Quantum-Safe Digital Twin Authentication for ML-Driven Early Disease Detection in Healthcare Systems

Abhishek Kumar Pandey, Basudeb Bera, Anusha Vangala, Ashok Kumar Das, *Senior Member, IEEE*, Youngho Park, *Member, IEEE*, Biplab Sikdar, *Fellow, IEEE*

***Abstract*— The current healthcare ecosystem heavily relies on smart services such as disease detection, intelligent drug recommendation, and real-time patient monitoring. In such a scenario, ensuring patient privacy and securing sensitive health data present significant challenges. To address these issues, this article proposes a secure digital twin-enabled ML-based disease detection framework. The proposed framework allows real patients to securely synchronize their real-time health data within a privacy-preserving environment to their corresponding digital twin, which is equipped with ML-based disease detection capabilities. This enables patients to effectively monitor their health vitals and securely identify potential future risks. To ensure security and robustness, the proposed system employs a lattice-based authentication scheme that is resistant to quantum threats. Furthermore, the article conducts experiments on both the authentication mechanism and the ML-based disease detection process to evaluate the robustness of the proposed approach. The results demonstrate that a secure data pipeline from data collection to processing on the digital twin server is essential, as experiments with white-box attacks reveal that models can collapse easily in the absence of proper security mechanisms.**

***Index Terms*— Smart Healthcare, Post-quantum Authentication, ML-based disease detection, Digital Twin, Security.**

I. Introduction

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (Ministry of Science and ICT) (RS-2024-00450915).
(Corresponding authors: Ashok Kumar Das; Youngho Park).

Abhishek Kumar Pandey is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India (e-mail: abhishek.pandey@research.iiit.ac.in).

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

Anusha Vangala is with the Department of Computer Science and Engineering, National Institute of Technology, Warangal 506 004, India (e-mail: anusha_vangala@nitw.ac.in).

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India, and also with the Department of Computer Science and Engineering, College of Informatics, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul 02841, South Korea (e-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in).

Youngho Park is with the School of Electronics Engineering, Kyungpook National University, Daegu 41566, Republic of Korea (e-mail: parkyh@knu.ac.kr).

THE modern smart healthcare industry is increasingly dependent on intelligent and automated services designed to minimize human intervention in complex medical processes such as drug recommendation, disease diagnosis, and telemedicine. Among these, machine learning (ML)-based disease detection has emerged as a vital and transformative component of contemporary healthcare systems.

To further enhance the efficiency and precision of such systems, the integration of *Digital Twin* (DT) technology has gained considerable attention. DTs enable healthcare organizations to create a virtual representation of a patient, allowing for advanced disease prediction and treatment simulation without physically impacting the real patient. This integration significantly strengthens the ML-based disease detection process by facilitating continuous monitoring, adaptive learning, and personalized care.

Despite these advantages, serious challenges persist in terms of security and trust. The synchronization process responsible for aligning the real patient's physiological state with its corresponding digital counterpart introduces multiple vulnerabilities. Any compromise in this synchronization or data transmission phase may lead to inaccurate diagnostics, data leakage, or even adversarial manipulation of medical insights, highlighting the critical need for secure and trustworthy synchronization mechanisms in ML-driven healthcare decisions.

To address and secure the synchronization process between the real and digital twin patients, this article proposes a quantum-safe hybrid authentication scheme. The primary objective of this scheme is to ensure that real-time patient data can be securely synchronized with its corresponding digital twin without any possibility of interception or manipulation during transmission. The proposed authentication mechanism is designed to be resistant to both classical and emerging quantum attacks, providing long-term robustness and forward security. By incorporating post-quantum cryptographic primitives, the scheme not only mitigates the risk of current Cyber threats but also proactively safeguards against the anticipated capabilities of quantum adversaries, ensuring reliable and future-proof data synchronization within intelligent healthcare systems.

