantum cryptography's effectiveness remains theoretical.

Hybrid quantum blockchains (HQBCs) blend classical blockchain technology with aspects of quantum cryptography, offering enhanced security and performance. These systems employ a combination of classical and quantum algorithms, enabling the gradual integration of quantum technologies for more manageable adoption. Although hybrid quantum blockchains provide a higher level of security compared to purely classical blockchains, their implementation can be complex due to the integration of both classical and quantum technologies, and they may introduce new attack vectors and vulnerabilities. HQBCs primarily rely on QKD, making them more practical than fully quantum blockchains but less efficient than post-quantum blockchains.

B. RESEARCH MOTIVATION

The research motivation of the presented work is given below.

The operations and mechanisms of quantum blockchain are based on quantum cryptography. Quantum blockchain has the potential to secure infrastructures. Therefore, it turns out to be a promising primitive for the future secure online infrastructures and applications (i.e., quantum blockchain-envisioned security framework for IoT communications). Therefore, in this survey article, we aim to focus on the security of blockchain-based frameworks, for example, how the current blockchain-based frameworks are vulnerable and how to make them secure with the inclusion of different techniques of quantum cryptography (i.e., quantum key distribution, quantum digital signature, quantum hashing, etc.) [15].

C. RESEARCH CONTRIBUTIONS

The research contributions of the article are given below.

- We discuss conventional cryptography and its security issues. Then, we discuss the security advantages of quantum cryptography-based systems.
- We propose a generic quantum blockchain-envisioned security framework for the IoT environment. In the proposed framework, we have followed the guidelines of the security framework for the IoT environment, along with the principles of the quantum blockchain.
- Some of the important applications of the proposed framework are also discussed.
- We present a review of some of the current real-world applications of quantum cryptography. These applications include quantum key distribution, mistrustful quantum cryptography, quantum commitment, position-based quantum cryptography, and measurement-device-independent (MDI) quantum cryptography.
- The value of blockchain technology and how blockchain technology operates, applications of blockchain technology, types of blockchain technology, the structure of blockchain technology, the structure of blockchain technology in classical blockchain technology, and the structure of a block in quantum blockchain technology are then discussed. In addition, the negative implications that quantum computing could have on the safety of blockchain-based frameworks have been brought to light.
- Next, a comparison of the current era and the quantum computing era is given. Furthermore, a detailed comparative study on quantum cryptography-based security schemes (i.e., quantum key distribution schemes, quantum digital signature schemes, and quantum hashing schemes) is provided.
- Finally, some prominent future research directions related to the developed generic quantum blockchain-envisioned security framework for IoT are highlighted.

D. ARTICLE ORGANIZATION

The remaining parts of the article are structured as described below. Section II explains quantum cryptography in further detail. In Section III, additional information regarding blockchain technology is presented. In Section V, we give the specifics of a generic quantum blockchain that is envisioned as a security framework for the IoT environment, along with its applications. In Section VI, the potentially detrimental implications of quantum computing on the safety of blockchain-based frameworks are dissected and analyzed. The evaluation of the various quantum security protocols may be found in Section VII. In addition, the particulars of the valuable experience are described in Section VIII. In the final section of the study, which is Section IX, some concluding remarks and recommendations for future research are included.

In this section, we discussed quantum computing, blockchain, quantum cryptography, quantum blockchain, IoT, applications of IoT, research motivation of the presented work, research contributions, and structure of the article. A summary of each section is given in Table 1.

II. QUANTUM CRYPTOGRAPHY

Quantum cryptography, quantum key distribution (QKD), the security of quantum key distribution (QKD), and several applications of quantum cryptography in the real world are covered in this portion of the article. Quantum cryptography is increasingly becoming more significantly relevant to our day-to-day lives as it can safeguard sensitive information in a manner that existing encryption techniques cannot. This is due to the fact that it can protect sensitive information in a

TABLE 1. Summary of Each Section of the Article

Section	Summary
Section I: Introduction	We discuss quantum computing, blockchain, quantum cryptography, quantum blockchain, IoT, applications of IoT, research motivation of the presented work, research contributions, and structure of the paper.
Section II: Quantum Cryptography	We discuss the usefulness of quantum cryptography, the procedure in quantum key distribution (QKD), the security of QKD, and current real-world applications of quantum cryptography.
Section III: Blockchain Technology	We discuss the usefulness of blockchain, working of blockchain, applications of blockchain, types of blockchain, structure of a blockchain, structure of a block in a blockchain, and structure of a block in the quantum blockchain.
Section V: Generic Quantum Blockchain-Envisioned Security Framework for IoT Environment	We provide the architecture of a generic quantum blockchain-envisioned security framework for the IoT environment. Further, we discuss how a generic quantum blockchain-envisioned security framework for the IoT environment is better than the traditional framework. A closely related threat model for the proposed framework is also provided.
Section VI: Adverse Effects of Quantum Computing on Blockchain-Based Frameworks and Evolution of Quantum Cryptography	The adverse effects of quantum computing on blockchain-based frameworks and the evolution of quantum cryptography are discussed. A comparison of the current era and quantum computing's era is given.
Section VII: Comparisons of Quantum Cryptography-Based Security Schemes	We provide the comparisons of various quantum cryptography-based security schemes, i.e., quantum key distribution mechanisms, quantum hashing algorithms, and quantum digital signature mechanisms. During comparisons, we consider various important features, like the overview of the scheme, the security problem that it solves, and its usability.
Section VIII: Lesson Learned	We provide information about the various lessons that we have learned in this study. We also provide information about the quantum security schemes, i.e., which scheme is more secure and provides more functionality features.
Section IX: Conclusion and Future Research Directions	We conclude the paper with some concluding remarks and some future research directions of the domain.

manner that is more secure. The following section delves into the practical applications of quantum cryptography [16].

A. USEFULNESS OF QUANTUM CRYPTOGRAPHY

When you make purchases online, you place a great deal of trust in financial institutions and other types of businesses to maintain the confidentiality of your credit card and other personal information. What would happen if companies of this nature were unable to protect the confidentiality of your personal information using the encryption methods that are currently available? Even while hackers are always trying to get access to encrypted data, as soon as quantum computers become operational, that data will be significantly more susceptible to being hacked. In the case of quantum cryptography, this is not going to be achievable because your data won't be susceptible to hacking [1], [15].

The term "post-quantum cryptography" refers to cryptographic methods that are thought to be secure against attacks made using classical computers as well as attacks made using quantum computers. The resolution of extremely challenging mathematical equations, such as integer factorization and the elliptic curve discrete logarithm problem (ECDLP), can take normal computers a number of months, or even years, to accomplish. Complex mathematical problems (for example, number theoretic computational problems: Discrete Logarithm Problem (DLP), Integer Factorization problem (IFP), etc.) are vulnerable to be cracked by quantum computers by executing the Shor's algorithm [17]. Post-quantum cryptography plays an important role in securing the systems in a better way. One of the ways to achieve this goal is the use of the lattice-based cryptography (LBC). Recently, LBC has been applied in Internet of Things (IoT) and Internet of Drones (IoD) applcations [18], [19], [20], [21].

Quantum cryptography, on the other hand, exploits the rules of quantum mechanics to transmit secure messages and, in contrast to mathematical encryption, is genuinely unbreakable. It does this by utilizing the laws of quantum mechanics. In contrast to mathematical encryption, quantum cryptography applies the principles of quantum physics to the process of encrypting data in order to make it nearly impossible to decipher [7], [16], [22].

A series of photons, which are individual particles of light, are used in the process of sending data from one point to another across a medium, such as a fiber optic cable, in the field of quantum cryptography. One of the common protocols that is based on quantum cryptography is known as quantum key distribution (QKD). By comparing measurements of a subset of the properties possessed by these photons, the two parties involved in the communication are able to generate a key that enables them to communicate safely with one another. The QKD procedure is outlined in the following text [23], [24], [25].

B. PROCEDURE IN QUANTUM KEY DISTRIBUTION (QKD)

- The photons travel via a filter known as a polarizer. They are given a polarization at random out of a total of four possibilities. The bit designations are completed as follows: "vertical (one bit), horizontal (zero bit), 45° right (one bit), or 45 ° left (zero bit)."
- When the photons arrive at the receiver, there are two beam splitters that are used to "read" the polarization of each individual photon. One beam splitter is horizontal/vertical, while the other beam splitter is diagonal. The receiver needs to make an educated guess in order to decide which beam splitter should be used for each individual photon.
- The sender is responsible for verifying the receiver's information in the order that polarizers appear in the message. In most cases, the key is transmitted after the stream of photons has been sent.

  After that, the information is relayed back to the sender by the receiver. For instance, for each photon in the sequence that it was transmitted, which beam splitter was used? In addition, the photons that were read with the incorrect beam splitter were destroyed after being examined. After then, the "sequence of bits" that was left over is deemed to be the key, and both the sender and the receiver will utilize it for the encryption and decryption of the information that is being sent.

C. SECURITY OF QUANTUM KEY DISTRIBUTION (QKD)

The following is an example of how the security analysis of the quantum key distribution (QKD) scheme that was explained earlier can be carried out. If the photon is read or copied in any way by an authorized person (also known as an attacker), then the state of the photon will be altered. The receiver at the endpoints can be given the ability to see the change. In another sense, we can state that it is impossible to read a photon, convey it to someone else, or replicate it without being discovered. This is because all three actions require the photon's presence. As a result, it is impossible for the adversary to engage in any form of eavesdropping or modification (also known as a man-in-the-middle attack (MiTM)) [1], [26].

D. CURRENT REAL-WORLD APPLICATIONS RELATED TO QUANTUM CRYPTOGRAPHY

Recently, quantum cryptography has transitioned from theory to practice. As a result, quantum cryptography is now being used for a wide variety of purposes. The details of some of the current real-world applications are given below [10], [16], [27], [28].

- *Quantum key distribution:* The most well-known use of quantum cryptography that our contemporary media makes use of is called quantum key distribution (QKD). The proper parties are the only ones who are privy to the sensitive keys that can be safely sent via QKD. The two people who are conversing with one another are able to use QKD to identify any third party that is attempting to look at the key. By employing quantum superpositions or quantum entanglement and sending information in the form of quantum states, it is possible to design a communication system that is capable of identifying any attempts at industrial espionage. Under quantum key distribution, the production and distribution of keys are the only activities that are allowed; the transmission of message contents is not one of them. After that, one can encrypt (and decrypt) a message by utilizing this key in conjunction with an encryption method. This technology is already beginning to be applied in real life. The second smartphone using quantum cryptography technology, the Galaxy Quantum2, has been introduced by the Korean company SK Telecom in partnership with Samsung. This occurred following the company's announcement that it had completed the development of "quantum virtual private network (VPN)" technology and had successfully integrated QKD technology into IP devices.
- *Quantum digital signature:* The quantum mechanical equivalent of either a classical digital signature is known as a quantum digital signature (QDS). A document, such as a digital contract, can be protected using QDS from forgery by a third party or by one of the involved parties. Additionally, QDS can be utilized to achieve secure authentication between the parties engaged in communication. The foundational tenets of quantum physics serve as the basis for QDS security systems. It enables a sender (in this case, Alice) to sign a message in a method that permits multiple participants to verify the signature. They are all able to confirm if the message originated with the intended recipient or not. Each recipient of the message needs a copy of Alice's "public key," which is a collection of quantum states whose particular identity is only known to Alice, in order to carry out the signature verification operation. Classical public keys are simpler to work with than quantum public keys. However, in the case of QDS, we are able to create digital signatures that are completely secure, which also offers full proof security for the generation and verification of the signatures [29], [30], [31].
- *Mistrustful quantum cryptography:* What should you do if you're not sure whether a collaborating party is reliable? This is where mistrustful quantum cryptography enters the picture. Mistrustful quantum cryptography is a great solution when both sides require reassurance that the other side is acting with good intentions. Both Bob and Alice must contribute personally to the project they are working on, but neither one can be assured the other won't cheat. Commitment schemes, which enable one to commit to a given value while keeping it secret from others and secure computations, are examples of tasks in mistrustful cryptography. The secure computation

enables parties to compute a function through their inputs jointly. Moreover, it keeps those inputs private.

