Quantum-Resistant Secure Communication Protocol for Digital Twin-Enabled Context-Aware IoT-Based Healthcare Applications

Basudeb Bera, Ashok Kumar Das, *Senior Member, IEEE*, Biplab Sikdar, *Fellow, IEEE*

***Abstract*—Digital Twins (DTs) play a crucial role in context-aware Internet of Things (IoT) applications within the healthcare sector, including the industrial healthcare domain, by facilitating the continuous sharing of sensitive and confidential patient data from physical objects in real time. This shared data is essential for treatment planning and decision-making processes, often being accessed remotely by authorized users. However, traditional security mechanisms, which rely on the integer factorization problem (IFP) and the elliptic curve discrete logarithm problem (ECDLP), are vulnerable to quantum attacks using algorithms like Shor's, posing significant risks to data protection. As a result, the healthcare sector faces several security challenges, including the vulnerability of sensitive patient data to cyberattacks, quantum threats, the risk of unauthorized access to medical devices and IoT systems, and the increasing sophistication of cybercriminals exploiting weak authentication methods. To address these issues, we propose a quantum-resistant protocol that safeguards data privacy in DT-enabled IoT healthcare applications, ensures secure transmission of information, maintains patient trust, supports long-term data confidentiality, and protects medical devices and IoT systems from potential breaches. By employing lattice-based cryptographic techniques, particularly the ring learning with errors (RLWE) problem, the proposed scheme effectively addresses contemporary security challenges, including those posed by quantum computing. Real-time experiments conducted on Raspberry Pi 4 devices, along with computational overhead analysis, demonstrate the protocol's efficiency. Additionally, formal security validation using the Scyther tool and security analysis with the RoR model reinforce the robustness of the proposed protocol. A comprehensive comparative evaluation against existing schemes highlights its lightweight, scalable, and efficient nature. Furthermore, performance evaluations in the context of unknown attacks show that the proposed scheme significantly outperforms current alternatives in terms of effectiveness.**

***Index Terms*—Quantum-resistant, security, digital twin, testbed, Scyther, healthcare, IoT.**

I. Introduction

A. Background

A digital twin (DT) is a computer-generated replica of a real-world physical system, entity, process, or abstraction. It is created and operated by computer programs or specialized software models, acting as a digital counterpart that interacts and synchronizes with its physical peer. The primary goal of a DT is to collaboratively enhance the efficiency and cost-effectiveness of a system or overall process. This involves leveraging a range of emerging technologies such as virtual modeling, simulation technologies, edge computing, and cloud computing, along with optimization tools [1]. DTs enable proactive analysis of physical processes through diverse simulation tools like OpenSim [2], GENIX [3], others, and employ technologies like artificial intelligence (AI), machine learning (ML), mathematical optimization, and others. The DT is employed not just for creating a virtual replica of a system's intricate operations but also for examining its present state, forecasting future behavior, and enhancing control optimization using the aforementioned technologies [4].

The exploration of conventional DT applications in healthcare traces back to 2014 with the introduction of the SIMULIA living heart project by Dassault Systemes [5]. This pioneering project marked the creation of the first DT of the human heart, faithfully replicating the functions of an actual heart. The success of this initiative demonstrated the substantial impact of DT technology on cardiac disease research and treatment. Researchers across diverse domains have been motivated to delve into the considerable potential of DTs in healthcare. DT in the healthcare sector offers substantial support in remote monitoring, diagnostics, prescription, surgical procedures, and rehabilitation. This capability serves to alleviate the considerable strain on conventional healthcare systems.

As the Internet of Things (IoT) expands its presence in the healthcare system, the multitude of smart devices has the potential to be represented as DTs. The integration of DTs into healthcare is poised to revolutionize the landscape of digital healthcare, introducing unprecedented advancements. The wealth of data emanating from interconnected DTs can be consolidated to extract comprehensive insights across a diverse array of physical entities (PEs), including but not limited to smart biosensors, thermometers, inhalers, smartwatches, fitness trackers (such as FitBits), ECG monitors, and blood pressure monitors. Subsequently, DTs empower healthcare professionals to remotely monitor vital signs, track medication adherence, and assess other pertinent metrics, eliminating the necessity for in-person visits [6].

In the realm of a context-aware IoT within the healthcare system, DTs actively collect real-time patient information that extends beyond fundamental details like age, gender, and ethnicity. This encompassing dataset incorporates personal-

Basudeb Bera is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583 (e-mail: b.bera26@nus.edu.sg).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India (e-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in). *(Corresponding author: Ashok Kumar Das)*

Biplab Sikdar is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583 (e-mail: bsikdar@nus.edu.sg).

ized elements such as genomic information, metabolomics, environmental factors, occupation, activities, habits (including travel frequency), and lifestyle choices (such as smoking, drinking, and dietary preferences). Additionally, it encompasses patient-specific data derived from medical examinations and the use of drugs, along with information gleaned from smart devices. Integrating and analyzing this diverse dataset aids in identifying and elucidating symptoms. Through the utilization of advanced technologies like machine learning and artificial intelligence, DTs can offer a holistic perspective of health, encompassing historical disease records, current health status, and potential future health risks [7], [8].

Healthcare information is predominantly sensitive, private, and confidential. Moreover, it is often both delay-sensitive and mission-critical. These data are exchanged through either wired or wireless networks, utilizing public channels that are inherently insecure [7]. Patient data associated with DTs traverses diverse networks, software, and applications throughout its lifecycle for service provision, posing challenges for comprehensive security measures and establishing trust across the entire process. Ensuring the synchronization of a digital replica encompassing physical objects, patients, systems, and entities, the personal data collected through pervasive IoT devices introduces potential avenues for criminal activities and misuse of private information.

In healthcare applications, Digital Twins (DTs) face several critical issues related to data security and privacy. The continuous sharing of sensitive patient data between physical objects and its digital representations exposes healthcare systems to significant cybersecurity risks, including potential unauthorized access to medical records and devices. Furthermore, medical IoT devices, which are integral to DTs, often suffer from weak authentication mechanisms, making them susceptible to cyberattacks. The increasing sophistication of cybercriminals also exacerbates these risks, as they exploit vulnerabilities in legacy security protocols. As healthcare systems become more interconnected and reliant on DTs for real-time monitoring, treatment planning, and decision-making, the need for robust, future-proof security solutions to address these vulnerabilities and protect patient data becomes increasingly urgent. The potential for data breaches, system manipulation, and privacy violations presents a growing challenge in the safe integration of DTs within healthcare. In a study by Wang et al. [6], the DT approach raises concerns regarding data security and privacy protection, including data quality and integrity. The research also identifies various attacks within this framework, including eavesdropping, message flooding, man-in-the-middle attacks, data tampering, data poisoning, semantic adversarial attacks, and semantic knowledge poisoning attacks.

B. Motivation

In the context-aware IoT in healthcare, DT-related data plays a pivotal role as the essence of the treatment process and as a critical component in the decision-making process, utilizing AI/ML techniques. Therefore, it is imperative that this data is not only authentic but also of high quality. If the data turns malicious, the AI/ML models may generate incorrect predictions, potentially impacting decision-making in the treatment plan. In a worst-case scenario, this misinformation could lead to patient harm, including fatalities due to mispredictions. Mitra et al. [9] have highlighted a significant impact on the decision-making process in the presence of a data poisoning attack. IBM Data Breach Cost Report in 2023 [10] highlighted that the average cost of a data breach across various industries stood at USD 4.45 million. Notably, the healthcare sector incurred the highest average cost for a data breach, reaching USD 10.93 million. This reflects a substantial increase of 53.3% in healthcare data breach costs over the past three years.

Traditional public-key cryptographic techniques, such as Rivest-Shamir-Adleman (RSA), Diffie-Hellman key exchange, and elliptic curve-based cryptography (ECC), rely on the computational complexity of problems like the integer factorization problem (IFP), discrete logarithm problem (DLP), and elliptic curve discrete logarithm problem (ECDLP). For decades, these techniques and various other security protocols, including authentication [11]–[13], key agreement [12], [14], [15], and access control [16], [17], have relied on the computational complexity of problems such as IFP, DLP, and ECDLP to address the aforementioned security challenges. Shor demonstrated that quantum computers can efficiently solve the IFP and DLP using Shor's algorithm [18]. Quantum algorithms, such as Grover's search algorithm [19], offer substantial speedup for analogous problems. Additional examples encompass quantum algorithms utilizing the quantum Fourier transform [20], quantum walks for solving search problems, and adiabatic quantum computing for optimizing problems. These developments give rise to security threats for these security protocols, prompting a need to explore new approaches in designing security protocols.

In the present scenario, the most significant concern arises from security threats in healthcare applications due to the aforementioned developments. To mitigate the security threats in the healthcare system within the quantum scenario, our motivation is to design quantum-resistant secure communication integrated with digital twins for context-aware IoT in healthcare.

C. Research Contributions

The primary contributions of this paper can be outlined as follows.

- **Enhanced Security Features:**
    1) *Quantum-Resistant Security:* The scheme utilizes RLWE hardness to ensure secure, quantum-resistant communication for DT-enabled IoT in healthcare, maintaining real-time data synchronization amidst threats.
    2) *Robust Security Guarantees:* Proven to be accurate and resilient against a variety of active and passive attacks, including those in quantum scenarios.
- **Technical Advantages:**
    1) *Formal Security Validation:* Verified for robustness using the Scyther tool, confirming its security against numerous attacks.

2) *Efficient Computation:* Tested on "Raspberry Pi 4 (model B)" devices, showing effective performance with minimal computational impact.

- **Innovative Aspects:**
  1) *Context-Aware Design:* Tailored for DT-enabled IoT healthcare applications, ensuring effective synchronization and security in dynamic environments.
  2) *Lightweight and Scalable:* Demonstrated as both lightweight and scalable, making it suitable for real-world use.
- **Experimental Validation:**
  1) *Real-Time Testing:* Validated in practical experiments, proving the protocol's effectiveness and feasibility on actual hardware.
  2) *Superior Performance:* Outperforms existing schemes significantly, especially under unknown attacks, as shown in comparative assessments.

D. Paper Organization

In the upcoming Section II, we discuss the existing literature in IoT-based healthcare and its related applications. Section III introduces the mathematical foundations essential for developing our proposed scheme, while Section IV provides a comprehensive exploration of the various phases within our scheme. Moving forward, Section V-B offers a formal security verification of our proposed scheme using the Scyther tool, followed by Section V-C, which conducts an informal security analysis to illustrate the scheme's resilience against various active and passive attacks, including quantum attacks. The real-time testbed experiments involving various cryptographic primitives and the ensuing comparison with existing schemes are detailed in Section VI and Section VII, respectively. Lastly, Section VIII encapsulates our concluding remarks on the proposed scheme.

II. Related works

In 2020, Li et al. [14] proposed an ECC-based user authentication scheme for wireless medical sensor networks. In their scheme, users can access sensory data from a sensor node through a gateway node by establishing a session key between them. Unfortunately, the session key they generated is susceptible to ephemeral secret leakage (ESL) attacks under the CK-adversary model, as it is generated using public information and a short-term random nonce. Wang et al. [21] proposed a key agreement protocol for smart healthcare applications. In this protocol, users, acting as patients with resource-limited smart medical devices, collect and upload health data to the associated edge server by negotiating a session key. However, Chang et al. [22] showed that Wang et al.'s scheme fails to ensure privacy and is vulnerable to Denial-of-Service (DoS) attacks. Zhang et al. [23] devised a user authentication protocol for the Internet of Drones (IoD). They incorporated FourQ curves along with the Boyko-Peinado-Venkatesan (BPV) pre-calculation techniques to enhance data confidentiality. However, their protocol displays significant drawbacks, including high computational and communication burdens, vulnerability to replay attacks, and a deficiency in user anonymity, as highlighted by the findings of Park et al. [24]. Dabra et al. [25] designed an anonymous authentication and key exchange scheme for mobile devices, aiming to address the previously mentioned concerns. However, their scheme lacks effectiveness in guarding against replay attacks and ensuring untraceability. Following this, Ding et al. [26] demonstrated that the reuse of the master key renders it vulnerable to signal leakage attacks.

In 2021, Yuanbing et al. [27] devised a key agreement and authentication protocol for smart healthcare utilizing a wireless medical sensor network. In their approach, a user establishes a connection with a sensor node via a gateway node by negotiating a session key, constructed based on ECC and a hash function. However, their scheme lacks robust security for the session key, as it is generated using public information, random numbers, and identities. Moreover, Lee et al. [28] discovered several security vulnerabilities in their scheme, including susceptibility to smart card stolen attacks, offline ID/password guessing attacks, user impersonation attacks, sensor node impersonation attacks, man-in-the-middle attacks, sensor node capture attacks, and a failure to ensure user anonymity. In 2021, Islam and Basu [29] proposed a three-party authentication protocol tailored for mobile communication under a post-quantum framework, leveraging RLWE hardness. Their protocol involves mobile users disclosing their actual identities to establish secure connections with the authentication server. However, this method poses a risk by exposing users' real identities over the public channel, making it susceptible to attacks on user anonymity and lacking support for the property of untraceability. Masud et al. [30] designed a user authentication mechanism for IoT-based healthcare systems. In their scheme, a doctor can verify authenticity and establish a session key with a IoT sensor node integrated into the medical device, allowing them to monitor real-time healthcare information. This scheme does not provide security against replay attacks. Shihab and Riham [31] have identified several serious security flaws in their scheme, including susceptibility to long-term secret disclosure attacks, session key disclosure attacks, lack of forward secrecy, and vulnerability to desynchronization attacks.