The rest of the paper is organized in the following way. In Section II, we critically review and analyze the existing works from the literature, specifically those proposed recently. Next,

we discuss the network architecture and threat model used in the proposed scheme in Section III. The basic mathematical foundation of lattice theory and computational hard problems, such as Ring Learning With Error (RLWE), is provided in Section IV. We then provide the details on various phases related to our proposed quantum-safe digital twin authentication scheme in Section V. In Section VI, we provide the detailed security analysis of the proposed scheme. Furthermore, in Section VII, to demonstrate the effectiveness of the proposed authentication scheme, we conduct various experiments using an ML-based early disease detection process in different scenarios. In Section VIII, we then conduct a comparison analysis of the proposed scheme with the existing schemes. Finally, the concluding remarks and the limitations of the work are highlighted in Section IX.

II. Related Work

In this section, we analyze the existing literature relevant to the topic of this study. Although there are no works that directly address all aspects of the proposed framework, several studies explore partial components related to our research. To provide a clear and structured understanding, this section categorizes and discusses the reviewed literature under distinct thematic areas corresponding to the major components of this work. The classification of these literature sources and their respective discussions is presented as follows.

A. Secure disease detection and Digital Twin in Healthcare

In this subsection, we analyze studies that focus on secure disease prediction mechanisms. Gopalan et al. [1] proposed a privacy-preserving secure disease prediction scheme based on logarithmic round elliptic curve cryptography. The authors introduced an authentication mechanism that allows patients to use mobile healthcare applications to securely analyze their health conditions. Furthermore, Ren et al. [2] presented a study on disease detection for Alzheimer's disease using digital twin technology; however, the work does not address the security aspects of the system. Similarly, Amofa et al. [3] proposed a secure disease detection framework by integrating digital twin technology with blockchain-based smart contracts. Additionally, Abdullah et al. [4] explored the use of digital twin technology for identifying health vulnerabilities in adults through deep learning techniques, though their study also lacks a discussion on the security considerations.

A study by Christos et al. [5] discusses secure big data transmission and storage in cloud-based healthcare environments. Their approach employs DT technology as the primary component to ensure secure data transmission and storage within the cloud infrastructure. Furthermore, Jameil and Raweshidy [6] proposed a real-time healthcare monitoring system that leverages artificial intelligence (AI) and secure communication techniques to enhance patient diagnosis and monitoring through digital twin integration. Additionally, Zhao et al. [7] presented a framework for infectious disease detection, wherein hospitals collect patients' electronic health records (EHRs) and securely outsource the encrypted EHRs to a contracted cloud service for further analysis.

B. Quantum Secure Authentication

In this subsection, we have reviewed several quantum-secure authentication schemes implemented across different domains to understand their design principles and applicability. Babu et al. [8] provided a detailed review of quantum secure authentication and key agreement protocols. They explored different cryptographic methods used in the field of quantum computing and how they evolve for IoT-enabled applications.

Chaudhary et al. [9] proposed a three-party post-quantum authentication protocol that integrates Learning With Errors (LWE) and Elliptic Curve Cryptography (ECC) to enhance security. Similarly, Rewal et al. [10] introduced a lattice-based authentication framework enabling mobile devices to establish secure key agreements under post-quantum settings.

Cui et al. [11] presented a post-quantum authentication scheme for vehicular DT systems, utilizing the Ring Learning With Errors (RLWE) computational hardness assumption to establish secure key exchange. Khalid et al. [12] developed a robust end-to-end encryption and mutual authentication mechanism designed to protect intelligent transportation systems from quantum attacks using post-quantum cryptographic primitives. Furthermore, Ahmad and Jagatheswari [13] proposed a three-party post-quantum authentication scheme designed for the medical domain, ensuring strong resistance against quantum adversaries while maintaining efficient communication overhead.

C. Research Gap and Contribution

After carefully analyzing the existing literature, the authors have identified several critical research gaps that must be addressed to enhance the robustness and security of current healthcare systems, particularly those leveraging digital twin and ML-based disease detection. The major research gaps are summarized as follows:

- **Security against quantum threats:** Most existing studies on ML-based disease detection operate under classical threat models and do not consider quantum adversaries. This omission poses a serious challenge, as the rapid advancement of quantum computing threatens to compromise traditional cryptographic mechanisms, leaving healthcare systems vulnerable to future attacks.
- **Secure synchronization between real patients, digital twins, and ML-based disease detection:** Although several studies have explored DT technology in healthcare, very few have addressed the secure integration of digital twins with ML-driven disease detection processes. Ensuring secure synchronization between the real patient data, its digital representation, and the ML analytics layer remains an open and critical challenge.