- *Quantum commitment:* A party may make a commitment to a particular value through a quantum commitment. The sender cannot alter the fixed value, and the receiver is in the dark until the sender discloses it. Such commitment techniques are frequently employed in cryptographic schemes, such as "secure two-party computation, zero-knowledge proof, and quantum coin flipping."
- *Position-based quantum cryptography:* The location of a player is the only thing that counts toward their credibility in this setting. A participant might send a message to the receiving party at a known place in order to guarantee that the recipient can only read the data at the predetermined location. Quantum tagging was the umbrella under which the first position-based quantum approaches were investigated in 2002. After that, in 2006, the United States government granted a patent, and two years later, in 2010, the concept of utilizing quantum phenomena for the purpose of location verification was presented.
- *Measurement-device-independent (MDI) quantum cryptography:* The MDI protects the detection system, which is typically the weakest link in the chain when it comes to the implementation of cryptographic systems, from any and all attacks. Because of this, the integrity of the underlying physical devices does not affect the level of security that is maintained. As a result of this unique property, measurement-device-independent quantum cryptography is an excellent option for providing protection from potentially harmful devices.

In this section, we discussed the usefulness of quantum cryptography, the procedure in quantum key distribution (QKD), the security of QKD, and current real-world applications of quantum cryptography.

III. BLOCKCHAIN TECHNOLOGY

Blockchain technology, which is typically utilized in the form of a distributed ledger, is a type of technology that facilitates the possibility of exchanging and storing data in a protected manner. As is common knowledge, a database stores information. A ledger, on the other hand, is nothing more than an account book in which transactions are recorded. A database or ledger of this kind that is distributed digitally is referred to as a blockchain [32]. The authority to make changes to a blockchain is distributed among the members (nodes) of a network, whether it be public or private. DLT stands for distributed ledger technology, which is another name for blockchain. Incentives in the form of digital tokens (equivalent to a certain sum of money) are offered to miner nodes (also known as participating servers) in the form of a consensus method in order to incentive them to update blockchains [33]. Because of blockchain technology, it is now possible to preserve data in the form of certain transactions in a way that is permanent, transparent, and unchangeable [34], [35]. Because it is a decentralized and immutable database, blockchain makes it simpler to record transactions and assets and to keep track of their movement [28].

A. USEFULNESS OF BLOCKCHAIN

Information is currently the primary motivator behind most businesses. It is preferable if it can be received without delay and if it is correct. Because it provides data in real-time that is shared as well as completely transparent, blockchain is the greatest technology for delivering that information because it is stored on an immutable ledger and can only be accessed by members of a network that has been granted permission to do so. These days, data is what drives the majority of enterprises. It would be fantastic if it were received in a timely manner and accurately. Blockchain technology is ideal for the delivery of data of this kind because it provides data in real-time that is entirely shareable and transparent, data that is stored on an immutable ledger, and data that is only accessible to members of a network that has been granted permission to access it. Orders, payments, accounts, and production may all be monitored using a blockchain network. In addition, you are able to watch every step of a transaction, from its commencement to its conclusion. because everyone can view the exact same version of the ledger at the same time [36].

B. WORKING OF BLOCKCHAIN

The working of a blockchain is explained below.

- *Occurrence of a transaction and its recording in a block:* These transactions represent the transfer of an asset, which may be either tangible (a product) or intangible (intellectual), depending on the nature of the asset. Who, what, when, where, how much, and even the scenario, which refers to the weather in a particular region, are all important questions to ask. These are all pieces of knowledge that are important. The data block is capable of storing anything and everything.
- *Consensus and addition of block in the blockchain:* When an asset is moved from one location to another, these blocks link together to form a chain of data. The blocks provide reassurance regarding the exact timing and sequence of the transactions, and the fact that they are securely connected to one another makes it impossible for any blocks to be altered or added in the space between two already existing blocks. The verification of the block that came before it and, as a result, the blockchain as a whole are both improved with each new block that is added. This makes it possible for the blockchain to be tamper-proof, and it also gives it its primary advantage of immutability. By following this approach, the users of the network will be able to establish a trustworthy ledger of transactions and eliminate the risk of intervention from malicious actors, such as hackers.

C. APPLICATIONS RELATED TO BLOCKCHAIN

Some of the potential applications of blockchain are given below [4], [37].

- *Payment processing and money transfer systems:* It may be possible to eliminate (or significantly reduce) the fees associated with bank transfers, and transactions conducted using a blockchain may be finalized in a matter of seconds.
- *Supply chain processing and management:* Businesses have the potential to utilize blockchain technology to detect issues more rapidly in their supply chains, monitor items in real-time, and verify the quality of their products as they move from the point of production to the point of consumption.
- *Digital identity system:* Certain companies in the information technology sector are conducting experiments using blockchain technology in an effort to provide customers with more control over who has access to their data and to assist customers in better managing their credentials.
- *Secure information sharing:* Blockchain technology has the potential to act as an intermediary for the secure transfer and storage of commercial data between different industries.
- *Copyright and royalties protection:* Blockchain technology has the potential to be exploited to construct a decentralized database that not only ensures the protection of rights (for example, music albums and movies) but also provides the original producers with royalties that are both transparent and paid in real-time. It's possible that blockchain technology will also be beneficial to open-source software developers.
- *Management of Internet of Things (IoT) network:* In order to establish the reliability of devices that are linked to a wireless network, it is necessary to monitor the activities of the devices that are connected to the network. In addition to this, if a new device, such as a smartphone, is introduced to the network, it immediately does an analysis to determine how trustworthy that device is. Under these conditions, blockchain has the potential to take on the role of an IoT network regulator.
- *Secure smart healthcare system:* The usage of blockchain technology might offer significant advantages to the healthcare sector. Payers and providers of healthcare are turning to blockchain technology to handle the data associated with clinical trials and electronic medical records while maintaining compliance with applicable regulations.

Apart from the above applications, the blockchain technology has been also applied in securing the following: smart and precision agricultural IoT networks [38], [39], [40]; smart grids [41], [42]; global roaming in mobility networks [43]; Big Data analytics [44], [45]; ransomware attacks detection [46]; vehicular ad-hoc networks (VANETs) and Internet of Vehicles (IoV) [47], [48], [49], [50]; crowdsourcing system [51]; Cyber–Physical System (CPS) [52]; Internet of Drones (IoD) [53], [54], [55], [56], [57], [58].

D. TYPES OF BLOCKCHAIN

The following types of blockchains are in practice.

- *Public blockchains:* Public blockchains are completely decentralized, do not require any authorization to access, and are available to anyone. Public blockchains give every node the same level of access to the ledger, the capacity to add new blocks of data to the chain, and the ability to validate the blocks of data that are already in the chain. Public blockchains are being used extensively in the mining and trading of bitcoins in the modern day. Take Bitcoin, Ethereum, and Litecoin as three instances of cryptocurrencies. On these open blockchains, the nodes "mine" for Bitcoin by constructing blocks for the network that contain the desired transactions by solving cryptographic puzzles. These blocks contain the requested transactions. As a form of compensation for the difficult work that they put in, the miner nodes are given a little amount of money. The miners perform much the same function as bank tellers in that they initiate a transaction and are subsequently compensated for their efforts.
- *Private blockchains:* Permissioned blockchains that a particular organization administers are referred to as private blockchains. These blockchains are also known as managed blockchains. A centralized authority is in charge of determining who can participate in the private blockchain. In addition, the central authority might not necessarily grant each node the same equal right to carry out particular obligations. Private blockchains are only partially decentralized because there are constraints placed on who can access them. One example of this is the private blockchain used by a smart healthcare system. Private blockchains are more vulnerable to fraud and dishonest players, while public blockchains typically have lengthier validation processes for the inclusion of new blocks. Both types of blockchains have their drawbacks, though. The introduction of consortium blockchain was done so as to remedy these deficiencies.
- *Consortium blockchains:* Consortium blockchains, also known as permission blockchains, differ from private blockchains in that, unlike private blockchains, a single organization does not own them. Consortia blockchains, on the other hand, are more decentralized than private blockchains, which contributes to an improvement in their level of safety. However, the process of constructing consortium blockchains can be challenging because it requires collaboration between multiple organizations. This creates logistical challenges in addition to potential antitrust risk. Additionally, some of the companies may not have the necessary infrastructure and technology to utilize blockchain technologies, and even those who have may consider that the upfront costs are too high of a price to pay in order to digitize their data and link it to the other players in the supply chain. Those who do have the necessary infrastructure and technology may be hesitant

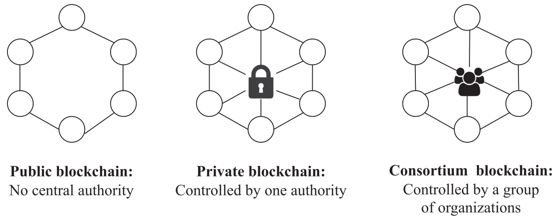

FIGURE 1. Different types of blockchains.

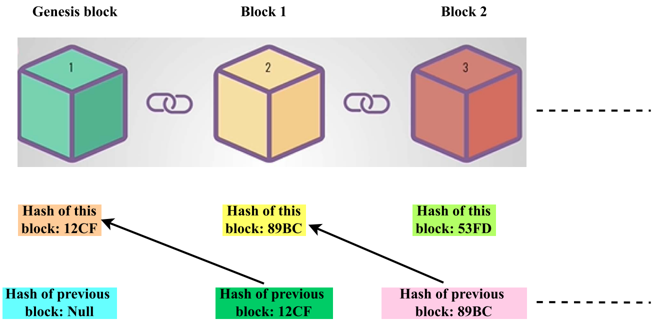

FIGURE 2. Structure of blockchain.

to use blockchain technologies because of the potential risks involved. Examples of well-known consortium blockchains include the Global Shipping Business Network, Marco Polo, and Voltron, to name just a few.

The different types of blockchains are also depicted in Fig. 1.