In 2023, Qiao et al. [32] proposed a key agreement scheme for IoT-enabled healthcare applications, where a fog server serves as a gateway node for exchanging information between a cloud server and a user. Their scheme utilizes Chebyshev chaotic maps and a hash functions to generate a session key. However, the session key is constructed based on public information, making it vulnerable to ESL attacks under the CK-adversary model. Zhang et al. [33] proposed a user authentication and key agreement scheme for IoT-based e-healthcare systems. In their model, a user, acting as a patient equipped with a smart card, engages in mutual authentication with a trusted server and a medical server. Subsequently, they establish a session key using a cryptographic hash function. Regrettably, their scheme does not provide support against replay attacks. Huang et al. [34] designed an architecture for the mutual authentication and a key establishment framework relying on computational hardness of ECC in healthcare

TABLE I
CRYPTOGRAPHIC METHODS, ADVANTAGES AND LIMITATIONS OF EXISTING SCHEMES IN IOT-BASED CE ENVIRONMENTS

Scheme	Year	Cryptographic methods	Advantages	Drawbacks/Limitations
Li et al. [14]	2020	* BCH code & hash functions * ECC point operations	* Authentication * Key agreement	* ESL attack under the CK-adversary model * Vulnerable to quantum attack
Wang et al. [21]	2021	* One-way hash function * ECC point operations	* Authentication * Key agreement	* Fails to ensure privacy * Vulnerable to Denial-of-Service (DoS) attacks
Zhang et al. [23]	2021	* Cryptographic hash function * Symmetric key encryption/decryption * HMAC	* Authentication * Key establishment	* Cannot resist replay attack * Fails to provide user anonymity
Dabra et al. [25]	2021	* One-way hash function * RLWE hardness	* Authentication * Key agreement	* Cannot resist replay & signal leakage attacks * Fail to ensure untraceability
Yuanbing et al. [27]	2021	* One-way hash function * ECC point operations	* Authentication * Key management	* Susceptible to smart card stolen & impersonation attacks * Offline ID/password guessing & MiTM attacks * Susceptible to node capture attacks & lack of anonymity
Qiao et al. [32]	2023	* One-way hash function * Chebyshev polynomial * Symmetric key encryption/decryption	* Authentication * Key management	* Vulnerable to ESL attack under the CK-adversary model
Zhang et al. [33]	2023	* Symmetric key encryption/decryption, * One-way hash function	* Authentication * Key agreement	* Vulnerable to replay attack * Does not support dynamic drone addition
Huang et al. [34]	2023	* One-way hash function * ECC point multiplications * Symmetric key decryption	* Authentication * Key management	* Vulnerable to ESL attack under the CK-adversary model
Wang et al. [35]	2023	* One-way hash function * ECC point multiplications	* Authentication * Key management	* Vulnerable to ESL attack under the CK-adversary model * Susceptible to replay attack
Mishra et al. [36]	2023	* One-way hash function * RLWE hardness	* Authentication * Key management	* Susceptible to anonymity and untraceability
Rewal et al. [37]	2023	* One-way hash function * RLWE hardness	* Authentication * Key management	* Fail to resist user anonymity and untraceability * Lack of scalability

application. Following mutual authentication, the cloud server has the capability to delegate the remaining verification tasks to fog nodes. The fog nodes, in turn, are entrusted with the responsibility of authenticating the device and distributing the established session key. In their scheme, the session key between the sensor device and fog node is generated using public information, random numbers, and identities. This renders it vulnerable to ESL attacks under the CK-adversary model. In 2023, Wang et al. [35] devised an authentication and key agreement scheme for cloud-assisted IoT applications. In their proposed model, IoT devices, users, gateway nodes, and cloud centers mutually authenticate each other before establishing a session key. The session key is constructed using a hash function and ECC, with random numbers and public parameters employed in its generation, rendering it vulnerable to ESL attacks under the CK-adversary model. Additionally, their scheme is unable to resist replay attacks.

In 2023, Mishra et al. [36] proposed a communication mechanism for the IoD designed to withstand scalable quantum computers. However, the true identities of the communicating parties become revealed through the public communication channel, rendering this scheme susceptible to concerns related to anonymity and untraceability. In 2023, Rewal et al. [37] suggested an authentication scheme grounded in the ring learning with errors (RLWE) lattice assumption, tailored for mobile communication in a post-quantum setting. However, their scheme exposes the actual identities of mobile users over the communication channel, leading to an incapacity to ensure "user anonymity and untraceability." Additionally, the scheme does not offer support for the dynamic addition of devices, resulting in a lack of scalability.

A recent development presented by Ghaemi et al. [38] provides a solution to address the security challenges posed by quantum computing and blockchain in cross-industry communications. Their technical contribution lies in the development of a quantum-resilient authentication protocol for IIoT machines, which eliminates the need for intermediary servers. This protocol integrates blockchain technology with self-certification mechanisms to enhance security, integrity, and efficiency across diverse industries. It enhances efficiency, showing 13% and 91% improvements in communication and computation overheads, respectively, compared to existing protocols. Abbasinezhad-Mood et al. [39] presented a security method to enhancing security and efficiency in vehicle-to-vehicle (V2V) communications. By integrating blockchain technology with a dual-signature mechanism, the protocol addresses key challenges related to anonymity and cross-domain authentication in multi-domain Internet of Vehicles (IoV) environments. The protocol employs dual signatures (one from the sender and one from the receiver) to provide improved authentication and integrity during key exchange, ensuring tamper-proof communication. Blockchain integration further ensures that the key-sharing process is decentralized, transparent, and resistant MiTM and replay attacks. The protocol supports efficient key management by reducing overhead and latency in real-time V2V communication, making it suitable for multi-domain IoV applications, such as autonomous driving and intelligent transportation systems.

Shahidinejad et al. [40] proposed blockchain-assisted charging scheduling scheme for vehicular edge networks uses the NanoPi NEO to improve the efficiency and security of electric vehicle (EV) charging. They utilized blockchain to ensure transparent, tamper-proof transactions, and anonymous communication between EVs and charging stations. Their system optimizes energy consumption, vehicle availability, and station load, while using cryptographic techniques to enhance security and privacy, making it ideal for resource-constrained environments and real-time edge-based charging applications. Ghaemi et al. [41] addressed significant limitations in existing roaming authentication protocols. By eliminating the need for

a home agent, their protocol enhances fault tolerance and reduces communication overhead, achieving a 37% decrease in message exchanges compared to traditional methods.

The summarized key differences between the proposed scheme and other existing related schemes, in terms of cryptographic methods, year, advantages, and limitations, are provided in Table I.

III. Preliminaries

Consider $\mathbb{Z}$ as the set of integers, and let $n \in \mathbb{Z}$ represent a security parameter. Furthermore, we denote $\mathbb{Z}[x]$ and $\mathbb{Z}_q[x]$ as the polynomial rings over $\mathbb{Z}$ and $\mathbb{Z}_q$, respectively. In $\mathbb{Z}_q[x]$, the coefficients of all polynomials are reduced modulo q, where $q \in \mathbb{Z}$ is large prime number. We define the polynomial quotient ring $\mathbb{R}$ as $\mathbb{R} = \frac{\mathbb{Z}[x]}{<x^n+1>}$, where $< x^n + 1 >$ stands for $mod(x^n + 1)$ and $(x^n + 1)$ as an irreducible polynomial (cyclotomic polynomial) over $\mathbb{Z}$ and $\mathbb{R}_q = \frac{\mathbb{Z}_q[x]}{<x^n+1>}$ with similar notion. Let χ_β denote a discrete Gaussian distribution over $\mathbb{R}_q$, with $\beta > 0$ is the standard deviation of χ_β.

Let $\mathbb{S} = \{-\lfloor \frac{q}{4} \rfloor, \cdots, \lfloor \frac{q}{4} \rfloor\}$ be a subset of $\mathbb{Z}_q = \{-\frac{q-1}{2}, \cdots, \frac{q-1}{2}\}$. Then, a characteristic function $Cha(\cdot)$ of the complement of $\mathbb{S}$ can be defined as:

$$Cha(x) = \begin{cases} 0, & \text{if } x \in \mathbb{S} \\ 1, & \text{if } x \notin \mathbb{S} \end{cases}. \tag{1}$$

The modular function $Mod_2 : \mathbb{Z}_q \times \{0,1\} \rightarrow \{0,1\}$ is defined as $Mod_2(u, v) = (u + v.\frac{(q-1)}{2}) \pmod q \pmod 2$, where $u \in \mathbb{Z}_q$ and $v = Cha(u)$ [42], [43].

Lemma 1. *Let s and t be arbitrary elements in $\mathbb{R}_q$, where q is an odd prime and $|t| < \frac{q}{8}$. If $a = s + 2 \cdot t$ and $e = Cha(s)$, then $Mod_2(s, e) = Mod_2(a, e)$ holds [42].*

The difficulty of the following mathematical problems is widely recognized, and these problems have been extensively employed to assess the security of numerous cryptographic protocols grounded in ideal lattices.

Definition 1 (Ring Learning With Error (RLWE))**.** *Consider a sample $S_{a,\chi_\beta} = (x, y)$ drawn from $\mathbb{R}_q \times \mathbb{R}_q$, where $a \leftarrow \mathbb{R}_q$ and $y = x \cdot a + e$, with $a \leftarrow \mathbb{R}_q$ and $e \leftarrow \chi_\beta$. The $RLWE(q, \beta)$ problem posits that distinguishing elements of A_{a,χ_β} from the uniform distribution on $\mathbb{R}_q \times \mathbb{R}_q$ in polynomial time is a challenging task for any adversary [44].*

Definition 2 (Pairing with Error (PWE) Problem)**.** *Consider a function $g : \mathbb{R}_q \times \mathbb{R}_q \rightarrow 0, 1$ defined as $g(x, s) = Mod_2(x \cdot s, Cha(x \cdot s))$, where $x, s \leftarrow \mathbb{R}_q$. The goal of the PWE problem is to ascertain $g(x, s)$ for the unknown values of $s, e \in \chi_\beta$, given $x, y, a \in \mathbb{R}_q$, where $y = a \cdot s + 2 \cdot e$ [45].*

Proof. Since the hardness of RLWE holds, we have $x = y \cdot s + 2e \approx_C u' + e$. Because the hardness of Ideal-BDD (Bounded Distance Decoding Problem) holds [46], we also have $u' + e \approx_C u''$, where $u', u'' \in \mathbb{R}_q$. Thus, PWE is hard. □

Definition 3 (Decision Pairing with Error (DPWE) Problem)**.** *With the provided values $x, y, u \in \mathbb{R}_q$, the objective of the DPWE problem is to discern whether (x, u) is uniformly random in $\mathbb{R}_q \times \mathbb{R}_q$. Here, $x = y \cdot s + 2e$ with the unknown values of $s, e \in \chi_\beta$ [44], [45].*

The RLWE problems can be efficiently transformed into the subsequent problems, indicating that if the PWE or DPWE problem can be effectively solved in polynomial time, it implies that the RLWE problem can also be solved by any quantum computer within polynomial time.

IV. QRSC-IoTH: Propose Scheme

In this section, we illustrate the various phases that constitute the proposed quantum-resistant secure communication for a digital twin-enabled context-aware IoT in the healthcare system, referred to as QRSC-IoTH.

A. Workflow of DTs with the QRSC-IoTH System

DT in our system is hosted on the medical server and continuously updated with real-time data from the smart medical device through QRSC-IoTH protocol described in Sec. IV-D3. This ensures secure, periodic data flow, reflecting the device's current state. The DT interacts bidirectionally with the device, allowing for real-time monitoring and feedback. We summarize the DT framework of the proposed scheme based on [47] and [48], which consists of the following components:

- *Creation of the DT:* In our system, DT is created and hosted on the medical server platform (for example, AWS, microsoft azure, or google cloud) using appropriate tools, such as azure digital twins, siemens digital twin, altair smartWorks, GE digital twin software, and so on.
- *Data Collection:* A DT requires medical data from its physical object, which is typically acquired through multiple sources from healthcare institutions, such as electronic health records (EHR), biomedical examinations, and medical images. The data is gathered at regular intervals and includes patient-specific health metrics (e.g., heart rate, blood pressure, and biomarker concentrations), sensor readings, and system performance indicators.
- *Interaction with the QRSC-IoTH System:* The DT on the medical server interacts with its physical counterpart through the proposed QRSC-IoTH protocol, which guarantees that data integrity is maintained. This protocol enables seamless real-time updates, allowing the DT to reflect the current state of the device. This interaction is bidirectional, meaning that changes or anomalies detected by the DT can trigger alerts or automatic actions in the physical medical device.
- *Nature of the DT:* The DT in our system is indeed a true digital twin, not merely an offline simulator. Unlike traditional simulation models, the DT is continuously updated based on real-time data from the physical system, ensuring that the virtual model accurately mirrors the behavior of its physical counterpart.
- *Computation:* Computation frameworks are essential in HDT to perform various tasks. Data must be accurately extracted, processed, securely transmitted, and executed using AI-driven techniques.

- *Data Management:* DT generates vast, heterogeneous, multi-scale, and noisy data from various sources, requiring efficient data management frameworks (for examle, Milvus vector database using vector similarity search technique) for building and evolving the its virtual representation.
- *Data Analysis and Decision Making:* Use tools like Azure machine learning, Amazon SageMaker, or IBM AIOps solutions to analyze patient data. These tools can process incoming health data, compare it against historical patterns, and predict potential health risks (e.g., detecting early signs of a heart attack from ECG data). Based on DT data, automated decision support systems (e.g., alerting doctors or triggering emergency responses) can be set up.

Here, we focus solely on designing secure communication between medical devices and their digital twins installed on the medical server. Data from the devices are synchronized through our secure communication protocol.

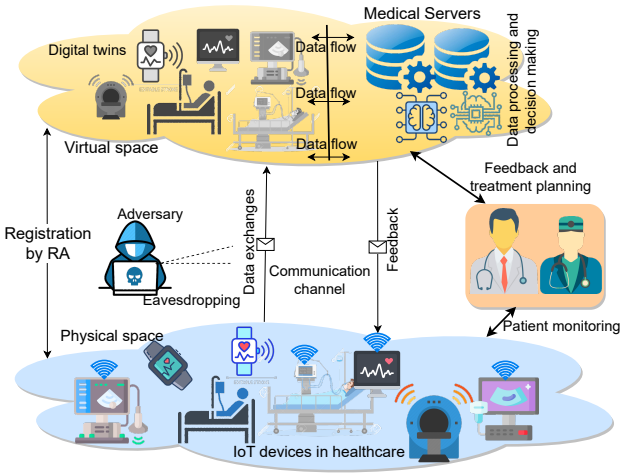

Fig. 1. DT architecture for context-aware IoT in healthcare.

B. Network Architecture

The proposed framework for context-aware IoT in smart healthcare is built upon physical entities existing in physical space, digital twins representing their virtual counterparts in the software realm of virtual/cyber space, and communication links connecting both virtual and physical spaces through input big data and output feedback. The PEs in the physical space encompass medical IoT sensors (MDs), such as wearable devices, attached to a patient's body, responsible for real-time data collection of patient information. In the virtual space, the DTs are virtual representations of their corresponding physical entities. These DTs are instantiated by a computer program or software model deployed within a medical server (MS), interacting and synchronizing with their physical counterparts in real-time through the MS. A fully trusted Registration Authority (RA) serves the purpose of registering MDs through MS in the smart healthcare system. Following a successful registration through a secure channel or offline mode, MDs and MS are deployed in their respective application areas, where they actively perform their functions. The communication link enables real-time data transmission between the DTs and their corresponding PEs. Beyond providing instant visualization of the status of the PEs, DTs also facilitate proactive operations for their physical counterparts, enabling intelligent services such as 3-D simulation, preventive maintenance, and informed decision-making. For example, DTs of MDs attached to a patient can acquire information about the patient's condition. Doctors can access this information remotely by logging into the MS and subsequently devise a treatment plan accordingly. Figure 1 demonstrates the DT architecture for context-aware IoT in healthcare.

C. Security Threats

In the proposed scheme, MDs synchronize their real-time healthcare information with their DTs through MS via a communication link. This communication occurs over a wireless or wired medium, which is a public channel. Since the public channel is not secure, MDs share patient information with the MS by establishing a secret key called a session key. Therefore, if the session key is not secure enough under quantum computing, this sensitive information may be breached by an adversary $\mathcal{A}$ for misuse. We consider widely-adopted security models to construct the session key over the insecure channel, such as Dolev-Yao (DY) [49], Canetti and Krawczyk (CK) [50], and the extended CK-adversary (eCK) models [51], [52]. In the DY adversary model, $\mathcal{A}$ has the capability to eavesdrop on communication messages and can modify, delete, or inject false content into the communication channel. On the other hand, within the CK-adversary model, $\mathcal{A}$ acquires heightened abilities by seizing control of the communicated messages. As a result, $\mathcal{A}$ can not only delete, modify, or insert fake content but can also reveal both short-term and long-term secrets essential for constructing the session key, achieved by compromising a session state. While the eCK adversary model shares its roots with the CK adversary model, it extends beyond by granting $\mathcal{A}$ additional powers and capabilities, making it a more formidable adversary than the traditional CK model. These added capabilities may involve actively executing various query sequences, such as a Session Key Reveal query targeting a specific session ID (e.g., sid), thereby jeopardizing the freshness of the session. If a session like sid or its corresponding session sid^* is compromised in the eCK model, it is deemed exposed by $\mathcal{A}$.

Furthermore, we contemplate the possibility of a quantum attack being launched by $\mathcal{A}$ during communications between MD and MS. Additionally, we account for the potential scenario where $\mathcal{A}$ physically captures MD, enabling the launch of quantum computer power side-channel attacks, such as power analysis attacks [53], [54], aimed at withdrawing information from the compromised MD's memory. $\mathcal{A}$ extacting the capability to initiate a quantum lattice reduction attack, with the objective of finding a short vector to recover the secret session keys [55].

D. Details of QRSC-IoTH

In this section, we provide the details of various phases related to the proposed QRSC-IoTH.

1) Setup Phase: This phase is executed by the MS with the following steps to select initial parameters.

Step 1: The MS first picks a large odd prime number q and an integer $n \in \mathbb{Z}_q$, where $q \pmod{2n} \equiv 1$.

Step 2: The MS then selects a discrete Gaussian distribution with a standard deviation of β over the polynomial ring $\mathbb{R}_q = \frac{\mathbb{Z}_q[x]}{<x^n+1>}$, where $q > 16\beta^2 n^{3/2}$, denoted as χ_β.

Step 3: Next, the MS randomly chooses $a \in \mathbb{R}_q$, a master secret key $m \in \chi_\beta$, and computes public key P_m as $P_m = a \cdot m + 2 \cdot e$, where $e \in \chi_\beta$. The MS also defines a one-way hash function $h : \{0, 1\}^* \rightarrow \{0, 1\}^b$, where b is a fixed hash output length.

Step 4: Finally, the MS publishes the parameters $\{n, q, \chi_\beta, a, P_m, h(\cdot)\}$ and keeps m as the master secret key.

2) Registration Phase: In this phase, a medical smart device MD_i is registered with the following steps by the MS with the help of the RA either offline or via a secure channel.

Step 1: The MS picks a unique and distinct identity ID_i, and a temporal identity TID_i for a MD_i. The MS selects a secret key $s_i \in \chi_\beta$ and then computes $v_i = h(ID_i \,||s_i \,||RTS_i \,||m)$, where RTS_i is the registration timestamp.

Step 2: The MS loads the registration credentials $\{TID_i, v_i, s_i\}$ into MD_i's memory and also stores $\{(TID_i, v_i), m\}$ into its own database. A detailed summary of this phase is shown in Fig. 2.

MD_i	MS
	Pick an identity ID_i, a temporal identity TID_i, secret key $s_i \in \chi_\beta$, and compute $v_i = h(ID_i \,||s_i \,||RTS_i \,||m)$, where RTS_i is the registration timestamp.
	$\xleftarrow{\{TID_i, v_i, s_i\}}$
Store $\{TID_i, v_i, s_i\}$	Store $\{(TID_i, v_i), m\}$

Fig. 2. Summary of the MD registration phase.

3) Secure Communications: In this phase, a session key is established between a MD_i and MS through the following steps to synchronize real-time data from the context-aware IoT device (MD_i) to its DTs, which are virtualized in MS.

Step 1: MD_i randomly selects r_d, $f_d \in \chi_\beta$, and a current timestamp TS_1. MD_i then computes $x_d = a \cdot r_d + 2 \cdot f_d$, $A_d = r_d \cdot P_m$, $B_d = Cha(A_d)$, $C_d = Mod_2(A_d, B_d)$, $D_d = v_i \oplus h(s_i \,||r_d \,||TS_1)$, and $E_d = h(v_i \,||TID_i \,||C_d \,||D_d \,||x_d \,||TS_1 \,||B_d)$. Next, MD_i constructs a message $M_1 = \{x_d, TID_i, B_d, TS_1, D_d\}$ and sends it to the MS through a public channel.

Step 2: After receiving the message M_1 from MD_i at a timestamp TS_1^*, MS checks the freshness of the message with the condition: $|TS_1^* - TS_1| < \Delta T$, where ΔT is maximum message transmission delay in the network. If it is verified, MS then fetches v_i corresponding TID_i and computes $A'_d = x_d \cdot m$, $C'_d = Mod_2(A'_d, B_d)$, and $E'_d = h(v_i \,||TID_i \,||C'_d \,||D_d \,||x_d \,||TS_1 \,||B_d)$. Next, MS verifies $E'_d = E_d$. If it is valid, MS accepts the message M_1 and believes that MD_i is authenticated. Now, MS derives $h(s_i \,||r_d \,||TS_1) = D_d \oplus v_i$, randomly selects r_s and f_s from χ_β, and obtains a fresh timestamp TS_2. Next, MS computes $x_s = a \cdot r_s + 2 \cdot f_s$, $T_s = x_d \cdot r_s$, $U_s = Cha(T_s)$, $V_s = Mod_2(T_s, U_s)$, and $W_s = h(m \,||r_s \,||TS_2) \oplus v_i$. Next, MS computes a session key SK as $SK = h(h(m \,||r_s \,||TS_2) \,||h(s_i \,||r_d \,||TS_1) \,||V_s \,||TS_1 \,||TS_2)$ and picks a new temporal identity TID_n. MS then calculates $TID_n^* = TID_n \oplus h(SK \;TID_i \,||TS_2)$, and a session key verifier SKV as $SKV = h(SK \,||TID_n^* \,||x_s \,||TS_2 \,||W_s \,||U_s)$. After that, MS generates a reply message $M_2 = \{TID_n^*, SKV, TS_2, x_s, W_s, U_s\}$ and sends it to MD_i via a public channel.

Step 3: MD_i receives the message M_2 from MS at a timestamp TS_2^* and checks the freshness by $|TS_2^* - TS_2| < \Delta T$. If it satisfies the condition, MD_i derives $h(m \,||r_s \,||TS_2) = W_s \oplus v_i$ and then computes $T'_s = x_s \cdot r_d$ and $V'_s = Mod_2(T'_s, U_s)$. Next, MD_i generates a session key $SK' = h(h(m \,||r_s \,||TS_2) \,||h(s_i \,||r_d \,||TS_1) \,||V'_s \,||TS_1 \,||TS_2)$. MD_i derives the new temporal identity by $TID_n = TID_n^* \oplus h(SK' \,||TID_i \,||TS_2)$, and generates the session key verifier $SKV' = h(SK' \,||TID_n^* \,||x_s \,||TS_2 \,||W_s \,||U_s)$. After that, MD_i verifies $SKV' = SKV$. If it is valid, MD_i then updates TID_i with new TID_n. MD_i then generates a fresh timestamp TS_3 and computes an acknowledgment $ACK = h(SK' \,||TID_n \,||TS_3)$. Next, MD_i constructs a message $M_3 = \{ACK, TS_3\}$ and sends it to MS via public channel.

Step 4: After receiving the message M_3 at a timestamp TS_3^*, MS checks it's freshness by the condition: $|TS_3^* - TS_3| < \Delta T$. If it is satisfied, MS computes $ACK' = h(SK \,||TID_n \,||TS_3)$ and verifies $ACK = ACK'$. Once it is verified, MS believes that MD_i has generated the same session key and finally MS updates TID_i with the new TID_n.

The protocol overview is shown in Fig. 3. A summary of this phase is demonstrated in Fig. 4.

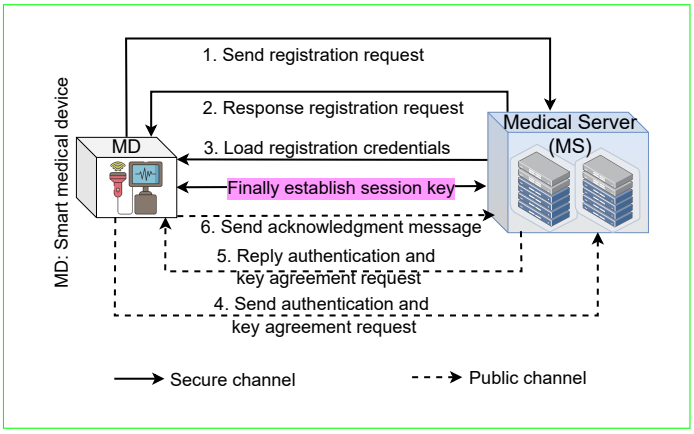

Fig. 3. Protocol overview.

4) Dynamic Devices Addition Phase: In this phase, whenever a new smart device, such as MD_n, is added to the healthcare system, it undergoes registration by MS before deployment through the following steps offline or via a secure channel.