E. STRUCTURE OF BLOCKCHAIN

The fundamental structure of the blockchain is where it gets its name. Blocks are connected together to form the blockchain's organizational structure. Understanding the architecture of the blockchain is necessary to comprehend blockchain security. The distributed ledger of a blockchain is composed of blocks, which serve as data storage. The shared state of the blockchain network is expanded by the many transactions contained in each block of the blockchain. The header and the body are the two sections that make up each block [59]. The blockchain header information includes the block's identification number, timestamp value, random nonce value, hash of the current block, the hash of the previous block, Merkle tree root value, owner's public key, owner's identification number, and block's signature. While the bodily part incorporates transactions (i.e., in plaintext or encrypted). It is common to refer to the blockchain's structure as a collection of blocks that are joined together in a way that prevents their alteration [2], [3]. The blocks' hash values are what connect them. The structure of the blockchain is given in Fig. 2.

The information on different fields of a block in a blockchain is given below.

- *Block's identification number:* It is the identification number of a block, which provides a unique identity of a block in a blockchain.
- *Timestamp value:* It is a timestamp value, which provides information about the creation of the block, i.e., when it was created.
- *Random nonce value:* It is a random nonce value, which is uniquely assigned to a block.
- *Hash of the current block:* It is the hash value of the block, which is produced for a block by applying a hashing method, in this case, the Secure Hash Amgorithm 256 (SHA256). If there is even a minute alteration to the information included within the block, the hashing value of the block will be completely disrupted.
- *Hash of the previous block:* It is the hash value of the preceding block, which is produced for a block using a hashing technique, namely, Secure Hash Algorithm 256 (SHA256). This value is used to verify transactions and prevent double-spending. It is put to use in the process of connecting the various blocks that make up the blockchain. For instance, in the blockchain, the Hash of the current block field of the current block is connected to the Hash of the current block field of the previous block.
- *Merkle tree root value:* A Merkle tree root can be considered as the hash of different hash values. On the blockchain network, a hash is connected to every transaction. Instead of being kept on the block in a sequential manner, these hashes are instead organized into a tree-like structure, with each hash being connected to its parent through a parent-child relationship. A Merkle root is produced as a result of hashing all of the transaction hashes in a block since there are many transactions placed on that block. A Merkle tree root can be used to check the integrity of the blocks of the blockchain in an efficient way.
- *Owner's identification number:* It is a unique identification number of the owner of the block, which informs about the creator of the block.
- *Owner's public key:* It is a public key value of the owner of the block. For example, if we use Elliptic Curve Cryptography (ECC) for the encryption of the data, G is a base point, Q_{OW} is a public key and k_{OW} is a private key, then $Q_{OW} = k_{OW}.G$.
- *Transactions:* This field contains the actual data of the blockchain-based communication environment. The entire data is converted in the form of some transactions (i.e., T_x where $x = 1, 2, \cdots i$) and then stored in the blocks of the block. It depends on the scenario, in which we can put the transactions either in the encrypted form (i.e., $E_{Q_{OW}}(T_x)$) or in the plaintext (i.e., T_x).
- *Block's signature:* This field contains the signature value of each block, which is maintained in the blockchain. The legitimacy of a block can be verified through its signature.

The structure of a block in a blockchain is given in Fig. 3. Moreover, the structure of a block of the quantum blockchain is given in Fig. 4. Most of the operations that have been

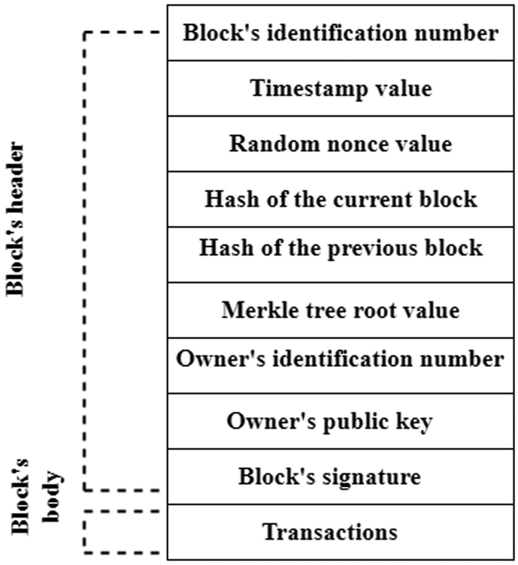

FIGURE 3. Structure of a block in a blockchain.

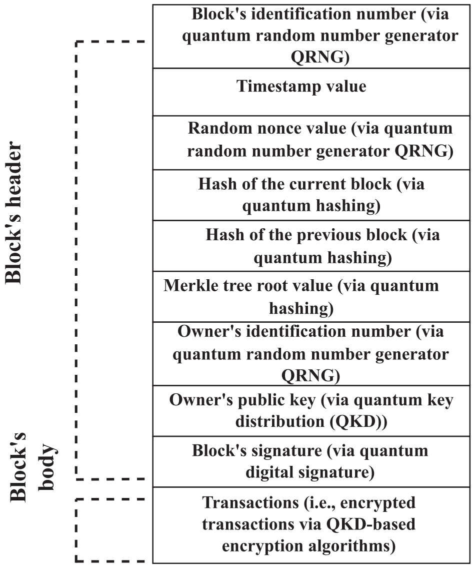
Block's header
Block's body
Block's identification number (via quantum random number generator QRNG)
Timestamp value
Random nonce value (via quantum random number generator QRNG)
Hash of the current block (via quantum hashing)
Hash of the previous block (via quantum hashing)
Merkle tree root value (via quantum hashing)
Owner's identification number (via quantum random number generator QRNG)
Owner's public key (via quantum key distribution (QKD))
Block's signature (via quantum digital signature)
Transactions (i.e., encrypted transactions via QKD-based encryption algorithms)

FIGURE 4. Structure of a block in a quantum blockchain.

performed are quantum secure and have unbreakable security against classical attacks as well as quantum attacks.

In this section, we discussed the usefulness of blockchain, working of blockchain, applications of blockchain, types of blockchain, structure of a blockchain, structure of a block in a blockchain, and structure of a block in quantum blockchain.

IV. EXISTING SURVEYS

In this section, we briefly discuss the state of art existing related surveys, and compare them with the proposed survey.

Yang et al. [14] first discussed post-quantum blockchains, where they utilize the classical cryptographic primitives that are resilient to quantum attacks. Next, they explored the quantum blockchains, that can leverage the power of quantum computers as well as networks for the foundations of blockchains. They also provided a comprehensive overview and comparative study among the post-quantum and quantum blockchains, and they explored open questions and challenges in these domains.

Karakaya and Ulu [60] conducted a comprehensive survey on the recent developments in quantum-resistant blockchain architectures, which are intended for use across various platforms and scenarios. Furthermore, they emphasized the potential of quantum-based secure blockchain structures in a wide range of applications, such as cryptocurrencies, communication, voting, smart grids, and healthcare.

Fernandez-Carames and Fraga-Lamas [6] explored the current state of the art in post-quantum cryptographic primitives, highlighting their application to blockchains and "Distributed Ledger Technologies (DLTs)". They further examined significant post-quantum blockchain systems and their main challenges. Additionally, they conducted a comparative analysis of the characteristics and performance of post-quantum public-key encryption and digital signature schemes tailored for blockchain applications.

Thanalakshmi et al. [61] investigated the incorporation of post-quantum signatures into the "InterPlanetary File System (IPFS)" within a blockchain framework. They proceeded to compare post-quantum signatures, recommended by the "National Institute of Standards and Technology (NIST)", with the "Elliptic Curve Digital Signature Algorithm (ECDSA)" in a Bitcoin exchange scheme. This comparison aimed to demonstrate the system's effectiveness in mitigating quantum threats while preserving optimal performance.

Li et al. [62] reviewed various advancements in the quantum blockchain field. They also provided a brief analysis of its benefits over traditional blockchain technology. Subsequently, they explored the architecture and framework of the quantum blockchain. Lastly, they examined the approach for integrating quantum technology into specific aspects of the conventional blockchain.

A summary table among these surveys and the proposed survey is also provided in Table 2. We have considered the following attributes for comparative study purpose: A01: "Overview of Blockchain Technology"; A02: "Details on Quantum Cryptography"; A03: "Post-quantum Cryptography"; A04: "Quantum Blockchains"; A05: "Classical Blockchains *versus* Quantum Blockchains"; A06: "Comparison of Post-quantum and Quantum Blockchains"; A07: "Generic Quantum Blockchain-envisioned Security Framework for IoT Applications"; A08: "Quantum Key Distribution Mechanisms Comparison"; A09: "Quantum Digital Signature Mechanisms Comparison"; A10: "Quantum Hashing Mechanisms Comparison"; A11: "Lessons Leearned"; A12: "Future Research Directions". It is evident from Table 2, our present survey provides more in-depth analysis and attributes as compared to other existing state of the art survey works.

TABLE 2. Comparative Study With Existing Surveys

Study	Year	A01	A02	A03	A04	A05	A06	A07	A08	A09	A10	A11	A12
Yang et al. [14]	2023	✓	✓	✓	✓	✓	✓	×	✓	×	×	✓	✓
Karakaya and Ulu [60]	2023	✓	×	✓	×	×	×	×	×	✓	×	✓	×
Fernandez-Carames and Fraga-Lamas [6]	2020	✓	×	✓	×	×	×	×	×	✓	×	✓	✓
Thanalakshmi et al. [61]	2023	✓	×	✓	✓	×	×	×	×	✓	×	×	×
Li et al. [62]	2019	✓	×	×	✓	×	×	×	×	×	×	×	✓
Present Survey	2024	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Note: A01: "Overview of Blockchain Technology"; A02: "Details on Quantum Cryptography"; A03: "Post-quantum Cryptography"; A04: "Quantum Blockchains"; A05: "Classical Blockchains *versus* Quantum Blockchains"; A06: "Comparison of Post-quantum and Quantum Blockchains"; A07: "Generic Quantum Blockchain-envisioned Security Framework for IoT Applications"; A08: "Quantum Key Distribution Mechanisms Comparison"; A09: "Quantum Digital Signature Mechanisms Comparison"; A10: "Quantum Hashing Mechanisms Comparison"; A11: "Lessons Leearned"; A12: "Future Research Directions".

✓ : "Covered in Survey"; × : "Not Covered in Survey".

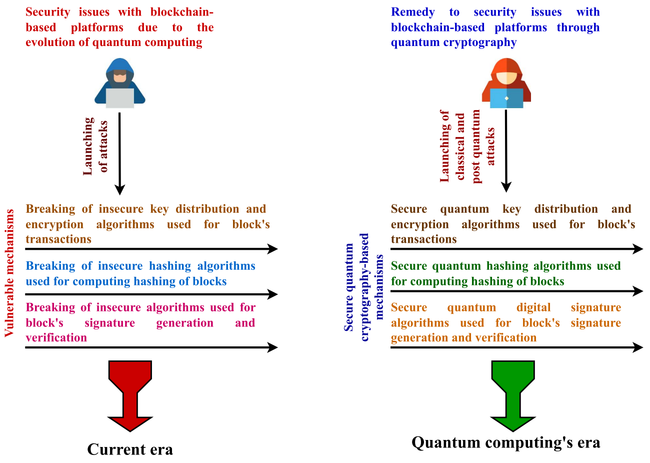
Security issues with blockchain-based platforms due to the evolution of quantum computing
Launching of attacks
Vulnerable mechanisms
Breaking of insecure key distribution and encryption algorithms used for block's transactions
Breaking of insecure hashing algorithms used for computing hashing of blocks
Breaking of insecure algorithms used for block's signature generation and verification
Current era
Remedy to security issues with blockchain-based platforms through quantum cryptography
Launching of classical and post quantum attacks
Secure quantum cryptography-based mechanisms
Secure quantum key distribution and encryption algorithms used for block's transactions
Secure quantum hashing algorithms used for computing hashing of blocks
Secure quantum digital signature algorithms used for block's signature generation and verification
Quantum computing's era

FIGURE 5. Comparison of the current era and quantum computing's era.