Step 1: The MS selects a unique and distinct identity ID_n for the new MD_n, a temporal identity TID_n, and also chooses

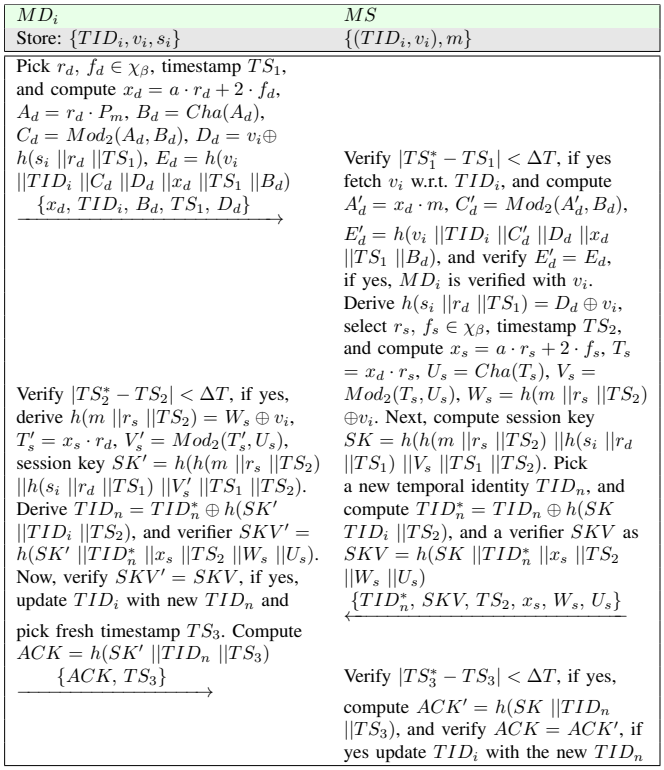

Fig. 4. Summary of secure communication phase.

a long-term secret key $s_n \in \chi_\beta$. Subsequently, MS computes the verification factor $v_n = h(ID_n \,||s_n\, ||RTS_n\, ||m)$, where RTS_n is the registration timestamp.

Step 2: The MS proceeds to load the registration credentials $\{TID_n, v_n, s_n\}$ into the memory of MD_n and also records $\{(TID_n, v_n)\}$ in its own database.

V. Security Analysis

A. Formal Security Analysis under ROR Model

We have applied the widely recognized Real-Or-Random (ROR) oracle model [56], and [57] to demonstrate the security of our proposed QRSC-IoTH scheme. The session key security of the QRSC-IoTH scheme is evaluated using the semantic security approach defined in Definition 5, as detailed in Theorem 1. Let Ω^P be the i-th instance of the participant P, where $P \in \{MD_i, MS\}$ and P follows an oracle having three states:

Accept: the oracle receives a valid message;

Reject: the oracle receives an invalid message;

Null: no response is generated.

We also consider that $\mathcal{A}$ can execute the threat models outlined in Section IV-C and employs oracle queries while interacting with Ω^P, using a probabilistic polynomial-time algorithm to attempt to breach the session key security. Let $\mathcal{A}$ interacts with Ω^P using the following queries:

- $Execute(\Omega^{MD_i}, \Phi_j^{MS})$: $\mathcal{A}$ performs this query to capture the messages exchanged between MD_i and the MS, effectively simulating a passive attack.
- $Send(\Omega^{MD_i}, M)$: Executing this query, $\mathcal{A}$ send a message M to Ω^U and receive a valid reply, simulating an active attack.
- $CorruptMD(\Omega^{MD_i})$: Performing this query, $\mathcal{A}$ retrieve the loaded secret information of a compromised MD_i's insecure memory.
- $Reveal(\Omega^P)$: Through this query, $\mathcal{A}$ obtains the valid session key $SK(= SK')$, enabling both Ω^P and its corresponding partner to move to the *Accept* state.
- $Test(\Omega^P)$: By issuing this query, $\mathcal{A}$ gains the ability to request that Ω^P validate a session key, while Ω^P independently selects a bit, denoted as c. If $c = 0$, a random string $\mathcal{S} \in 0, 1^l$ is returned as the response. However, if $c = 1$, the $Reveal$ query is triggered, and the original session key $SK(= SK')$ is provided as the response. It is crucial to note that $\mathcal{A}$ is allowed to send only one $Test$ query to Ω^P or its partner (see Definition 4).

Definition 4. *Ω^{MD_i}, and Ω^{MS} are called partners iff:*

- *they have the same session identifier,*
- *they are in Accept state,*
- *Ω^{MD_i} is Ω^{MS}'s partner, and vice-versa.*

Definition 5 (Semantic security)**.** *Let $\mathcal{N}(S)$ denote the event where $\mathcal{A}$ correctly guesses the random bit c', which matches the bit c chosen in the $Test$ oracle query, and let $\mathcal{P}[S]$ represent the probability of this event. Therefore, the advantage of $\mathcal{A}$ in breaking the semantic security of QRSC-IoTH within polynomial time t, denoted as $Adv_{\mathcal{A}}^{QRSC-IoTH}(t)$, is defined as the absolute difference: $Adv_{\mathcal{A}}^{QRSC-IoTH}(t) = |2\mathcal{P}[S] - 1|$. The proposed QRSC-IoTH scheme ensures semantic security under two conditions: (a) Ω^P and its counterpart reliably transition to the Accept state and compute the same session key, and (b) the advantage of $\mathcal{A}$ is negligible, i.e., $Adv_{\mathcal{A}}^{QRSC-IoTH}(t) < \eta$, for the adversary $\mathcal{A}$ operating within probabilistic polynomial time.*

Theorem 1. *Let $Adv_{\mathcal{A}}^{QRSC-IoTH}(t)$ be an advantage of $\mathcal{A}$ for breaking the semantic security of the session key $SK(= SK')$ within a polynomial time t. Then*

$$Adv_{\mathcal{A}}^{QRSC-IoTH}(t) \leq \frac{q_h^2}{2^l} + \frac{(q_s + q_e)^2}{q} + 2Adv_{\mathcal{A}}^{RLWE}(t).$$

Here, q_h, q_e, q_s, q, l, and $Adv_{\mathcal{A}}^{RLWE}(t)$ represent the number of hash queries, execute queries, send queries, the order of $\mathbf{R}_q$, the number of output bits in $h(\cdot)$, and the advantage of breaking the RLWE problem in polynomial time t, respectively.

Proof. We adopt a proof technique similar to those used in related protocols [25], [45], and [56] for this theorem. A series of games is employed to model the attacks from adversary $\mathcal{A}$. Notably, for each $Game_i$ $(0 \leq i \leq 3)$, the event $\mathcal{N}(S_i)$ occurs when $\mathcal{A}$ correctly guesses the bit c in the $Test$ query and wins the game, with the probability of this event denoted as $\mathcal{P}[S_i]$, i.e., $Adv_{\mathcal{A},Game_i}^{QRSC-IoTH} = \mathcal{P}[S_i]$.

$Game_0$: In this case, $\mathcal{A}$ initiates the real attack on the proposed QRSC-IoTH scheme within the ROR model. Prior

to starting $Game_0$, $\mathcal{A}$ selects a random bit c. According to Definition 5, we have:

$$Adv_{\mathcal{A}}^{QRSC-IoTH}(t) = |2\mathcal{P}[S_0] - 1|. \tag{2}$$

$Game_1$: In this case, $\mathcal{A}$ intercepts the messages exchanged between MD_i and the MS. By issuing the $Execute$ query, $\mathcal{A}$ attempts to reveal the session key. At the end of this process, $\mathcal{A}$ uses $Reveal$ and $Test$ queries to determine whether the session key is real or random. It is important to note that an eavesdropping attack alone does not give $\mathcal{A}$ any advantage in deducing the session key. As a result, both $Game_0$ and $Game_1$ are indistinguishable, leading to the following conclusion:

$$|\mathcal{P}[S_0] - \mathcal{P}[S_1]| = 0. \tag{3}$$

$Game_2$: In this game, $\mathcal{A}$ launches an active attack by using the $Send$, $Execute$, and hash oracle $\mathcal{H}$ queries. Despite intercepting the messages M_1, M_2, and M_3, no hash collisions occur, as the components within these messages are protected by the collision-resistant one-way hash function $h(\cdot)$. To induce a hash collision, $\mathcal{A}$ must issue a $\mathcal{H}$ query. According to the birthday paradox, the probability of a collision in the hash oracle is at most $\frac{q_h^2}{2^{l+1}}$. Similarly, the probability of collisions for the parameters x_d and x_s, derived from the $Send$ and $Execute$ queries, is at most $\frac{(q_s+q_e)^2}{2q}$, since the transcripts x_d and x_s are generated from random samples of a discrete Gaussian distribution χ_β over $\mathbb{R}_q$. Notably, both $Game_1$ and $Game_2$ are indistinguishable, differing only in the simulation of the $Send$, $Execute$, and hash $\mathcal{H}$ queries. Therefore, we have:

$$|\mathcal{P}[S_1] - \mathcal{P}[S_2]| \leq \frac{q_h^2}{2^{l+1}} + \frac{(q_s+q_e)^2}{2q}. \tag{4}$$

$Game_3$: In this game, $\mathcal{A}$ issues the $CorruptMD(\Omega^{MD_i})$ query to obtain the information $\{TID_i,\ v_i,\ s_i\}$ of the compromised device MD_i. Subsequently, $\mathcal{A}$ attempts to deduce the private keys s_i and v_i, and tries to generate a session key $SK'(= SK)$. Furthermore, in this particular game, the session key is guessed without simulating $\mathcal{H}$. In the proposed QRSC-IoTH scheme, session key $SK' = h(h(m\ ||r_s\ ||TS_2)\ ||h(s_i\ ||r_d\ ||TS_1)\ ||V_s'\ ||TS_1\ ||TS_2)$, where $x_d = a\cdot r_d + 2\cdot f_d$, $x_s = a\cdot r_s + 2\cdot f_s$, $T_s' = x_s \cdot r_d$, $T_s = x_d \cdot r_s$, $U_s = Cha(T_s)$, and $V_s' = Mod_2(T_s', U_s)$. In order to successfully guess the SK', $\mathcal{A}$ needs to solve the RLWE problem to find V_s'. As a result, games $Game_3$ and $Game_2$ become indistinguishable, without considering the guessing attack on MD_i's session key. Thus, we have:

$$|\mathcal{P}[S_2] - \mathcal{P}[S_3]| \leq Adv_{\mathcal{A}}^{RLWE}(t). \tag{5}$$

At the end of this game, $\mathcal{A}$ chooses a random bit c in an effort to win the game $Game_3$, resulting in the following conclusion:

$$\mathcal{P}[S_3] = \frac{1}{2}. \tag{6}$$

From (2), (3), and (6), we obtain the following result:

$$\begin{aligned} \frac{1}{2}.Adv_{\mathcal{A}}^{QRSC-IoTH}(t) &= |\mathcal{P}[S_0] - \frac{1}{2}| \\ &= |\mathcal{P}[S_1] - \frac{1}{2}| \\ &= |\mathcal{P}[S_1] - \mathcal{P}[S_3]| \\ &= |\mathcal{P}[S_1] - \mathcal{P}[S_2]| \\ &+ |\mathcal{P}[S_2] - \mathcal{P}[S_3]|. \end{aligned} \tag{7}$$

From (4), (5), and (7), we have

$$\begin{aligned} \frac{1}{2}.Adv_{\mathcal{A}}^{QRSC-IoTH}(t) &\leq \frac{q_h^2}{2^{l+1}} + \frac{(q_s+q_e)^2}{2q} \\ &+ Adv_{\mathcal{A}}^{RLWE}(t). \end{aligned} \tag{8}$$

Now, multiplying both sides of (8) by 2, we arrive at the final result.

$$\begin{aligned} Adv_{\mathcal{A}}^{QRSC-IoTH}(t) &\leq \frac{q_h^2}{2^{l}} + \frac{(q_s+q_e)^2}{q} \\ &+ 2Adv_{\mathcal{A}}^{RLWE}(t). \end{aligned}$$

□

B. Formal Security Verification under Scyther Tool

In this section, we conduct a formal security validation of the QRSC-IoTH scheme through the utilization of the Scyther tool. Scyther serves as an automated verification tool specifically designed for security protocols [58], [59]. It provides assurances of termination and allows for the validation of correctness across an unbounded number of sessions. Scyther includes predefined security models like the DY threat model, CK-adversary, eCK-adversary, and more, eliminating the requirement for users to define adversary capabilities themselves [60]. Within this threat model, Scyther can identify potential attacks within the proposed QRSC-IoTH scheme while considering realistic adversary assumptions.

Scyther employs its proprietary specification language, denoted as "spdl," to articulate the nuances of a security protocol's implementation. This language allows users to delineate the specific roles involved in the protocol and specify the communication flow between them. Additionally, it provides a set of functions, such as "sent" and "recv," to facilitate the sending and receiving of messages among these roles, formatted as "sent_" or "recv_." For a more details, please see the Scyther manual [59].