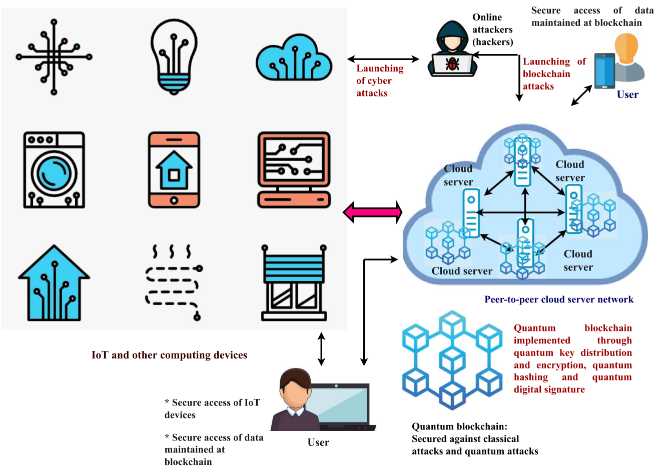
Online attackers (hackers)
Secure access of data maintained at blockchain
Launching of cyber attacks
Launching of blockchain attacks
User
Cloud server
Cloud server
Cloud server
Cloud server
Peer-to-peer cloud server network
IoT and other computing devices
Quantum blockchain implemented through quantum key distribution and encryption, quantum hashing and quantum digital signature
* Secure access of IoT devices
* Secure access of data maintained at blockchain
User
Quantum blockchain: Secured against classical attacks and quantum attacks

FIGURE 6. Generic quantum blockchain-envisioned security framework for IoT environment.

V. GENERIC QUANTUM BLOCKCHAIN-ENVISIONED SECURITY FRAMEWORK FOR IOT ENVIRONMENT

In this section, we describe a generic quantum blockchain-envisioned security framework for an IoT environment.

A. GENERIC QUANTUM BLOCKCHAIN-ENVISIONED SECURITY ARCHITECTURE

The architecture of a generic quantum blockchain-envisioned security framework for the IoT environment is given in Fig. 6. It contains different IoT devices and other computing devices, i.e., laptops, smartphones, etc. These devices generate data in an enormous amount, which is stored in some servers (in relational database management systems). In the normal case, the authorized user can access the IoT devices and associated data from the servers for their various uses. However, there are also some malicious actors (i.e., hackers) who always try to breach the security of the system for their various gains. The malicious actors can launch various classical attacks (replay, man-in-the-middle, impersonation, credential guessing, unauthorized information update), quantum attacks blockchain attacks (i.e., 51% mining, Sybil, double spending) on this infrastructure. Therefore, it is suggested to store the data over some blockchains [63]. However, such an arrangement is also vulnerable to various quantum attacks. Hence, we introduce the concept of quantum blockchain. The quantum blockchain incorporates various secure mechanisms, like, quantum key distribution, quantum hashing, quantum digital signature, and quantum random number generator. It stores the data in the form of blocks and also protects it against the various classical attacks and quantum attacks [64].

Through the usage of the quantum blockchain, only the users who have been verified and given permission to do so can access the system's data. After completing the necessary stages of an authentication or access control protocol, they also have the ability to access any Internet of Things device directly. Fig. illustrates the structure of a block in a classical blockchain, while Fig. illustrates the structure of a block in a quantum blockchain. Over the peer-to-peer cloud server network, the quantum blockchain is kept updated and maintained. After completing the necessary phases of the consensus mechanism, known as practical Byzantine Fault Tolerance (pBFT), the blocks are then added to the quantum blockchain. During these steps, the number of valid minor nodes (also known as servers) take part and commit to the addition of a newly produced block [65]. The proposed architecture calls for a number of different entities, including users and cloud servers, IoT devices and cloud servers, and cloud servers to cloud servers, to carry out the stages of authentication and key establishment.

Remark 1: There are also some malicious actors, like hackers, who always try to breach the security of traditional communication frameworks for their various gains. The hackers can launch various classical attacks (replay, man-in-the-middle, impersonation, credential guessing, unauthorized information update), quantum attacks, and blockchain attacks (i.e., 51% mining, Sybil, double spending). Therefore, it is suggested to store the data over some blockchains. However, such an arrangement is also vulnerable to various quantum attacks. Hence, we introduce the concept of quantum blockchain. The quantum blockchain incorporates various secure mechanisms, like quantum key distribution, quantum hashing, quantum digital signature, and quantum random number generator. It stores the data in the form of blocks and also protects it against various classical attacks and quantum attacks. However, such facilities are not available in the traditional communication frameworks. Through the usage of the quantum blockchain, only the users who have been verified and given permission to do so can access the system's data. After completing the necessary stages of an authentication or access control protocol, they also have the ability to access any Internet of Things device directly. Over the peer-to-peer cloud server network, the quantum blockchain is kept updated and maintained. After completing the necessary phases of the consensus mechanism, the blocks are then added to the quantum blockchain. The proposed architecture calls for a number of different entities, including users and cloud servers, Internet of Things devices and cloud servers, and cloud servers to cloud servers, to carry out the stages of authentication and key establishment. Therefore, the proposed quantum blockchain-envisioned security framework is applicable for the secure communication of different applications, like smart healthcare systems, intelligent transportation systems, smart agriculture and farming, smart grid and energy systems, smart manufacturing and industrial control systems, smart surveillance, and security systems, and banking and finance systems.

B. THREAT MODEL

When creating the proposed framework, the guidelines of a well-known danger model called the Dolev-Yao (DY) threat model were used. This model was named after its authors [66]. According to the DY model, the entirety of the communicating system, including smart IoT devices, servers, and users, communicates over the public channel, which is insecure by its very definition. The current enemy, which consists of hackers connected to the Internet, has the potential to interfere with the communication that is currently taking place [67]. Because of this, the information that was shared may be disclosed, altered, or removed. An attacker may physically capture some of the smart devices and then attempt to use a power analysis attack to retrieve information from the devices' memories after doing so [68]. In addition, the continuing connection can be attacked in many different ways, including classical attacks, quantum attacks, man-in-the-middle attacks, replay attacks, impersonation attacks, credentials leakage attacks, blockchain attacks, 51% mining attacks, double spending attacks, sybil attacks, and many more [34], [69]. Because there are so many threats, we require certain security frameworks to secure the information that is being transmitted as well as the infrastructure that is involved with it [70], [71], [72].

In this section, we have provided the architecture of a generic quantum blockchain-envisioned security framework for the IoT environment. Further, we have discussed how generic quantum blockchain-envisioned security framework for the IoT environment better than the traditional framework. A closely related threat model for the proposed framework was also provided.

VI. ADVERSE EFFECTS OF QUANTUM COMPUTING ON BLOCKCHAIN-BASED FRAMEWORKS AND EVOLUTION OF QUANTUM CRYPTOGRAPHY

A. ADVERSE EFFECTS OF QUANTUM COMPUTING ON SECURITY IN BLOCKCHAIN-BASED FRAMEWORKS

The goal of post-quantum cryptography, also known as quantum-proof cryptography, is to develop encryption techniques that are impervious to attack by quantum computer algorithms in the future. The security of current encryption techniques won't necessarily hold true if and when quantum computers are developed. the RSA algorithm, as an illustration. As we all know, the foundation of applications like Internet browsers and digital signature software is the widely adopted secure data transfer technique known as RSA. In which the sets of public and private keys are produced. When you use an Internet browser or a digital signature to sign a document, the procedure takes place in the background. In the RSA algorithm, a secret private key is obtained through two large prime numbers. Then, using the sum of those two values plus an exponent, the public key is created. Anyone can encrypt data using the public key, but after it has been encrypted, only the private key can be used to decrypt it again. The encryption mechanism depends on the fact that it requires a lot of time and computational capabilities to factor in the large integer. These two factors of the large integer number help in the generation of public key and private key. Shor's algorithm, however, which was developed by mathematician Peter Shor and published in 1994, explains how, in theory, quantum computers may factor extraordinarily large numbers effectively. The security of RSA-based communication systems can thus be compromised using techniques like Shor's algorithm [73]. Blockchain-based frameworks are utilized important cryptographic techniques, like, encryption, digital signature, and hashing, to achieve various information security requirements. For example, Elliptic Curve Cryptography (ECC) algorithm can be used to do the encryption of the transactions and Elliptic Curve Digital Signature Algorithm (ECDSA) can be used for the signature generation and verification of the blocks. The security of these algorithms depends on the properties of the elliptic curve discrete logarithm problem, which is difficult to solve with the current computer systems. However, the security of these algorithms can be broken with the help of quantum computers, as we have discussed for the RSA algorithm [25], [26].

B. RISE OF QUANTUM BLOCKCHAIN-ENVISIONED FRAMEWORKS WITH INCLUSION OF QUANTUM CRYPTOGRAPHY

As a result, it is quite possible that people will switch to new public key cryptography techniques based on problems that we do not believe quantum computers are capable of efficiently resolving. Finding solutions to problems like these is one of the main focuses of ongoing research in the subject of quantum cryptography, sometimes known as future cryptography. The principles of quantum physics are used in quantum encryption, which is a method of securely transmitting confidential information that prevents illegal listening. For instance, one method of quantum cryptography known as quantum key distribution (QKD) is the one that has received the most attention from researchers and is now the most applicable. This method uses a series of photons to send a key that is a secret random sequence. By comparing the results of the measurements taken at each end of the transfer, users will be able to establish whether or not the key has been compromised. If someone were to wiretap a phone in order to intercept confidential data stealthily, the callers would be unaware of the intrusion. Under those conditions, it is not possible to estimate a quantum encryption key without causing disturbances in the photons and changing the outcomes of the measurements carried out at both ends of the chain. This is due to the uncertainty principle, which is a statement of quantum physics that stipulates that measuring one feature of a quantum system may affect some of the other properties of the quantum item (for example, a photon). The uncertainty principle is the reason why this is the case. Therefore, the communicating system, which uses QKD seems secure against all possible threats, even the threats caused by the quantum computing [10], [28]. In a similar way, we have other quantum cryptographic techniques, like quantum digital signatures and quantum hash functions, which can be further utilized in the implementation of future blockchains to provide more security and robustness to the associated applications [6], [16], [74], [75].

The comparison of the current era and quantum computing's era is given in Fig. 5. From the information given in Fig. 5, it is clear that the schemes, like key distribution, hashing, and digital signature, are more secure in the case of quantum computing's era. As they can mitigate various types of attacks with the help of quantum cryptographic operations. However, in the current era, these schemes seem vulnerable to various attacks.

In this section, the adverse effects of quantum computing on blockchain-based frameworks and the evolution of quantum cryptography were discussed. A comparison of the current era and quantum computing's era was given.

VII. COMPARISONS OF QUANTUM CRYPTOGRAPHY-BASED SECURITY SCHEMES

In this section, we provide a comparison of various quantum cryptography-based security schemes, i.e., quantum key distribution mechanisms, quantum hashing algorithms, and quantum digital signature mechanisms.

A. COMPARISON OF QUANTUM KEY DISTRIBUTION SCHEMES

In this section, we provide a comparison of various quantum key distribution schemes. We also review some state-of-art schemes.

1) SCHEME OF LUCAMARINI ET AL. (YEAR 2015)

- The security proof of "effective decoy-state BB84 protocol for QKD" was expanded by Lucamarini et al. [76] to include the broadest attack permitted by the laws of physics.
- Additionally, they enhanced the protocol by adding features like the option to remove the presumption of complete state preparation on the sender's end. This flaw was a part of the quality component, which the consumers should have described in advance.

2) SCHEME OF CAO ET AL. (YEAR 2019)

- The deployment costs of QKD-over-WDM backbone networks were explored in detail by Cao et al. [77].
- They presented a standard framework for QKD over WDM backbone networks. To further explain the cost-minimized problem, a novel cost-oriented model was developed, in which a variety of QKD network elements, such as "QKD transceivers, QKD auxiliary equipment for QKD backbone nodes and trusted repeater nodes (TRNs), and QKD links," were taken into account.
- They also included in their defined model the physical-layer factors such as "secret-key rate, physical distance, and TRN layout." To tackle the cost-minimized challenge, they created an innovative "cost-efficient QKD networking (CEQN)" heuristic method using an integer linear programming (ILP) model.
- Their proposed strategies were beneficial in lowering the cost of constructing QKD-over-WDM backbone networks, according to comprehensive simulations, where the CEQN algorithm was successfully shown.
- Finally, the various open challenges of future work were mentioned.

3) SCHEME OF GHALAII ET AL. (YEAR 2020)

- Ghalaii et al. [78] investigated the performance of a CV-QKD system that utilized a quantum scissor as the pre-homodyne receiver and quadrature phase shift keying modulation at the encoder.

- The purpose of this research was to discover whether or if using quantum scissors (QS) as a nondeterministic amplifier can improve the system's rate behavior over extended distances and, if so, to what degree this is possible.
- By optimizing the relevant system parameters, they demonstrated that the discrete-modulation system with a QS could withstand less excess noise than the discrete-modulation system without a QS. As a result, the QS-equipped system could continue further at positive quantities of excess noise.

4) SCHEME OF LIU ET AL. (YEAR 2021)

- Liu et al. [79] suggested an improved RFIMDI-QKD procedure that was very resistant to statistical fluctuations in the finite-size domain.
- They provided a method that reduces computational complexity and raises the key rate by extending the double scanning method to multi-basis computations.
- Simulation findings with various data sizes confirm their method's effectiveness.
- Additionally, even with the reference frames not being perfectly aligned, they were still able to carry out the RFI-MDI-QKD experiment over a 300 km fiber range.

5) SCHEME OF AL-DARWBI ET AL. (YEAR 2022)

- Al-Darwbi et al. [80] proposed a technique for the distribution of quantum keys called QKeyShield, which was receiver-device independent. A biased operator selection was utilized, which resulted in an increase in the total amount of bits generated. The qubits that were transmitted had been safeguarded using a variety of different built-in procedures.
- In addition, safety analyses for a number of different attacks that are allowed by quantum mechanics have been provided, demonstrating the efficiency and safety of QKeyShield.
- When compared to protocols that came before it, QKeyShield offered some advantages, including the ability to achieve high utilization efficiency and the possibility of enabling conference quantum key distribution. These were just two of the advantages.

6) SCHEME OF YU ET AL. (YEAR 2022)

- Yu et al. [81] researched scenarios involving partially trustworthy relays and focused his attention on the main routing used by these scenarios in a variety of common network topologies.
- Within the context of a partially trusted relay-based QKD technique, the potential of a pair of optical nodes sharing secret keys when trusted and untrusted relays coexist was proposed. This scenario occurs when trusted and untrusted relays coexist.
- A new approach called secret-key provisioning with collaborative routing (SKP-CR) was introduced in order to locate the most efficient key-relay routing path.
- They ran the simulations using different amounts of traffic, starting secret key values in the quantum key pools (QKPs) and ratios of trustworthy relays to untrusted relays.
- The results of the simulations revealed that the utilization of mesh topology by the SKP-CR algorithm has the potential to significantly boost the success rate of key distribution for the conventional trusted-relay-based scheme by up to 62%.

The summary of various quantum key distribution schemes is also given in Table 3.

B. COMPARISON OF QUANTUM DIGITAL SIGNATURE SCHEMES

In this section, we provide a comparison of various quantum digital signature schemes.

1) SCHEME OF SHAFIEINEJAD ET AL. (2017)

- Shafieinejad et al. [82] proposed a One-time signatures (OTS), which was better than the hash-based OTS.
- The OTS scheme's performance was improved by employing Bloom filters as one-way functions rather than hash functions. This modification keeps the system quantum-safe while addressing the fundamental issue with hash-based OTS, which was memory needs.
- Comparing the proposed approach to the original hash-based OTS, both the signature and the public verification key size are reduced.

2) SCHEME OF ZHANG ET AL. (YEAR 2018)

- In order to construct a secure blockchain-based system that is resistant to quantum attacks, blind signatures can also be used [83].
- Zhang et al. [84] gave a presentation in which he detailed a method for producing a post-quantum blind signature that was based on lattice assumptions.
- They demonstrated that the possible security issue could be resolved using any existential forgery against the security of the scheme that was ultimately produced.
- The methodology that they developed was based on the rejection sampling theory as its primary conceptual underpinning. Their innovative solution featured a blind signature with a size that was noticeably less in comparison to all of the other blind signature schemes that had been offered previously for use with lattices, and the predicted number of times that were required to generate a blind signature was at most e^2 under aborting.

3) SCHEME OF SHAHID ET AL. (YEAR 2020)

- Shahid et al. [85] proposed a new one-time signature mechanism, called NOTS, to make the system resistant to quantum attacks.

TABLE 3. Summary of Various Quantum Key Distribution Schemes

Scheme	Overview	Security problem solved	Usability
Lucamarini et al. [76] (2015)	The security proof of "effective decoy-state BB84 protocol for QKD" was expanded. They discussed the broadest attack permitted by the laws of physics. They improved the protocol by adding features like the option to remove the presumption of complete state preparation on the sender's end.	Quantum key distribution.	The scheme can be used for the quantum key distribution and secure data transmission.
Cao et al. [77] (2019)	They presented a standard framework for QKD over WDM backbone networks. They discussed a variety of QKD network elements, such as "QKD transceivers, QKD auxiliary equipment for QKD backbone nodes and trusted repeater nodes (TRNs), and QKD links".	Quantum key distribution.	Quantum key distribution, cost-efficient QKD networking (CEQN).
Ghalaii et al. [78] (2020)	They looked at the performance of a CV-QKD system that employed a quantum scissor as the pre-homodyne receiver and quadrature phase shift keying modulation at the encoder. They wanted to determine whether and to what degree using quantum scissors (QS) as a nondeterministic amplifier may enhance the system's rate behavior across extended distances.	Quantum key distribution.	The scheme can be used for the quantum key distribution and secure data transmission.
Liu et al. [79] (2021)	They suggested an improved RFIMDI-QKD procedure that was very resistant to statistical fluctuations in the finite-size domain. They provided a method that reduces computational complexity. They carried out the RFI-MDI-QKD experiment over a 300 km fiber range.	Quantum key distribution.	The scheme can be used for the quantum key distribution and secure data transmission.
Al-Darwbi et al. [80] (2022)	They proposed QKeyShield, a receiver-device agnostic quantum key distribution technique. It used a biassed operator selection, which boosts the number of bits produced. The security studies for a variety of attacks permitted by quantum mechanics were offered, demonstrating the efficacy and security of QKeyShield.	Quantum key distribution.	The scheme can be used for the secure key distribution and encryption in the quantum computing era.
Yu et al. [81] (2022)	They investigated partially-trusted relay scenarios and concentrated on its key routing in various types of common network topologies. The possibility of a pair of optical nodes sharing secret keys when trusted and untrusted relays coexist was described. To find the ideal key-relay routing path, a "secret-key provisioning with collaborative routing (SKP-CR)" algorithm was presented.	Quantum key distribution and collaborative routing.	The scheme can be used for quantum key distribution and collaborative routing.

- It provided minimal key and signature sizes from all of the OTS/FTS methods that were already in use. Comparing NOTS to the well-known WOTS method, both the key and signature sizes were reduced by 88%.
- Additionally, NOTS reduced the signature and key sizes by 84% and 86%, respectively, in comparison to the current systems.

4) SCHEME OF WANG ET AL. (YEAR 2021)

- The increased anonymity of quantum digital signatures was necessary in order to give users more privacy when creating them. In some situations, the quantum ring signature system focused on anonymity. The quantum message signer concealed his identity within a group by using the quantum ring signature mechanism. The user of the quantum ring signature system did not require any type of central administration at the same time. There is no user collaboration involved in choosing the group that would be utilized to conceal the signer's identity.
- Because the quantum finite automaton signature method was quite effective, Wang et al. [86] presented a new quantum ring signature strategy based on it. They demonstrated the accuracy, anonymity, and unforgeability of their method.
- Additionally, the new scheme could only be carried out logically, making it simple to put into practise.

5) SCHEME OF LI ET AL. (YEAR 2022)

- For representative nodes to quickly generate appropriate blocks and normal nodes to reach a consensus, a new consensus technique called quantum delegated proof of stake (QDPoS) based on quantum voting was presented by Li et al. [8].
- Quantum computers were not able to change QDPoS's fairness, even if they became a reality in the future.
- It was suggested that an efficient quantum blockchain-based system might be created by designing quantum blocks with a single qubit, combining quantum blocks in weighted graph states or weighted hypergraph states, and coupling quantum digital signature with the developed consensus mechanism QDPoS. These steps could be taken in combination with one another.

The summary of various quantum digital signature schemes is given in Table 4.

C. COMPARISON OF QUANTUM HASHING SCHEMES

In this section, we discuss the various quantum hashing schemes.

1) SCHEME OF LI ET AL. (YEAR 2013)

- Li et al. [87] presented two different sorts of interactions. The demonstration of a two-particle quantum stroll was done.
- They researched the traits of this form of quantum walks as well as the two particles' temporal progression.