Figure 5 illustrates the output obtained from the verification process of the proposed scheme using the Scyther tool. In this experiment, we focused on the communication interactions between a medical sensor device as **SensorMD** and a server as **ServerMS** within the proposed scheme. Here, **ServerMS** takes on the responsibility of securely registering **SenorMD** via a secure channel. The generation of random numbers in the secure communication process is achieved through the use of the "fresh" or "var" keyword. Additionally, the "match()"

Scyther results : verify

Claim				Status		Commer
QRSC_IoTH	ServerMS	QRSC_IoTH,ServerMS1	Alive	Ok	Verified	No attacks.
		QRSC_IoTH,ServerMS2	Nisynch	Ok	Verified	No attacks.
		QRSC_IoTH,ServerMS3	Niagree	Ok	Verified	No attacks.
		QRSC_IoTH,ServerMS4	Secret m	Ok	Verified	No attacks.
		QRSC_IoTH,ServerMS5	Secret rs	Ok	Verified	No attacks.
	SensorMD	QRSC_IoTH,SensorMD1	Alive	Ok	Verified	No attacks.
		QRSC_IoTH,SensorMD2	Secret si	Ok	Verified	No attacks.
		QRSC_IoTH,SensorMD3	Secret rd	Ok	Verified	No attacks.
		QRSC_IoTH,SensorMD4	Nisynch	Ok	Verified	No attacks.
		QRSC_IoTH,SensorMD5	Niagree	Ok	Verified	No attacks.

Done.

Fig. 5. Simulation results using Scyther tool.

function is employed to assign values provided by the Scyther tool. Scyther utilizes "claim" events as a means to express security requirements, wherein these claims can manifest in different ways. For instance, designating a value as "secret" implies its confidential nature, subject to verification within the established security model, accounting for potential adversarial scenarios. Additionally, Scyther employs Nisynch to denote non-injective synchronization and Niagree to represent non-injective agreement. The outcomes presented in Fig. 5 confirm that Scyther has not detected any vulnerabilities or deficiencies within the proposed QRSC-IoTH scheme.

C. Informal Security Analysis

In this section, we present a thorough security analysis of the QRSC-IoTH scheme, illustrating its ability to withstand an array of both active and passive attacks orchestrated by potential adversaries.

1) Replay Attack: Within the proposed framework, three messages denoted as $\{M_1, M_2, M_3\}$ are exchanged during the secure communication phase outlined in Section IV-D3. Each of these messages carries a unique timestamp, and these timestamps are obfuscated by a quantum-resistant cryptographic hash function. Upon receiving these messages, all recipients validate their freshness by cross-referencing the timestamps before accepting the messages. The proposed QRSC-IoTH scheme ensures security against replay attacks, as any attempt to replay an older message can be promptly detected.

2) Man-in-the-Middle (MiTM) Attack: In this attack scenario, an adversary denoted as $\mathcal{A}$ exploits the DY threat model to intercept the secure communication request message $M_1 = \{x_d, TID_i, B_d, TS_1, D_d\}$. The adversary's objective is to generate a similar message, denoted as M_1^*. To achieve this, $\mathcal{A}$ selects r_d^* and f_d^* from χ_β, generates a fresh timestamp TS_1^*, and calculates the values $x_d^* = a \cdot r_d^* + 2 \cdot f_d^*$, $A_d^* = r_d^* \cdot P_m$, $B_d^* = Cha(A_d^*)$, $C_d^* = Mod_2(A_d^*, B_d^*)$, $D_d^* = v_i \oplus h(s_i \,||r_d^* \,||TS_1^*)$, and $E_d^* = h(v_i \,||TID_i \,||C_d^* \,||D_d^* \,||x_d^* \,||TS_1^* \,||B_d^*)$. The generation of valid values for D_d^* requires knowledge of the secret values $\{v_i, s_i\}$. As these keys are not accessible to $\mathcal{A}$, it is unable to proceed with the attack. Consequently, $\mathcal{A}$ cannot generate other valid messages, ensuring that the proposed QRSC-IoTH remains secure against MiTM attacks.

3) Device Impersonation Attack: In this particular attack, $\mathcal{A}$ undertakes the role of an imposter mimicking a genuine communicating entity on behalf of a legitimately registered device, denoted as MD_i. The objective is to generate a valid response message $M_3 = \{ACK, TS_3\}$ in real-time. The construction of an authentic message M_3, outlined in Section IV-D3, necessitates knowledge of specific secret values, namely $\{SK', v_i, s_i, V_s'\}$. Devoid of access to these crucial values, $\mathcal{A}$ encounters an impediment and is consequently unable to proceed. Consequently, the imposter cannot effectively emulate a bona fide device. Therefore, the proposed QRSC-IoTH stands resilient against device impersonation attacks.

4) Privileged-Insider Attack: In the QRSC-IoTH scheme, during the registration phase, MS registers each MD_i through an offline or secure channel. In this registration process, MS selects a unique private key for each device and computes the registration credentials, which are then loaded into the memory of MD_i. Subsequently, MS removes the secret key of MD_i from its database. The session is established using this secret key, which is further concealed by a one-way hash function. Consequently, MS remains oblivious to the original secret key, preventing any privileged-insider from launching an attack. Thus, QRSC-IoTH is resilient against privileged-insider attacks.

5) Ephemeral Secret Leakage (ESL) Attack: During the secure communication process, a session key between MS and MD_i is generated as $SK = h(h(m \,||r_s \,||TS_2) \,||h(s_i \,||r_d \,||TS_1) \,||V_s \,||TS_1 \,||TS_2)$, where $x_s = a \cdot r_s + 2.f_s$, $T_s = x_d \cdot r_s$, $U_s = Cha(T_s)$, and $V_s = Mod_2(T_s, V_s)$. The construction of this session key incorporates both ephemeral or short-term secrets (r_d, f_d, r_s, and f_s) and long-term secrets (e.g., s_i, v_i, and m). Therefore, an adversary $\mathcal{A}$ can only compromise the session key if they manage to expose both the long-term and short-term secrets. Under the CK-adversary model, if a session key is compromised within a specific session, it does not pose a threat to session keys in previous or subsequent sessions. This inherent uniqueness across different sessions results from the use of timestamps, random secrets, and long-term secrets. Consequently, it becomes computationally infeasible for $\mathcal{A}$ to generate a valid SK. Thus, the proposed QRSC-IoTH is not susceptible to the ESL attack under the CK-adversary model.

6) Key Compromise Impersonation Attack (KCIA): In the KCIA, if an adversary $\mathcal{A}$ gains access to the secrets of the MD, it could use this information to impersonate other entities to MD. As a result, this attack could have more severe consequences than perfect forward secrecy, and requires careful consideration [61]. The protocol resist KCIA by leveraging quantum-resistant cryptographic techniques that provide robust security against key exposure. In the event of a key compromise, the protocol's use of post-quantum cryptography, such as RLWE ensures that even if an attacker $\mathcal{A}$ obtains a private key, the structure of the cryptographic scheme remains secure. For example, if $\mathcal{A}$ compromises a secret key s_i of a MD_i, but does not have the corresponding secret v_i, $\mathcal{A}$ cannot impersonate the MD_i. According to the eCK adversary model, even if $\mathcal{A}$ compromises a session-specific ID, it does

not affect the session key of previous or future sessions. The protocol likely incorporates additional measures, such as key renewal and forward secrecy, to minimize the risk of impersonation by regularly changing session keys and ensuring that past communication sessions cannot be retroactively used. Furthermore, by using secure key exchange mechanisms, the protocol can verify the authenticity of communicating entities, ensuring that even with key exposure, an attacker cannot impersonate a legitimate device without being detected. These combined mechanisms help mitigate the impact of a key compromise and prevent unauthorized access, thus defending against KCI attacks.

7) Device Anonymity and Untraceability: In the proposed QRSC-IoTH scheme, the actual identities of the communicating parties (MS and MD_i) are never transmitted over the public channel within the messages M_1, M_2, and M_3. Instead of real identities, a temporal identity is transmitted, which conceals the genuine identity of any communicating party. Consequently, $\mathcal{A}$ cannot recover the authentic identities from these messages, preserving the anonymity of both MS and MD_i in the proposed scheme. Moreover, as the transmitted messages are generated with random nonces and current timestamps, they exhibit dynamic characteristics in each session. Additionally, the temporal identity changes with each session, ensuring that the messages are distinct and unique for different sessions. Consequently, $\mathcal{A}$ is unable to trace the recipients of the messages. Hence, QRSC-IoTH also upholds the property of untraceability.

8) Device Physical Capture Attack: In this scenario, $\mathcal{A}$ has the ability to physically capture a MD and may attempt to launch side-channel attacks utilizing a quantum computer, such as power analysis attacks [53]. These attacks aim to extract information from the compromised MD's non-tamper-proof memory. It is crucial to emphasize that the stored credentials for each MD are unique and exclusive to that specific registered MD. Consequently, if $\mathcal{A}$ captures one MD, it will not expose any secret credentials related to any other non-captured MD. Thus, QRSC-IoTH remains resilient against physical device capture attacks.

9) Quantum Lattice Reduction Attack: The proposed QRSC-IoTH scheme is built upon the lattice hardness problem RLWE, as specified in Section III. This problem can be transformed into the standard LWE problem. The LWE problem is characterized by three essential parameters: the modulus q, the matrix dimension n, and the error distribution χ_β. The distribution χ_β is typically represented as a rounded continuous or discrete Gaussian distribution over $\mathbb{R}_q$ with a mean of zero and a standard deviation of β. In RLWE, each pair $(s, a = s \cdot t + e) \in \mathbb{R}_q \times \mathbb{R}_q$ can be associated with (M, a) in the LWE problem, where M is a matrix created from the coefficients of the polynomial s [44]. Our main emphasis is directed towards two Block Korkine-Zolotarev (BKZ) attacks, namely the primal and dual attacks [62]. These will be elaborated upon in the following paragraphs:

The primal lattice reduction attack, often employed in the BKZ algorithm, focuses on transforming the given lattice basis to a basis where one of the lattice vectors becomes significantly shorter. This reduction is performed iteratively, aiming to produce a basis where the shortest vector is short enough to efficiently solve the RLWE problem associated with QRSC-IoTH. According to the BKZ models, the primal attack achieves success if and only if $\beta\sqrt{k} \leq \Delta^{2k-l-1} \cdot q^{\frac{m}{l}}$, where $\Delta = ((\pi k)^{\frac{1}{k}} \cdot \frac{k}{2\pi e})^{\frac{1}{2(k-1)}}$, $l = m+n+1$, m denotes the count of samples r_d, and k signifies the block size dimension for finding the unique solution in BKZ [63]. It's crucial to highlight that the runtime of the BKZ lattice reduction algorithm experiences exponential growth with k, specifically as $k \cdot 2^{ck}$ CPU clock cycles, where c denotes an exponential constant. In the classical scenario, the most widely acknowledged value for c is 0.292, whereas in the quantum realm, it is 0.265 [55].

In the dual attack, the aim is to search for a short vector within the dual lattice, defined as $\mathbb{D}^* = \{(x, y) \in \mathbb{Z}^m \times \mathbb{Z}^m | M^t x = y \pmod q\}$, intending to employ it as a discriminator for the decision-LWE problem. The BKZ algorithm produces such a vector with a length of $t = \Delta^{l-1} q^{\frac{n}{l}}$ and a block size of k. The maximum variation distance between these two distributions is constrained by $\epsilon \approx 4e^{-2\pi^2 v^2}$, where $v = \frac{t\gamma}{q}$. Consequently, the attacker must enhance their chances of success by identifying roughly $\frac{1}{\epsilon^2}$ of these short vectors. For a given vector $2^{0.2075k}$, the attack needs to be executed at least $T = \max(1, \frac{1}{(2^{0.2075k}\epsilon^2)})$ times for optimal effectiveness [63].

VI. Experimental Setup and Results

In this section, our emphasis revolves around conducting hands-on experiments utilizing Raspberry Pi devices set up as MD and a laptop configured as a server MS.

Timing measurements were conducted for diverse cryptographic operations utilizing cryptography standard library version 37.0.2, renowned for its widespread application in cryptographic functionalities such as symmetric encryption/decryption (AES), ECC, one-way hash functions, and more. In this experimental context, the variables T_h, T_{eca}/T_{ecm}, T_{senc}/T_{sdec}, and T_{mtp} denote the execution times for a one-way hash function, ECC point addition/multiplication, AES encryption/decryption, and the conversion of a message to an elliptic curve point, respectively.

For ECC operations, we have considered a non-singular elliptic curve known as secp256r1, which follows the equation form $y^2 = x^3 + rx + s \pmod q$ (for more details, please refer to RFC5480). We conducted all our experiments under the Raspberry PI configuration: Raspberry PI 4 Model B, with CPU: 64-bit, Processor: 1.4 GHz Quad-core, 4 cores, Memory (RAM): 1GB, and OS: Ubuntu 20.04 LTS, 64-bit, and server configuration: Ubuntu 22.04 LTS, with memory: 16 GB, processor: Intel Core i7-9750H CPU @ 2.60GHz processor with 6 cores; 12 threads, OS type: 64-bit and disk type: SSD 256 GB. The experiment was iterated 500 times, and the maximum, minimum, and average execution times (in milliseconds) for each cryptographic operation were computed. The outcomes of these experiments have been recorded in Table II. The execution times for lattice-based cryptographic operations, sourced from Feng et al. [45], are detailed in Table III. Notably, we observe that the Mod_2 operation in $\mathbb{R}_q$ essentially functions as an AND operation, rendering it negligible in our analysis.