TABLE 4. Summary of Various Quantum Digital Signature Schemes

Scheme	Overview	Security problem solved	Usability
Shafieinejad et al. [82] (2017)	They proposed a One-time signatures (OTS), which was better than the hash-based OTS. The OTS scheme's performance was improved by employing Bloom filters as one-way functions. In the proposed approach to the original hash-based OTS, both the signature and the public verification key size are reduced.	Quantum digital signature.	Authentication and integrity checking.
Zhang et al. [84] (2018)	A method that is based on lattice assumptions and can be used to create a post-quantum blind signature was provided. The signature size required by their innovative approach was noticeably less than that required by any of the other blind signature schemes suggested previously for use over lattices.	Quantum digital signature.	Authentication and integrity checking.
Shahid et al. [85] (2020)	They proposed a new one-time signature mechanism called NOTS. It provided minimal key and signature sizes from all of the OTS/FTS methods. NOTS reduced the signature and key sizes by 84% and 86%, respectively.	Quantum digital signature.	Authentication and integrity checking.
Wang et al. [86] (2021)	They presented a new quantum ring signature strategy. They demonstrated the accuracy, anonymity, and unforgeability of their method.	Quantum digital signature.	Authentication and integrity checking.
Li et al. [8] (2022)	A novel method of reaching consensus, known as quantum delegated proof of stake (QDPoS), which is based on quantum voting, was introduced in order to facilitate the rapid generation of appropriate blocks by representative nodes and the arrival at a decision by regular nodes. The design of quantum blocks consisting of a single qubit was presented, as was the connecting of quantum blocks in weighted graph states or weighted hypergraph states, as well as the coupling of quantum digital signature with the developed consensus method QDPoS.	Quantum digital signature and blockchain's consensus.	Execution of blockchain's consensus, authentication, and integrity checking.

- Then they presented and described a type of quantum hash technique based on two-particle interacting quantum walks.
- This particular type of quantum hash technique dramatically improved the security of hash schemes by relying on the initial state's limitless possibilities rather than the computational difficulty of the hard problems.

2) SCHEME OF ABLAYEV ET AL. (YEAR 2013)

- Ablayev et al. [88] came up with the idea of a variation of the quantum hash function that was based on non-binary discrete functions.
- The quantum method was founded on the classical-quantum model, and it generated a quantum state by taking as its input a string of classical bits.
- The function that was generated possessed the property of being a one-way function, in addition to the collision resistance and second pre-image resistance that are typical of conventional cryptographic hashes.
- This function may be easily utilized in a quantum digital signature system if it is designed properly.

3) SCHEME OF YANG ET AL. (YEAR 2016)

- Yang et al. [89] looked into the potential of a quantum hash function that may be created by slightly altering the well-known quantum computation model known as quantum walks.
- It was discovered that a quantum hash function might work as a hash function for more secure quantum key distribution networks that amplify privacy.
- Due to its intrinsic chaotic dynamics, the quantum hash function could also be employed to generate pseudo-random numbers as a byproduct.
- Additionally, they provided a novel image encryption algorithm and examined the use of the quantum hash function for image encryption.

4) SCHEME OF AL-KHATEEB ET AL. (YEAR 2010)

- Al-Khateeb et al. [90] presented a key distribution technique based on the use of hash functions for the secure quantum computing system.
- A series of random characters were transferred from sender to recipient as the foundation of the protocol. The key was then created using a chosen hash or a cascade of two hash algorithms along with a long-term shared secret.
- As a result, the sender and receiver sides independently applied a hash function to the random text to create the session key on-site.
- Additionally, it was recommended to employ a technique of out-of-band authentication built on the quantum protocol, known as "deterministic six-state quantum protocol (6DP)."

The summary of various quantum hashing schemes is given in Table 5. In this section, we have provided the comparisons of various quantum cryptography-based security schemes, i.e., quantum key distribution mechanisms, quantum hashing algorithms, and quantum digital signature mechanisms. During comparisons, we have considered various important features, like the overview of the scheme, the security problem that it has solved, and its usability.

TABLE 5. Summary of Various Quantum Hashing Schemes

Scheme	Overview	Security problem solved	Usability
Al-Khateeb et al. [90] (2010)	They presented a key distribution technique based on using hash functions for the secure quantum computing system. A series of random characters were transferred from sender to recipient as the foundation of the protocol. The key was then created using a chosen hash or a cascade of two hash algorithms along with a long-term shared secret. The sender and receiver sides independently applied a hash function to the random text to create the session key.	Quantum hashing and quantum key distribution.	Their scheme can be used for integrity checking and quantum key distribution.
Li et al. [87] (2013)	They showed and discussed a method of computing quantum hashes that is based on the interaction of quantum walks between two particles. Because it relies on the endless possibilities of the beginning state rather than the computational difficulty of the hard issues, this specific sort of quantum hash approach is responsible for the enormous improvement in hash scheme security that it brought about.	Quantum hashing.	Their scheme can be used for integrity checking for the quantum secure system.
Ablayev et al. [88] (2013)	The presentation covered a form of the quantum hash function that was based on non-binary discrete functions. The function that was constructed possessed the quality of being a one-way function, in addition to the collision resistance and second pre-image resistance that are characteristic of conventional cryptographic hashes.	Quantum hashing and quantum digital signature.	Their scheme can be used for integrity checking and authentication.
Yang et al. [89] (2016)	They looked into the potential of a quantum hash function that may be created by slightly altering the well-known quantum computation model known as quantum walks. It was discovered that a quantum hash function might work as a hash function for more secure quantum key distribution networks that amplify privacy.	Quantum hashing and encryption.	Their scheme can be used for hashing (i.e., integrity checking) and encryption of data (i.e., images) for the quantum secure system.

VIII. LESSON LEARNED

We discussed conventional cryptography and security issues with that. Then, we discussed the security advantages of the quantum cryptography-based systems. Further, the procedure of quantum key distribution was explained. After that, we provided the summary of current real-world applications of quantum cryptography, i.e., quantum key distribution, mistrustful quantum cryptography, quantum commitment, position-based quantum cryptography, and measurement-device-independent (MDI) quantum cryptography. We have presented a generic quantum blockchain-envisioned security framework for the IoT environment. Then, we discussed some of the potential applications of the proposed framework. Further, the details of blockchain, i.e., the usefulness of blockchain, were provided. We then explained the workings of blockchain, applications of blockchain, types of blockchain, the structure of blockchain, the structure of blockchain in a classical blockchain, and the structure of a block in a quantum blockchain. Again, the adverse effects of quantum computing on the security of blockchain-based platforms were highlighted. Then, a discussion on the evolution of quantum cryptography and the security benefits of blockchain-based platforms was given. It was discussed that the communicating system, which used QKD seemed secure against all possible threats, even the threats caused by quantum computing. In a similar way, the other quantum cryptographic techniques, like quantum digital signatures and quantum hash functions, could be further utilized in the implementation of future blockchains to provide more security and robustness to the associated application. Then, a comparison of the current era and quantum computing's era was given. Furthermore, the comparisons of quantum cryptography-based security schemes, i.e., quantum key distribution schemes, quantum digital signature schemes, and quantum hashing schemes, were provided. It was identified that the schemes of Al-Darwbi et al. [80] and Cao et al. [77] (in QKD schemes), the schemes of Shahid et al. [85], Li et al. [8] (in QDS schemes) and the scheme of Yang et al. [89] (in quantum hashing schemes) performed better as they provide more security and functionality features.

In this section, we have provided information about the various lessons that we have learned in this study. We have also provided information about the quantum security schemes, i.e., which scheme was more secure and provided more functionality features.

IX. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

In this article, we discussed conventional cryptography and security issues. We presented a generic quantum blockchain-envisioned security framework for the IoT environment. Some of the important applications of the proposed framework were discussed. Furthermore, the details of blockchain were provided, along with the adverse effects of quantum computing on the security of blockchain-based frameworks. The comparisons of quantum cryptography-based security schemes, i.e., quantum key distribution schemes, quantum digital signature schemes, and quantum hashing schemes, are also provided.

Some of the future research directions related to the designed generic quantum blockchain-envisioned security framework for IoT are discussed below.

- *Compatibility issues:* The generic quantum blockchain-envisioned security framework for IoT is an amalgamation of various technologies, like communication technologies, various information security mechanisms, different machine learning/ deep learning algorithms, consensus algorithms, etc. Due to the missing of these many tools/ techniques, there may be issues related to compatibility. Hence, we should design the schemes wisely where we do not have these issues [91].

- *Security of the system:* The presented framework tries to provide security to the communication environment. It is enabled with various quantum cryptography-based security schemes, i.e., quantum key distribution & encryption, quantum digital signature, and quantum hashing. Therefore, it is secured against various classical and quantum attacks. However, in the system, there may be some zero-day attacks or some other forms of advanced attacks, which may break the security of the system [92]. Hence, a security framework should be designed in such a way that it should provide full proof of security [93].
- *Efficiency of the system:* The generic quantum blockchain-envisioned security framework for IoT is an amalgamation of various technologies, like information security, machine learning/deep learning algorithms, consensus algorithms, etc. Some of these algorithms are resource-intensive in nature and require high computation, communication, and storage resources, which is not feasible for all circumstances. Hence, a security framework should be designed with the incorporation of lightweight algorithms, which require less computation, communication, and storage resources.
- *Accuracy of the system:* Sometimes, we need to include machine learning or deep learning-based algorithms to make a system more autonomous, which can predict a phenomenon, i.e., chances of getting the accident, the possibility of getting a heart attack, etc. However, the inclusion of machine learning or deep learning-based algorithms is also challenging and risky if the data is not pre-processed properly or the machine learning model is not trained accurately. Therefore, under these situations, we may have issues related to the accuracy of the system. Hence, we need to take care of such issues while we go for the designing of a security framework.
- *Privacy of data:* The generic quantum blockchain-envisioned security framework for IoT processes and stores, the data which is sensitive in nature, i.e., health-related data. Any kind of revealing of such data may cause big problems. Therefore, it should be processed and stored in such a way that we do not have data privacy-related problems. Hence, a security framework should be designed with the inclusion of guidelines for good privacy models [94].
- *Regulatory and legal difficulties:* It is possible that new regulatory and legal difficulties will arise as a result of the introduction of quantum blockchain and its potential impact on the existing systems. The landscape is continuously shifting, and governments and regulatory organizations will need to adjust accordingly. Therefore, some research is required in this direction, where we can design new tools/technologies for the proper functioning of the quantum blockchain-envisioned security frameworks without any regulatory and legal difficulties.
- *Secure and lightweight digital signature techniques:* Digital signatures play a vital role in facilitating secure and trustworthy transactions within the context of blockchain technology. The integration of quantum-secure digital signatures, which are based on lattice cryptography or hash-based signatures, is imperative for the incorporation of these cryptographic techniques into blockchain platforms. Some research is required in this direction for the designing of secure and lightweight digital signature techniques that are resistant to quantum attacks and applicable to quantum blockchain-envisioned security frameworks.
- *Secure block validation mechanism:* There is a possibility that traditional nodes and miners on the blockchain are not secure against quantum attacks. In order to keep the network secure, quantum-resistant nodes and miners will need to be built and put into use. Therefore, some mechanisms are required for the quantum-secure block validation procedure in the generic quantum blockchain-envisioned security frameworks.

ACKNOWLEDGMENT

The authors would like to acknowledge for the valuable suggestions and feedback of the reviewers and the associate editor for improving the presentation and technical quality of the article.

REFERENCES

[1] M. Rezai and J. A. Salehi, "Quantum CDMA communication systems," *IEEE Trans. Inf. Theory*, vol. 67, no. 8, pp. 5526–5547, Aug. 2021.

[2] H. Halaburda, "Blockchain revolution without the blockchain?," *Commun. ACM*, vol. 61, no. 7, pp. 27–29, 2018.

[3] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[4] S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, and R. Cunningham, "Blockchain technology: What is it good for?," *Commun. ACM*, vol. 63, no. 1, pp. 46–53 2019.

[5] Quantumxchange, "Quantum cryptography, explained," What is Quantum Cryptography?, 2022. Accessed: Dec. 12, 2023. [Online]. Available: https://quantumxc.com/blog/quantum-cryptography-explained/

[6] T. M. Fernández-Caramès 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.

[7] Z. Yang, T. Salman, R. Jain, and R. D. Pietro, "Decentralization using quantum blockchain: A theoretical analysis," *IEEE Trans. Quantum Eng.*, vol. 3, 2022, Art. no. 4100716, doi: 10.1109/TQE.2022.3207111.

[8] Q. Li, J. Wu, J. Quan, J. Shi, and S. Zhang, "Efficient quantum blockchain with a consensus mechanism QDPoS," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 3264–3276, 2022.

[9] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.

[10] D. Dharminder, C. B. Reddy, A. K. Das, Y. Park, and S. S. Jamal, "Post-quantum lattice based secure reconciliation enabled key agreement protocol for IoT," *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2680–2692, Feb. 2023, doi: 10.1109/JIOT.2022.3213990.

[11] F. Merabet, A. Cherif, M. Belkadi, O. Blazy, E. Conchon, and D. Sauveron, "New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 2, pp. 439–474, 2020.

[12] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, "A multimodal malware detection technique for android IoT devices using various features," *IEEE Access*, vol. 7, pp. 64411–64430, 2019.

[13] Z. Liu et al., "An integrated architecture for IoT malware analysis and detection," in *Proc. IoT Service*, 2019, pp. 127–137.

[14] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. D. Pietro, and A. Erbad, "A survey and comparison of post-quantum and quantum blockchains," *IEEE Commun. Surveys Tuts.*, early access, Oct. 19, 2023, doi: 10.1109/COMST.2023.3325761.

[15] L. O. Mailloux, C. D. Lewis II, C. Riggs, and M. R. Grimaila, “Post-quantum cryptography: What advancements in quantum computing mean for IT professionals,” *IT Professional*, vol. 18, no. 5, pp. 42–47, 2016.

[16] K.-A. Shim, “A survey on post-quantum public-key signature schemes for secure vehicular communications,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 14025–14042, Sep. 2022.

[17] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

[18] P. Bagchi et al., “Public blockchain-envisioned security scheme using post quantum lattice-based aggregate signature for internet of drones applications,” *IEEE Trans. Veh. Technol.*, vol. 72, no. 8, pp. 10393–10408, Aug. 2023, doi: 10.1109/TVT.2023.3260579.

[19] D. Dharminder, C. B. Reddy, A. K. Das, Y. Park, and S. S. Jamal, “Post-quantum lattice-based secure reconciliation enabled key agreement protocol for IoT,” *IEEE Internet Things J.*, vol. 10, no. 3, pp. 2680–2692, Feb. 2023.

[20] D. Dharminder, A. K. Das, S. Saha, B. Bera, and A. V. Vasilakos, “Post-quantum secure identity-based encryption scheme using random integer lattices for IoT-enabled AI applications,” *Secur. Commun. Netw.*, vol. 2022, 2022, Art. no. 5498058, doi: 10.1155/2022/5498058.

[21] P. Bagchi, B. Bera, A. K. Das, S. Shetty, P. Vijayakumar, and M. Karuppiah, “Post quantum lattice-based secure framework using aggregate signature for ambient intelligence assisted blockchain-based IoT applications,” *IEEE Internet Things Mag.*, vol. 6, no. 1, pp. 52–58, Mar. 2023.

[22] T. Mohanty, V. Srivastava, S. K. Debnath, A. K. Das, and B. Sikdar, “Quantum secure threshold private set intersection protocol for IoT-Enabled privacy preserving ride-sharing application,” *IEEE Internet Things J.*, vol. 11, no. 1, pp. 1761–1772, Jan. 2024, doi: 10.1109/JIOT.2023.3291132.

[23] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.

[24] R. Jain, C. A. Miller, and Y. Shi, “Parallel device-independent quantum key distribution,” *IEEE Trans. Inf. Theory*, vol. 66, no. 9, pp. 5567–5584, Sep. 2020.

[25] H. Abulkasim, B. Goncalves, A. Mashatan, and S. Ghose, “Authenticated secure quantum-based communication scheme in internet-of-drones deployment,” *IEEE Access*, vol. 10, pp. 94963–94972, 2022, doi: 10.1109/ACCESS.2022.3204793.

[26] Q. Wang, D. Wang, C. Cheng, and D. He, “Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices,” *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 1, pp. 193–208, Jan./Feb. 1, 2023, doi: 10.1109/TDSC.2021.3129512.

[27] Quantlr, “Quantum,” 2022, Quantum Cryptography In Real-World Applications. Accessed: Dec. 2022. [Online]. Available: https://quantlr.com/quantum/quantum-cryptography-in-real-world-applications

[28] R. Saha et al., “A blockchain framework in post-quantum decentralization,” *IEEE Trans. Serv. Comput.*, vol. 16, no. 1, pp. 1–12, Jan./Feb. 2023, doi: 10.1109/TSC.2021.3116896.

[29] D. Gottesman and I. Chuang, “Quantum Digital Signatures,” 2001, *arXiv:quant-ph/0105032*.

[30] S. Babu, R. Abdulhammed, K. Elleithy, and S. Babu, “Blind Digital Signature schemes with four particle entanglement states,” in *Proc. IEEE Long Island Syst., Appl. Technol. Conf.*, 2017, pp. 1–6.

[31] W. Zhang and Y. Huang, “Photonic energy-time entangement in quantum communications,” in *Proc. IEEE Int. Conf. Signal, Inf. Data Process.*, 2019, pp. 1–4.

[32] P. Ramanan, D. Li, and N. Gebraeel, “Blockchain-based decentralized replay attack detection for large-scale power systems,” *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 52, no. 8, pp. 4727–4739, Aug. 2022.

[33] B. Alangot, D. Reijsbergen, S. Venugopalan, P. Szalachowski, and K. S. Yeo, “Decentralized and lightweight approach to detect eclipse attacks on proof of work blockchains,” *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1659–1672, Jun. 2021.

[34] M. Saad et al., “Exploring the attack surface of blockchain: A comprehensive survey,” *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1977–2008, thirdquarter 2020.

[35] G. Ebrahimpour, M. S. Haghighi, and M. Alazab, “Can blockchain be trusted in industry 4.0? Study of a novel misleading attack on bitcoin,” *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8307–8315, Nov. 2022.

[36] S. Feng, W. Wang, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang, “On cyber risk management of blockchain networks: A game theoretic approach,” *IEEE Trans. Serv. Comput.*, vol. 14, no. 5, pp. 1492–1504, Sep./Oct. 2021.

[37] synopsys, “Blockchain,” 2022, Blockchain explained. Accessed: Dec. 5, 2022. [Online]. Available: https:https://www.synopsys.com/glossary/what-is-blockchain.html

[38] A. Vangala, A. K. Das, A. Mitra, S. K. Das, and Y. Park, “Blockchain-enabled authenticated key agreement scheme for mobile vehicles-assisted precision agricultural IoT networks,” *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 904–919, 2023.

[39] A. Vangala, A. K. Das, N. Kumar, and M. Alazab, “Smart secure sensing for IoT-based agriculture: Blockchain perspective,” *IEEE Sensors J.*, vol. 21, no. 16, pp. 17591–17607, Aug. 2021.

[40] A. Vangala, S. Roy, and A. K. Das, “Blockchain-based lightweight authentication protocol for IoT-enabled smart agriculture,” in *Proc. IEEE Int. Conf. Cyber- Phys. Social Intell.*, 2022, pp. 110–115.

[41] K. Park, J. Lee, A. K. Das, and Y. Park, “BPPS: Blockchain-enabled privacy-preserving scheme for demand-response management in smart grid environments,” *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 2, pp. 1719–1729, Mar./Apr. 2023.

[42] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, “Designing blockchain-based access control protocol in IoT-enabled smart-grid system,” *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5744–5761, Apr. 2021.

[43] M. Indushree, M. Raj, V. K. Mishra, R. Shashidhara, A. K. Das, and V. Bhat, “Mobile-chain: Secure blockchain based decentralized authentication system for global roaming in mobility networks,” *Comput. Commun.*, vol. 200, pp. 1–16, 2023.

[44] P. Tekchandani, I. Pradhan, A. K. Das, N. Kumar, and Y. Park, “Blockchain-enabled secure Big Data analytics for Internet of Things smart applications,” *IEEE Internet Things J.*, vol. 10, no. 7, pp. 6428–6443, Apr. 2023.

[45] A. Mitra, B. Bera, A. K. Das, S. S. Jamal, and I. You, “Impact on blockchain-based AI/ML-enabled Big Data analytics for cognitive Internet of Things environment,” *Comput. Commun.*, vol. 197, pp. 173–185, 2023.

[46] M. Wazid, A. K. Das, and S. Shetty, “BSFR-SH: Blockchain-enabled security framework against ransomware attacks for smart healthcare,” *IEEE Trans. Consum. Electron.*, vol. 69, no. 1, pp. 18–28, Feb. 2023.

[47] S. K. Dwivedi, R. Amin, A. K. Das, M. T. Leung, K.-K. R. Choo, and S. Vollala, “Blockchain-based vehicular ad-hoc networks: A comprehensive survey,” *Ad Hoc Netw.*, vol. 137, 2022, Art. no. 102980.

[48] V. Srivastava, S. K. Debnath, B. Bera, A. K. Das, Y. Park, and P. Lorenz, “Blockchain-envisioned provably secure multivariate identity-based multi-signature scheme for Internet of Vehicles environment,” *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 9853–9867, Sep. 2022.

[49] M. Wazid, B. Bera, A. K. Das, S. P. Mohanty, and M. Jo, “Fortifying smart transportation security through public blockchain,” *IEEE Internet Things J.*, vol. 9, no. 17, pp. 16532–16545, Sep. 2022.

[50] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, “Design of blockchain-based lightweight V2I handover authentication protocol for VANET,” *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 1346–1358, May/Jun. 2022.

[51] M. Wazid, A. K. Das, R. Hussain, N. Kumar, and S. Roy, “BUAKA-CS: Blockchain-enabled user authentication and key agreement scheme for crowdsourcing system,” *J. Syst. Architecture*, vol. 123, 2022, Art. no. 102370.

[52] A. K. Das, B. Bera, S. Saha, N. Kumar, I. You, and H.-C. Chao, “AI-Envisioned blockchain-enabled signature-based key management scheme for industrial cyber-physical systems,” *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6374–6388, May 2022.

[53] B. Bera, D. Chattaraj, and A. K. Das, “Designing secure blockchain-based access control scheme in IoT-enabled internet of drones deployment,” *Comput. Commun.*, vol. 153, pp. 229–249, 2020.