TABLE II
EXECUTION TIME (IN MILLISECONDS) FOR CRYPTOGRAPHIC PRIMITIVES

Primitive	Server time (ms)	Raspberry PI 4 time (ms)
T_h	0.0424	0.3187
T_{senc}	0.0173	0.0926
T_{sdec}	0.0163	0.0945
T_{ecm}	0.1590	1.0712
T_{eca}	0.0229	0.1509
T_{mtp}	0.6627	7.7039

TABLE III
EXECUTION TIME (IN MILLISECONDS) FOR LATTICE-BASED OPERATIONS TAKEN FROM FENG ET AL. [45]

Primitive	Server time (ms)	User time (ms)
T_{gs}	0.000075503	0.000561483
T_{sm}	0.000000296	0.000006655
T_{pm}	0.000000307	0.000013052
T_{ma}	0.000002549	0.000029505
T_{cha}	0.000000689	0.000035515

"T_{gs}: time for sampling from χ_β, T_{sm}: time for one component-wise multiplication with scalar operation in $\mathbb{R}_q$, T_{pm}: time for one component-wise multiplication in $\mathbb{R}_q$, T_{ma}: time for one component-wise multiplication and addition operation in $\mathbb{R}_q$, and T_{cha}: time for the characteristic function in $\mathbb{R}_q$"

A. Implementation of the Proposed QRSC-IoTH Scheme

In this section, we outline the implementation of the proposed scheme described in Section IV-D3 using a client-server model, often referred to as socket programming, within the Python programming environment. The protocol was implemented based on the available primary source code from the repository in [64]. To establish a connection between the medical device MD_i (represented by a Raspberry Pi) and the medical server MS (as a laptop), we set up a private wireless network using Wi-Fi Hotspot technology. After establishing the wireless connection, we used the Secure Shell (SSH) protocol to facilitate remote access from the laptop to the raspberry pi. The client code (client-1.py) was then run on the raspberry pi, while the server code (server-1.py) was executed on the laptop through the ubuntu terminal. Here, the MS is configured with Ubuntu 22.04 LTS, featuring 16 GB of RAM and an Intel® Core™ i7-9750H processor, CPU running at 2.60 GHz, equipped with 6 cores and 12 threads, operating on a 64-bit architecture with a 256 GB SSD. And a MD_i is configured with raspberry pi 4 model B Rev 1.5, featuring a 64-bit Cortex-A72 processor clocked at 1800 MHz with 4 cores and 7.6 GB of RAM, running Ubuntu 20.04.6 LTS on an aarch64 architecture. Figure 6 illustrates the successful implementation of the proposed scheme. The left side of the figure shows the session key generated on a MD_i, highlighted in a red box, while the right side displays the corresponding session key for the MS, also highlighted in red. Both sides demonstrate the creation of the same session key, confirming the claims made by the proposed scheme.

VII. COMPARATIVE STUDY

In this phase, we perform a comparative assessment of the proposed QRSC-IoTH scheme against various existing and relevant competing schemes. These schemes include those designed by Qiao et al. [32], Huang et al. [34], Dabra et al. [25], Irshad et al. [65], Islam and Basu [29], Zhang et al. [23], Mishra et al. [36], and Rewal et al. [37]. This comparative assessment encompasses communication costs, computation costs, and security and functionality features.

TABLE IV
COMPARATIVE ASSESSMENT OF COMMUNICATION COSTS

Scheme	No. of messages	Total cost (in bits)
Qiao et al. [32]	4	5568
Huang et al. [34]	4	19140
Dabra et al. [25]	3	9122
Irshad et al. [65]	3	4320
Islam and Basu [29]	8	19648
Zhang et al. [23]	4	9984
Mishra et al. [36]	3	14018
Rewal et al. [37]	4	18626
Proposed QRSC-IoTH	3	9730

A. Communication Cost Assessment

In computing the communication cost, we establish the following assumptions regarding the sizes of distinct elements: random numbers consist of 160 bits, real or temporal identities are 160 bits, AES encryption/decryption keys are 128 bits, timestamps amount to 32 bits, hash function outputs (using the SHA2 hashing algorithm) comprise 256 bits, ECC points are 320 bits, elements in $\mathbb{R}_q$ are 4096 bits, and both Cha and Mod_2 are 1 bit each.

In the proposed QRSC-IoTH, the communicated messages are $M_1 = \{x_d, TID_i, B_d, TS_1, D_d\}$, $M_2 = \{TID_n^*, SKV, TS_2, x_s, W_s, U_s\}$, and $M_3 = \{ACK, TS_3\}$. These messages need communication costs of (4096 + 160 + 1 + 32 + 256) = 4545 bits, (256 + 256 + 32 + 4096 + 256 + 1) = 4897 bits, and (256 + 32) = 288 bits, respectively, resulting in a total of 9730 bits. We considered that Huang et al.'s scheme [34] involves 100 devices, denoted as dn, installed within their network and $|S| = 10$ for Zhang et al.'s scheme. Table IV and Fig. 7 illustrate the communication costs along with the number of messages. It is evident from the data that our proposed QRSC-IoTH incurs lower communication costs compared to the schemes presented by Huang et al. [34], Islam and Basu [29], Zhang et al. [23], Mishra et al. [36], and Rewal et al. [37]. However, it exhibits higher communication costs when compared to the schemes of Qiao et al. [32], Dabra et al. [25], and Irshad et al. [65]. Unfortunately, the schemes proposed by Qiao et al., Dabra et al., and Irshad et al. do not meet all the security requirements necessary for ensuring robust security in such applications. For instance, Dabra et al.'s [25] scheme is vulnerable to replay attacks, lacks support for untraceability, and has not been verified using security verification tools like AVISPA, Scyther, or ProVerif. These deficiencies render it impractical for real-world applications. Notably, the scheme proposed by Irshad et al. [65] is based on DLP and ECDLP, making them susceptible to quantum attacks and Qiao et al.'s scheme is vulnerable to ESL attacks under the CK-adversary model.

B. Computation Cost Assessment

To assess the computational cost, we specifically focused on the secure communication phase outlined in Fig. IV-D3.

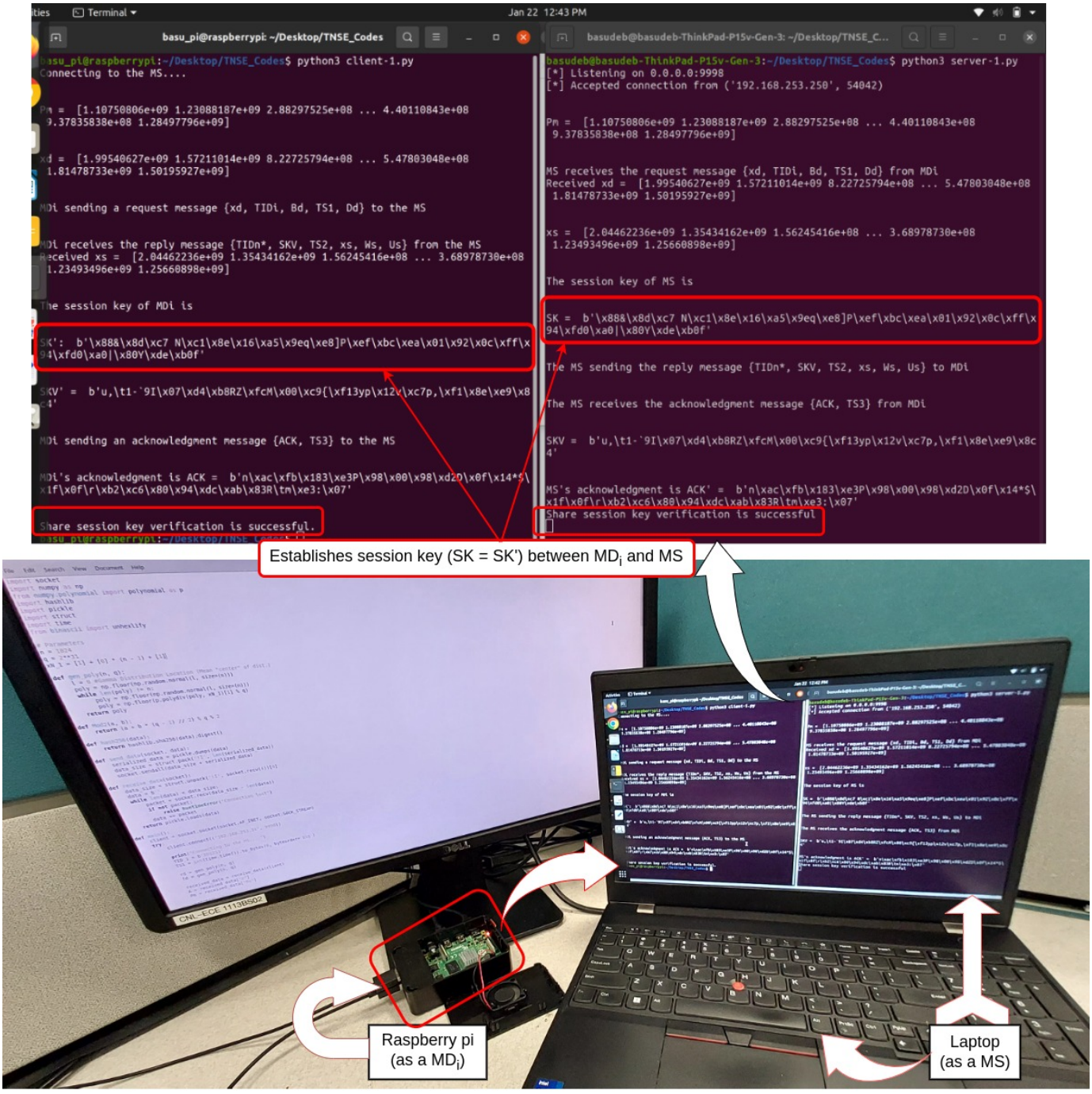

Fig. 6. Implementation of QRSC-IoTH using Raspberry PI device.

The evaluation includes the execution times of various cryptographic operations, as detailed in Table II and Table III. The computation cost for MD amounts to $5T_h + 2T_{gs} + T_{sm} + 2T_{pm} + T_{ma} + T_{cha} \approx 1.5947$ ms, while MS incurs computational cost of $6T_h + 2T_{gs} + T_{sm} + 2T_{pm} + T_{ma} + T_{cha} \approx 0.2546$ ms. To estimate the computation costs of Qiao et al. [32], T_c is approximated at 0.3042 ms for smart devices and 0.0450 ms for the server. To compute the computational costs associated with Dabra et al.'s scheme, we evaluate the expenses for two functions, $H_1(\cdot)$ and $H_2(\cdot)$, which are comparable to the cost of sampling from χ_β. Specifically, $T_{H_1}/T_{H_2} \approx T_{gs}$. Moreover, we also consider $T_{KDF(\cdot)}/T_{BPV} \approx T_h$ for Zhang et al.'s scheme. The comparison of computational costs between the proposed QRSC-IoTH and other existing schemes is summarized in Table V. Both Table V and Fig. 8 illustrate that our scheme requires lower computational costs for both MD and server MS compared to Qiao et al. [32], Huang et al. [34], Huang et al. [34], and others.

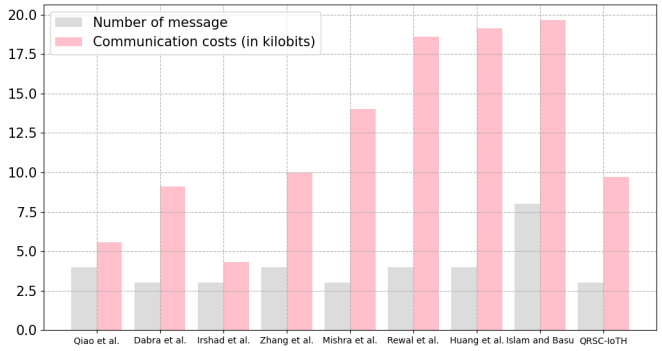

Fig. 7. Communication costs (in kilobits) along with number of messages.