[54] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 9097–9111, Aug. 2020.

[55] B. Bera, A. K. Das, and A. K. Sutrala, "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in internet of drones environment," *Comput. Commun.*, vol. 166, pp. 91–109, 2021.

[56] B. Bera, A. K. Das, S. Garg, M. Jalil Piran, and M. S. Hossain, "Access control protocol for battlefield surveillance in drone-assisted IoT environment," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2708–2721, Feb. 2022.

[57] B. Bera, M. Wazid, A. K. Das, and J. J. P. C. Rodrigues, "Securing internet of drones networks using AI-envisioned smart-contract-based blockchain," *IEEE Internet Things Mag.*, vol. 4, no. 4, pp. 68–73, Dec. 2021.

[58] M. Wazid, B. Bera, A. K. Das, S. Garg, D. Niyato, and M. S. Hossain, "Secure communication framework for blockchain-based Internet of Drones-enabled aerial computing deployment," *IEEE Internet Things Mag.*, vol. 4, no. 3, pp. 120–126, Sep. 2021.

[59] M. Fahmideh et al., "Engineering blockchain-based software systems: Foundations, survey, and future directions," *ACM Comput. Surv.*, vol. 55, no. 6, pp. 1–44, 2022, doi: 10.1145/3530813.

[60] A. Karakaya and A. Ulu, "A review on latest developments in post-quantum based secure blockchain systems," in *Proc. IEEE 11th Int. Symp. Digit. Forensics Secur.*, 2023, pp. 1–6.

[61] P. Thanalakshmi, A. Rishikhesh, J. Marion Marceline, G. P. Joshi, and W. Cho, "A quantum-resistant blockchain system: A comparative analysis," *Mathematics*, vol. 11, no. 18, 2023, Art. no. 3947. [Online]. Available: https://www.mdpi.com/2227-7390/11/18/3947

[62] C. Li, Y. Xu, J. Tang, and W. Liu, "Quantum blockchain: A decentralized, encrypted and distributed database based on quantum mechanics," *J. Quantum Comput.*, vol. 1, no. 2, pp. 49–63, 2019.

[63] F. Loukil, C. Ghedira-Guegan, K. Boukadi, A.-N. Benharkat, and E. Benkhelifa, "Data privacy based on IoT device behavior control using blockchain," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–20, 2021.

[64] M. A. Serrano, J. A. Cruz-Lemus, R. Perez-Castillo, and M. Piattini, "Quantum software components and platforms: Overview and quality assessment," *ACM Comput. Surv.*, vol. 55, no. 8, pp. 1–31, 2022, doi: 10.1145/3548679.

[65] J. Xu, C. Wang, and X. Jia, "A survey of blockchain consensus protocols," *ACM Comput. Surv.*, vol. 55, no. 13s, pp. 1–35, 2023, doi: 10.1145/3579845.

[66] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[67] M. R. Rahman, R. Mahdavi-Hezaveh, and L. Williams, "What are the attackers doing now? automating cyberthreat intelligence extraction from text on pace with the changing threat landscape: A survey," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–36, 2022, doi: 10.1145/3571726.

[68] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[69] Y. Bakos, H. Halaburda, and C. Mueller-Bloch, "When permissioned blockchains deliver more decentralization than permissionless," *Commun. ACM*, vol. 64, no. 2, pp. 20–22, 2021.

[70] Q. Wang, J. Yu, S. Chen, and Y. Xiang, "SoK: DAG-based blockchain systems," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–38, 2022, doi: 10.1145/3576899.

[71] S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed IoT network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021.

[72] M. Wazid, B. Bera, A. K. Das, and D. P. Singh, "IoT and blockchain technology-based healthcare monitoring," in *Blockchain in Digital Healthcare*, A. D. Borah, and R. M. Visconti, and G. C. Deka, Eds. London, U.K.: Chapman and Hall/CRC, 2021.

[73] "How will quantum technologies change cryptography?," 2022. Accessed: Dec. 10, 2022. [Online]. Available: https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography

[74] Q. Zhou and S. Lu, "Hash function based on controlled alternate quantum walks with memory (September 2021)," *IEEE Trans. Quantum Eng.*, vol. 3, 2022, Art. no. 3100310.

[75] H. Wang, G. Yao, and B. Wang, "A quantum concurrent signature scheme based on the quantum finite automata signature scheme," in *Proc. IEEE 14th Int. Conf. Anti-Counterfeiting, Secur., Identification*, 2020, pp. 125–129, doi: 10.1109/ASID50160.2020.9271729.

[76] M. Lucamarini, J. F. Dynes, B. Fröhlich, Z. Yuan, and A. J. Shields, "Security bounds for efficient decoy-state quantum key distribution," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, May/Jun. 2015, Art. no. 6601408.

[77] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Cost-efficient quantum key distribution (QKD) over WDM networks," *J. Opt. Commun. Netw.*, vol. 11, no. 6, pp. 285–298, 2019.

[78] M. Ghalaii, C. Ottaviani, R. Kumar, S. Pirandola, and M. Razavi, "Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 506–516, Mar. 2020.

[79] J.-Y. Liu et al., "Boosting the performance of reference-frame- independent measurement-device-independent quantum key distribution," *J. Lightw. Technol.*, vol. 39, no. 17, pp. 5486–5493, Sep. 2021.

[80] M. Y. Al-Darwbi, A. A. Ghorbani, and A. H. Lashkari, "QKeyShield: A practical receiver-device-independent entanglement-swapping-based quantum key distribution," *IEEE Access*, vol. 10, pp. 107685–107702, 2022.

[81] X. Yu et al., "Secret-key provisioning with collaborative routing in partially-trusted-relay-based quantum-key-distribution-secured optical networks," *J. Lightw. Technol.*, vol. 40, no. 12, pp. 3530–3545, Jun. 2022.

[82] M. Shafieinejad and R. Safavi-Naini, "A post-quantum one time signature using bloom filter," in *Proc. IEEE 15th Annu. Conf. Privacy, Secur. Trust*, 2017, pp. 397–3972.

[83] T. Peacock, P. Y. Ryan, S. Schneider, and Z. Xia, "Verifiable voting systems," in *Computer and Information Security Handbook*, 3rd ed., J. R. Vacca, Ed. Boston, MA, USA: Morgan Kaufmann, 2013, ch. e90, pp. e293–e315.

[84] P. Zhang, H. Jiang, Z. Zheng, P. Hu, and Q. Xu, "A new post-quantum blind signature from lattice assumptions," *IEEE Access*, vol. 6, pp. 27251–27258, 2018, doi: 10.1109/ACCESS.2018.2833103.

[85] F. Shahid, I. Ahmad, M. Imran, and M. Shoaib, "Novel one time signatures (NOTS): A compact post-quantum digital signature scheme," *IEEE Access*, vol. 8, pp. 15895–15906, 2020.

[86] L. Wang, C. Huang, and H. Cheng, "Quantum attack-resistant signature scheme from lattice cryptography for WFH," in *Proc. IEEE 2nd Int. Conf. Big Data, Artif. Intell. Internet Things Eng.*, 2021, pp. 868–871.

[87] D. Li, J. Zhang, F.-Z. Guo, W. Huang, Q.-Y. Wen, and H. Chen, "Discrete-time interacting quantum walks and quantum Hash schemes," *Quantum Inf. Process.*, vol. 12, no. 3, pp. 1501–1513, 2013.

[88] F. Ablayev and A. Vasiliev, "Quantum hashing," 2013, *arXiv: 1310.4922*.

[89] Y.-G. Yang, P. Xu, R. Yang, Y.-H. Zhou, and W.-M. Shi, "Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption," *Sci. Rep.*, vol. 6, no. 1, 2016, Art. no. 19788.

[90] K. A. S. Al-Khateeb, M. M. Saeb, M. M. A. Majeed, and M. R. Wahiddin, "A secure protocol using 6DP for quantum authentication and hash functions for key distribution (KDP-6DP)," in *Proc. IEEE Int. Conf. Comput. Commun. Eng.*, 2010, pp. 1–4, doi: 10.1109/ICCE.2010.5556781.

[91] C. Lin, D. He, S. Zeadally, X. Huang, and Z. Liu, "Blockchain-based data sharing system for sensing-as-a-service in smart cities," *ACM Trans. Internet Technol.*, vol. 21, no. 2, pp. 1–21, 2021.

[92] L. Tan, N. Shi, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchain-empowered access control framework for smart devices in green Internet of Things," *ACM Trans. Internet Technol.*, vol. 21, no. 3, pp. 1–20, 2021.

[93] M. Wazid and P. Gope, "BACKM-EHA: A novel blockchain-enabled security solution for IoMT-based e-healthcare applications," *ACM Trans. Internet Technol.*, vol. 23, no. 3, pp. 1–28, 2022.

[94] A. L. Martínez, M. G. Pérez, and A. Ruiz-Martínez, "A comprehensive review of the state of the art on security and privacy issues in healthcare," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–38, 2022, 2023, doi: 10.1145/3571156.

MOHAMMAD WAZID (Senior Member, IEEE) received the Master of Technology degree in computer network engineering from Graphic Era University, Dehradun, India, and the Ph.D. degree in computer science and engineering from the International Institute of Information Technology, Hyderabad, India. He is currently a Professor with the Department of Computer Science and Engineering, Graphic Era University. He is the Head of the cybersecurity and IoT Research Group, Graphic Era University. He has authored or coauthored more than 130 papers in international journals and conferences in his research areas which include security, remote user authentication, the Internet of Things, and cloud computing. He was the recipient of the University Gold Medal and the Young Scientist Award from UCOST, the Department of Science and Technology, Government of Uttarakhand, India. He is an Associate Editor for IEEE INTERNET OF THINGS JOURNAL and IET/WILEY COMMUNICATIONS JOURNAL.

ASHOK KUMAR DAS (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering, the M.Tech. degree in computer science and data processing, and the M.Sc. degree in mathematics from IIT Kharagpur, Kharagpur, India. He is currently a Full Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology Hyderabad, Hyderabad, India, and also a Visiting Research Professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA, USA. His Google Scholar H-index is 86 and i10-index is 256 with more than 21,200 citations. He has authored more than 415 papers in international journals and conferences in his research areas which include cryptography, system and network security including security in smart grid, Internet of Things, Internet of Drones, Internet of Vehicles, cyber-Physical Systems and cloud computing, intrusion detection, blockchain, AI/ML security, and post-quantum cryptography, including more than 350 reputed journal papers. He was the recipient of the Institute Silver Medal from IIT Kharagpur. He has been listed in the Web of Science (Clarivate^{TM}) Highly Cited Researcher 2022 and 2023 in recognition of his exceptional research performance. He was/is on the editorial board of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE SYSTEMS JOURNAL, JOURNAL OF NETWORK AND COMPUTER APPLICATIONS, and COMPUTER COMMUNICATIONS.

YOUNGHO PARK (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering, Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively. He is currently a Professor with the School of Electronics Engineering, Kyungpook National University. During 1996–2008, he was a Professor with the School of Electronics and Electrical Engineering, Sangju National University, Korea. During 2003–2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR, USA. His research interests include computer networks, multimedia, and information security.