TABLE V
COMPARATIVE ASSESSMENT ON COMPUTATION COSTS

Scheme	MD/U/IoT device	FN/Gateway node/Server
Qiao et al. [32]	$6T_h + 2T_c$ ≈ 2.5206 ms	$16T_h + 7T_c + 2T_{sdec}$ ≈ 1.0254 ms
Huang et al. [34]	$5T_h + 5T_{ecm} + T_{sdec}$ ≈ 7.044 ms	$18T_h + 13T_{ecm} + 2T_{senc}$ $+T_{sdec} \approx 2.881$ ms
Dabra et al. [25]	$6T_h + 6T_{gs} + 2T_{sm} +$ $T_{pm} + 3T_{ma} + T_{cha}$ ≈ 1.9157 ms	$5T_h + 5T_{gs} + 2T_{sm} +$ $T_{pm} + 3T_{ma} + T_{cha}$ ≈ 0.2123 ms
Zhang et al. [23]	$12T_h + 3T_{ecm} + T_{senc}$ $+T_{sdec} \approx 7.2250$ ms	$7T_h + T_{ecm} + T_{senc}$ $+T_{sdec} \approx 0.4894$ ms
Mishra et al. [36]	$8T_h + 4T_{gs} + 2T_{sm} +$ $3T_{pm} + 2T_{ma} + 2T_{cha}$ ≈ 2.553 ms	$6T_h + T_pm$ ≈ 0.255 ms
Rewal et al. [37]	$8T_h + 4T_{gs} + 2T_{sm} +$ $2T_{pm} + 2T_{ma} + T_{cha}$ ≈ 2.552 ms	$6T_h$ ≈ 0.254 ms
Islam and Basu [29]	$12T_h + 4T_g + 2T_{sm} +$ $2T_m + 2T_{ma} + 2T_{cha}$ ≈ 3.7613 ms	$6T_h$ ≈ 0.2544 ms
Irshad et al. [65]	$20T_h + 9T_{ecm} + 3T_{eca}$ ≈ 16.467 ms	$8T_h + 3T_{ecm} + 2T_{eca} +$ $2T_{senc}/T_{sdec} \approx 0.896$ ms
Proposed QRSC-IoTH	$6T_h + 2T_{gs} + T_{sm} +$ $2T_{pm} + T_{ma} + T_{cha}$ ≈ 1.9134 ms	$6T_h + 2T_{gs} + T_{sm} +$ $2T_{pm} + T_{ma} + T_{cha}$ ≈ 0.2546 ms

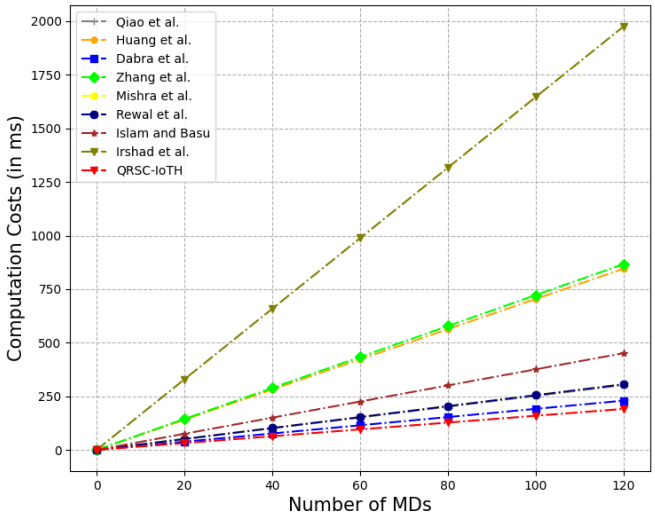

Fig. 8. Computation costs (in ms) versus the number of devices.

C. Functionality and Security (FS) Attributes

Table VI demonstrates that the proposed QRSC-IoTH scheme effectively fulfills all crucial security and functionality criteria required to establish a robust security solution within the healthcare system under quantum computing, whereas other present solutions fall short of achieving these objectives.

TABLE VI
COMPARATIVE ASSESSMENT ON VARIOUS FS ATTRIBUTES

Attribute	[36]	[37]	[27]	[25]	[30]	[23]	[65]	QRSC-IoTH
FS_1	✓	✓	✓	✗	✗	✗	✓	✓
FS_2	✓	✓	✗	✓	✓	✓	✓	✓
FS_3	✓	✓	✓	✓	✓	✓	✓	✓
FS_4	✓	✓	✗	✓	✓	✓	✓	✓
FS_5	✓	✓	✗	✓	✓	✓	✓	✓
FS_6	✓	✓	✗	✓	✗	✓	✓	✓
FS_7	✗	✗	✗	✓	✓	✓	✓	✓
FS_8	✗	✗	✗	✗	✓	✓	✓	✓
FS_9	✓	✓	✓	✓	✓	✓	✓	✓
FS_{10}	✗	✗	✓	$\mathcal{NA}$	✗	✓	✗	✓
FS_{11}	✗	✗	✓	✗	✗	✗	✓	✓
FS_{12}	✓	✓	✗	✓	✗	✗	✗	✓

FS_1: Resistant to replay attack; FS_2: Resistant to man-in-the-middle attack; FS_3: Key agreement; FS_4: Resistant to device impersonation attack; FS_5: Resistant to physical device capture attack; FS_6: Resistant to ESL attack under the CK-adversary model; FS_7: Resistant to anonymity leakage; FS_8: Resistant to Untraceability; FS_9: Resistant to privileged-insider attack; FS_{10}: Support dynamic MD/device addition phase; FS_{11}: Formal security verification using AVISPA/Scyther/ProVerif; FS_{12}: Resistant to quantum attacks
✓: Supports an attribute; ✗: Does not support an attribute; $\mathcal{NA}$: Not applicable.

D. Performance under Unknown Attacks

While we have confirmed the robustness of our proposed schemes against various well-documented active and passive attacks, as outlined in Section V-C, there remain unidentified threats whose occurrence and impact are unpredictable. Therefore, we now assess how our proposed scheme performs when faced with these unknown attacks. Specifically, we focus on detailing the communication and computation overhead incurred in response to such unforeseen threats:

$$Com_{avg} = \frac{Com_{fail} \times pr_{fail} + Com_{succ} \times pr_{succ}}{pr_{succ}}, \quad (9)$$

$$Com_{fail} = \sum_{i=1}^{T_m} \frac{Com_i}{T_m}. \quad (10)$$

The specific calculation outlined in the Eq. (9) similar to [60], where Com_{avg} represents the average communication/computation overhead incurred during incidents of unknown attacks. Here, Com_{fail} denotes the communication/computation overhead when secure communication defined in Section IV-D3 fails due to an unknown attack, and Com_{succ} denotes the overhead for successful secure communication. Additionally, pr_{fail} indicates the probability of an unknown attack occurring during protocol execution, where the success probability can be calculated by $pr_{succ} = 1 - pr_{fail}$. We assume that the total number of messages in the secure communication process is denoted as T_m, and the probability of an unknown attack occurring at step i is $\frac{1}{T_m}$. As a result, Com_{fail} can be derived from Eq. (10), where Com_i represents the cumulative communication overhead up to the occurrence of an unknown attack at step i.

The findings depicted in Fig. 9 and Fig. 10 demonstrate the superior performance of the proposed protocol compared to related schemes when faced with unknown attacks. This

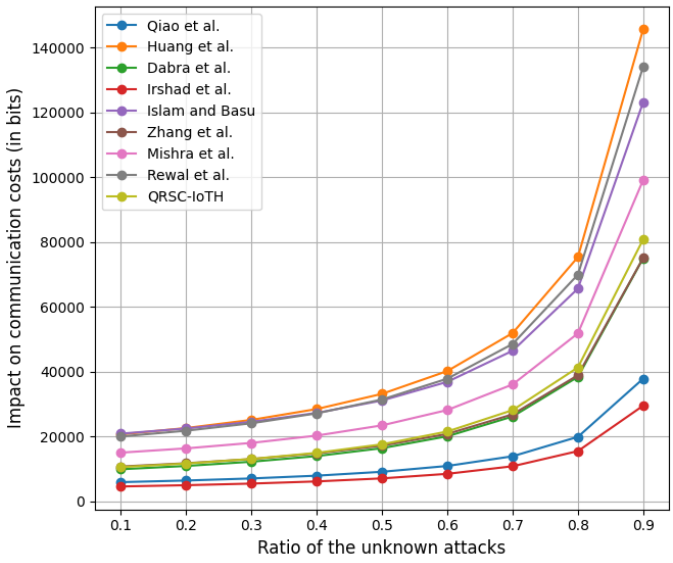

Fig. 9. Performance on communication costs under the unknown attacks.

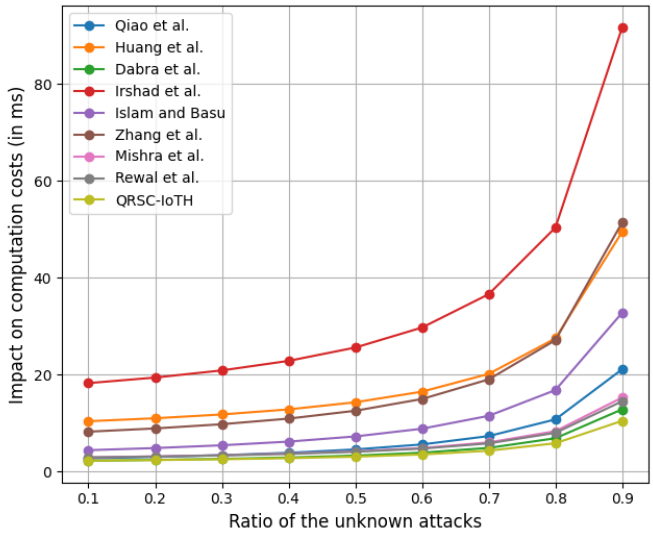

Fig. 10. Performance on computation costs (in ms) under the unknown attacks.

superiority is attributed to the lower computational and communication costs incurred by the proposed protocol. However, it is important to note that the proposed protocol does involve slightly higher communication overhead compared to scheme of Qiao et al., Dabra et al., and Irshad et al. due to their reduced communication requirements. A security analysis also identifies vulnerabilities in Qiao et al., Dabra et al., and Irshad et al., including susceptibility to replay attacks,lacks support for nntraceability, ESL attacks under the CK-adversary model, and quantum attacks. Consequently, these protocols are deemed unsuitable for deployment in real-time applications. In light of these observations, it can be concluded that the proposed protocol not only outperforms its counterparts in scenarios without known attacks but also demonstrates superior performance in scenarios involving unknown attacks.

VIII. Conclusion and Future Works

We designed a secure communication methodology to resist quantum attacks for IoT in healthcare systems with digital twins. Our primary objective is to secure real-time, context-aware, and sensitive healthcare data, which is synchronized with digital twins, enabling remote monitoring by doctors. The proposed scheme prioritizes robust security to support data analysis with AI/ML models in the presence of adversaries. The proposed scheme is secure against various active and passive attacks, including quantum attacks. The scheme underwent testbed experiments on Raspberry Pi 4 devices to evaluate computational overhead, affirming its practicality. Moreover, formal security verification using the Scyther automated software validation tool was conducted to emphasize the solution's robustness. In a comprehensive comparative evaluation against existing schemes, our QRSC-IoTH scheme emerged as lightweight, scalable, and efficient selection for real-world applications. Additionally, the performance analysis under unknown attacks shows that the proposed scheme significantly outperforms existing schemes.

In future work, we will incorporate a detailed evaluation of how the DT contributes to the overall system. This will include performance metrics such as latency, data accuracy, and resource utilization, as well as its role in improving system security through real-time anomaly detection and its effectiveness in decision-making, particularly in time-sensitive healthcare scenarios.

References

[1] L. U. Khan, Z. Han, W. Saad, E. Hossain, M. Guizani, and C. S. Hong, "Digital Twin of Wireless Systems: Overview, Taxonomy, Challenges, and Opportunities," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2230–2254, 2022.

[2] "OpenSim," https://opensim.stanford.edu/. Accessed on November 2023.

[3] "Digital Twin Framework," https://www.ge.com/research/project/digital-twin-framework. Accessed on November 2023.

[4] J. Chen, C. Yi, S. D. Okegbile, J. Cai, and X. S. Shen, "Networking Architecture and Key Supporting Technologies for Human Digital Twin in Personalized Healthcare: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2023, doi: 10.1109/COMST.2023.3308717.

[5] D. Systems, https://www.3ds.com/products-services/simulia/solutions/life-sciences-healthcare/living-heart-human-model/. Accessed on November 2023.

[6] Y. Wang, Z. Su, S. Guo, M. Dai, T. H. Luan, and Y. Liu, "A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects," *IEEE Internet of Things Journal*, vol. 10, no. 17, pp. 14 965–14 987, 2023.

[7] H. Elayan, M. Aloqaily, and M. Guizani, "Digital Twin for Intelligent Context-Aware IoT Healthcare Systems," *IEEE Internet of Things Journal*, vol. 8, no. 23, pp. 16 749–16 757, 2021.

[8] H. Yi, "Improving cloud storage and privacy security for digital twin based medical records," *Journal of Cloud Computing*, vol. 12, no. 1, p. 151, 2023.

[9] 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," *Computer Communications*, vol. 197, pp. 173–185, 2023.

[10] "Cost of a data breach report 2023," https://www.ibm.com/reports/data-breach? Accessed on November 2023.

[11] A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston, and Y. Zhang, "Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications," *IEEE Access*, vol. 6, pp. 33 552–33 567, 2018.

[12] Y. Chen, F. Yin, S. Hu, L. Sun, Y. Li, B. Xing, L. Chen, and B. Guo, "ECC-Based Authenticated Key Agreement Protocol for Industrial Control System," *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 4688–4697, 2023.

[13] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the Security: An ECC-Based Authentication Scheme for Internet of Drones," *IEEE Systems Journal*, vol. 15, no. 3, pp. 4431–4438, 2021.

[14] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, "A Secure Three-Factor User Authentication Protocol With Forward Secrecy for Wireless Medical Sensor Network Systems," *IEEE Systems Journal*, vol. 14, no. 1, pp. 39–50, 2020.

[15] S. Zou, Q. Cao, C. Wang, Z. Huang, and G. Xu, "A Robust Two-Factor User Authentication Scheme-Based ECC for Smart Home in IoT," *IEEE Systems Journal*, vol. 16, no. 3, pp. 4938–4949, 2022.

[16] S. Das and S. Namasudra, "Multiauthority CP-ABE-based Access Control Model for IoT-enabled Healthcare Infrastructure," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 821–829, 2023.

[17] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5914–5925, 2021.

[18] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Symposium on Foundations of Computer Science (SFCS'94)*, Santa Fe, NM, USA, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[19] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," in *Symposium on Theory of Computing (STOC'96)*, Philadelphia, Pennsylvania, USA, 1996, pp. 212–219, doi: 10.1145/237814.237866.

[20] D. Coppersmith, "An approximate Fourier transform useful in quantum factoring," 2002, https://arxiv.org/abs/quant-ph/0201067.

[21] W. Wang, H. Huang, F. Xiao, Q. Li, L. Xue, and J. Jiang, "Computation-transferable authenticated key agreement protocol for smart healthcare," *Journal of Systems Architecture*, vol. 118, p. 102215, 2021.

[22] Y.-F. Chang, C.-Y. Tsai, and W.-L. Tai, "Comments on a Computation-Transferable Authenticated Key Agreement Protocol for Smart Healthcare," in *International Conference on Applied System Innovation (ICASI'23)*, Chiba, Japan, 2023, pp. 62–64, doi: 10.1109/ICASI57738.2023.10179501.

[23] N. Zhang, Q. Jiang, L. Li, X. Ma, and J. Ma, "An efficient three-factor remote user authentication protocol based on BPV-FourQ for internet of drones," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 3319–3332, 2021.

[24] Y. Park, D. Ryu, D. Kwon, and Y. Park, "Provably Secure Mutual Authentication and Key Agreement Scheme Using PUF in Internet of Drones Deployments," *Sensors*, vol. 23, no. 4, 2023.

[25] V. Dabra, A. Bala, and S. Kumari, "LBA-PAKE: Lattice-Based Anonymous Password Authenticated Key Exchange for Mobile Devices," *IEEE Systems Journal*, vol. 15, no. 4, pp. 5067–5077, 2021.

[26] R. Ding, C. Cheng, and Y. Qin, "Further Analysis and Improvements of a Lattice-Based Anonymous PAKE Scheme," *IEEE Systems Journal*, vol. 16, no. 3, pp. 5035–5043, 2022.

[27] W. Yuanbing, L. Wanrong, and L. Bin, "An Improved Authentication Protocol for Smart Healthcare System Using Wireless Medical Sensor Network," *IEEE Access*, vol. 9, pp. 105 101–105 117, 2021.

[28] J. Lee, J. Oh, and Y. Park, "A Secure and Anonymous Authentication Protocol Based on Three-Factor Wireless Medical Sensor Networks," *Electronics*, vol. 12, no. 6, 2023.

[29] S. H. Islam and S. Basu, "PB-3PAKA: Password-based three-party authenticated key agreement protocol for mobile devices in post-quantum environments," *Journal of Information Security and Applications*, vol. 63, p. 103026, 2021.

[30] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2649–2656, 2022.

[31] S. Shihab and R. AlTawy, "Lightweight Authentication Scheme for Healthcare With Robustness to Desynchronization Attacks," *IEEE Internet of Things Journal*, vol. 10, no. 20, pp. 18 140–18 153, 2023.

[32] H. Qiao, X. Dong, Q. Jiang, S. Ma, C. Liu, N. Xi, and Y. Shen, "Anonymous Lightweight Authenticated Key Agreement Protocol for Fog-Assisted Healthcare IoT System," *IEEE Internet of Things Journal*, vol. 10, no. 19, pp. 16 715–16 726, 2023.

[33] L. Zhang, Y. Zhu, W. Ren, Y. Zhang, and K.-K. R. Choo, "Privacy-Preserving Fast Three-Factor Authentication and Key Agreement for IoT-Based E-Health Systems," *IEEE Transactions on Services Computing*, vol. 16, no. 2, pp. 1324–1333, 2023.

[34] Y.-T. Huang, T.-S. Chen, and S.-D. Wang, "Authenticated Key Agreement Scheme for Fog Computing in a Health-Care Environment," *IEEE Access*, vol. 11, pp. 46 871–46 881, 2023.

[35] C. Wang, D. Wang, Y. Duan, and X. Tao, "Secure and Lightweight User Authentication Scheme for Cloud-Assisted Internet of Things," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2961–2976, 2023, doi: 10.1109/TIFS.2023.3272772.

[36] D. Mishra, M. Singh, P. Reval, K. Pursharthi, N. Kumar, A. Barnawi, and R. Rathore, "Quantum-safe Secure and Authorized Communication Protocol for Internet of Drones," *IEEE Transactions on Vehicular Technology*, pp. 1–10, 2023, doi: 10.1109/TVT.2023.3292169.

[37] P. Rewal, M. Singh, D. Mishra, K. Pursharthi, and A. Mishra, "Quantum-safe three-party lattice based authenticated key agreement protocol for mobile devices," *Journal of Information Security and Applications*, vol. 75, p. 103505, 2023.

[38] H. Ghaemi and D. Abbasinezhad-Mood, "Novel Blockchain-Integrated Quantum-Resilient Self-Certified Authentication Protocol for Cross-Industry Communications," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 5, pp. 4493–4502, 2024.

[39] D. Abbasinezhad-Mood and H. Ghaemi, "Dual-Signature Blockchain-Based Key Sharing Protocol for Secure V2V Communications in Multi-Domain IoV Environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 10, pp. 13 407–13 416, 2024.

[40] A. Shahidinejad and D. Abbasinezhad-Mood, "Ultra-Lightweight and Secure Blockchain-Assisted Charging Scheduling Scheme for Vehicular Edge Networks by Utilization of NanoPi NEO," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 8, pp. 8116–8123, 2022.

[41] H. Ghaemi, D. Abbasinezhad-Mood, A. Ostad-Sharif, and Z. Alizadehsani, "Novel blockchain-assisted fault-tolerant roaming authentication protocol for mobility networks without home agent entanglement," *Journal of Network and Computer Applications*, vol. 224, p. 103843, 2024.

[42] J. Zhang, Z. Zhang, J. Ding, M. Snook, and Ö. Dagdelen, "Authenticated key exchange from ideal lattices," in *Advances in Cryptology-EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Sofia, Bulgaria, 2015, pp. 719–751.

[43] J. Ding, S. Alsayigh, J. Lancrenon, S. Rv, and M. Snook, "Provably secure password authenticated key exchange based on RLWE for the post-quantum world," in *Cryptographers' Track at the RSA conference*, San Francisco, CA, USA, 2017, pp. 183–204.

[44] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Advances in Cryptology – EUROCRYPT 2010*, French Riviera, 2010, pp. 1–23.

[45] Q. Feng, D. He, S. Zeadally, N. Kumar, and K. Liang, "Ideal Lattice-Based Anonymous Authentication Protocol for Mobile Devices," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2775–2785, 2019.

[46] V. Lyubashevsky and D. Micciancio, "On bounded distance decoding, unique shortest vectors, and the minimum distance problem," in *Advances in Cryptology - CRYPTO 2009*, Santa Barbara, CA, USA, 2009, pp. 577–594.

[47] J. Chen, C. Yi, S. D. Okegbile, J. Cai, and X. Shen, "Networking Architecture and Key Supporting Technologies for Human Digital Twin in Personalized Healthcare: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 706–746, 2024.

[48] J. Chen, Y. Shi, C. Yi, H. Du, J. Kang, and D. Niyato, "Generative-AI-Driven Human Digital Twin in IoT Healthcare: A Comprehensive Survey," *IEEE Internet of Things Journal*, vol. 11, no. 21, pp. 34 749–34 773, 2024.

[49] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[50] R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'02)*, Amsterdam, The Netherlands, 2002, pp. 337–351.

[51] R. M. Daniel, A. Thomas, E. B. Rajsingh, and S. Silas, "A strengthened eCK secure identity based authenticated key agreement protocol based on the standard CDH assumption," *Information and Computation*, vol. 294, p. 105067, 2023.

[52] C. C. Zheng Wei, C. Chai Wen, and J. Alawatugoda, "Review on Leakage Resilient Key Exchange Security Models," *International Journal of Communication Networks and Information Security*, vol. 11, no. 1, 2022.

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

[54] C. Xu, F. Erata, and J. Szefer, "Exploration of Quantum Computer Power Side-Channels," 2023, https://doi.org/10.48550/arXiv.2304.03315. Accessed on Oct 2023.

[55] S. Bhattacharya, Ó. García-Morchón, R. Rietman, and L. Tolhuizen, "spKEX: An optimized lattice-based key exchange," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 709, 2017, https://eprint.iacr.org/2017/709.pdf.

[56] D. Abbasinezhad-Mood and M. Nikooghadam, "An Anonymous ECC-Based Self-Certified Key Distribution Scheme for the Smart Grid," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 7996–8004, 2018.

[57] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *8th International Workshop on Theory and Practice in Public Key Cryptography (PKC'05), Lecture Notes in Computer Science*, vol. 3386, Les Diablerets, Switzerland, 2005, pp. 65–84.

[58] C. Cremers, "The Scyther Tool," 2006, https://people.cispa.io/cas.cremers/scyther/. Accessed on June 2023.

[59] C. J. F. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols," in *Computer Aided Verification*, A. Gupta and S. Malik, Eds. Princeton, NJ, USA: Springer Berlin Heidelberg, 2008, pp. 414–418.

[60] J. Cao, M. Ma, Y. Fu, H. Li, and Y. Zhang, "CPPHA: Capability-Based Privacy-Protection Handover Authentication Mechanism for SDN-Based 5G HetNets," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1182–1195, 2021.

[61] D. Abbasinezhad-Mood, S. M. Mazinani, M. Nikooghadam, and A. Ostad-Sharif, "Efficient Provably-Secure Dynamic ID-Based Authenticated Key Agreement Scheme With Enhanced Security Provision," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1227–1238, 2022.

[62] Y. Chen and P. Q. Nguyen, "Bkz 2.0: Better lattice security estimates," in *Advances in Cryptology – ASIACRYPT 2011*, Seoul, South Korea, 2011, pp. 1–20.

[63] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan, and D. Stebila, "Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE," in *ACM SIGSAC Conference on Computer and Communications Security (CCS'16)*, Vienna, Austria, 2016, pp. 1006–1018.

[64] P. M. Sosa, "Simple RLWE-KEX example using Python," 2017, https://github.com/pmsosa/rlwe-kex/blob/master/rlwe_kex.py.

[65] A. Irshad, G. A. Mallah, M. Bilal, S. A. Chaudhry, M. Shafiq, and H. Song, "SUSIC: A Secure User Access Control mechanism for SDN-enabled IIoT and Cyber Physical Systems," *IEEE Internet of Things Journal*, pp. 1–1, 2023, doi: 10.1109/JIOT.2023.3268474.

Basudeb Bera received his Ph.D. degree in computer science and engineering from the Center for Security, Theory and Algorithmic Research, IIIT Hyderabad, India, in 2022. He also received his M.Sc. degree in mathematics and computing in 2014 from IIT (ISM) Dhanbad, India, and M.Tech. degree in computer science and data processing in 2017 from IIT Kharagpur, India. He is currently working as a post-doctoral researcher on Security for the Internet of Intelligence in Next Generation Cellular Networks in the Department of Electrical and Computer Engineering, National University of Singapore (NUS), Singapore. He also worked as a postdoctoral research fellow on 5G security at Singapore University of Technology and Design (SUTD), Singapore. His research interests are cryptography, network security, blockchain technology, AI/ML security and post-quantum protocols. He has published more than 30 papers in international journals and conferences in his research areas.

Ashok Kumar Das (Senior Member, IEEE) received a Ph.D. degree in computer science and engineering, an M.Tech. degree in computer science and data processing, and an M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently a full Professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India. He is an adjunct professor at Korea University, South Korea. He was also a visiting research professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA 23435, USA. His research interests include cryptography, system and network security, blockchain, security in the Internet of Things (IoT), Internet of Vehicles (IoV), Internet of Drones (IoD), smart grids, smart city, cloud/fog computing, intrusion detection, AI/ML security, and post-quantum cryptography. He has authored over 470 papers in international journals and conferences in the above areas, including over 405 reputed journal papers. He was a 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 is/was on the editorial board of IEEE Transactions on Information Forensics and Security, IEEE Systems Journal, Journal of Network and Computer Applications (Elsevier), Computer Communications (Elsevier), Journal of Cloud Computing (Springer), Cyber Security and Applications (Elsevier), Alexandria Engineering Journal (Elsevier), International Journal of Communication Systems (Elsevier), IET Communications, KSII Transactions on Internet and Information Systems, and International Journal of Internet Technology and Secured Transactions (Inderscience). He also severed as one of the Technical Program Committee Chairs of the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, June 2019, International Conference on Applied Soft Computing and Communication Networks (ACN'20), October 2020, Chennai, India, second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, October 2020, and International Conference on Applied Soft Computing and Communication Networks (ACN'23), December 2023, Bangalore, India. His Google Scholar h-index is 93 and i10-index is 304 with over 25,600 citations.

Biplab Sikdar (Fellow, IEEE) received the B.Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He is a Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, where he serves as the Head of Department of the Department of Electrical and Computer Engineering. He was an Assistant Professor from 2001 to 2007 and an Associate Professor from 2007 to 2013 with the Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute from 2001 to 2013. His research interests include IoT and cyber-physical system security, network security, and network performance evaluation. Dr. Sikdar served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012 and an Associate Editor for the IEEE Transactions on Mobile Computing from 2014 to 2017. He is a member of Eta Kappa Nu and Tau Beta Pi.