In summary, we can say that all the existing digital-enabled healthcare research mainly utilizes classical technology, particularly to ensure security. To address the identified research gaps, this article makes the following contributions. A lattice-based hybrid authentication scheme is proposed for DT technology to enable secure ML-based disease detection. This framework ensures that the disease detection process receives secure and authenticated input from the digital twin source,

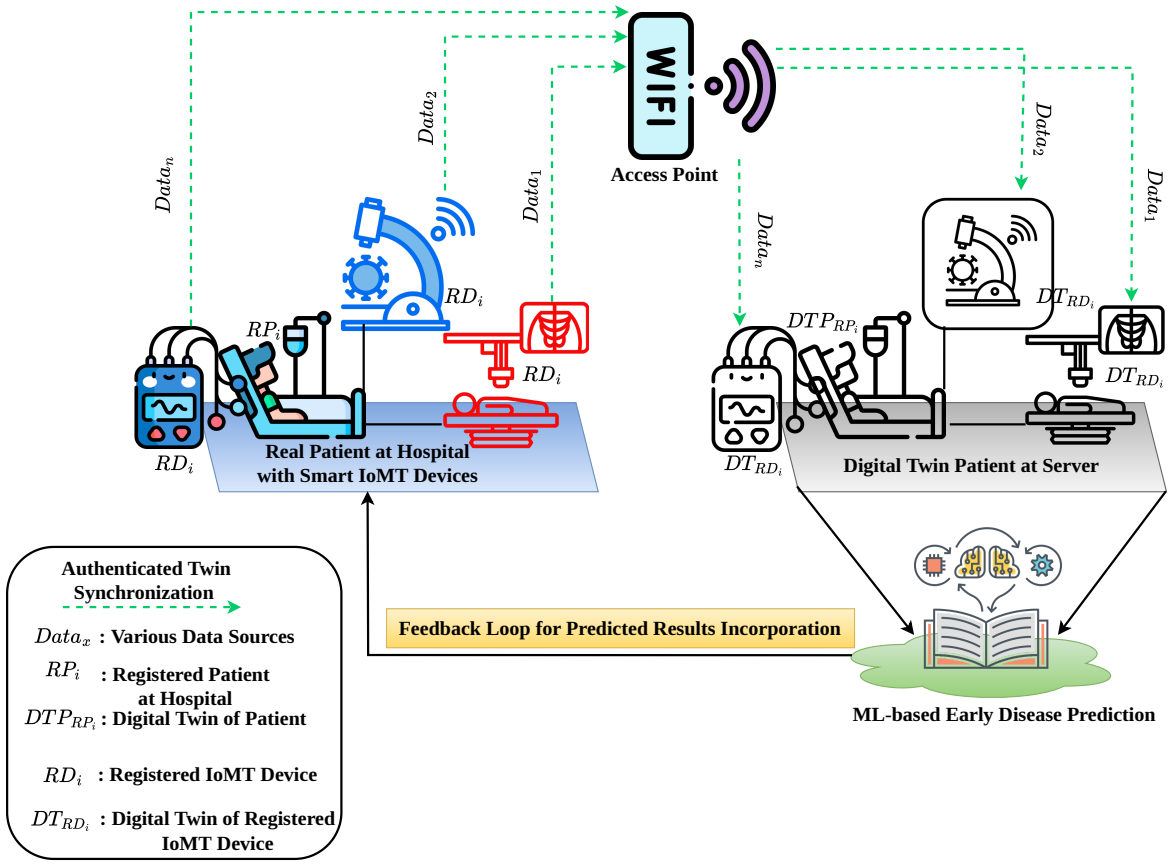


Fig. 1: Network model

as all participating entities are quantum-safe and mutually authenticated. This design guarantees data integrity, authenticity, and confidentiality throughout the ML-based disease detection pipeline. This is a quantum-secure authentication framework specifically designed to strengthen the digital twin ecosystem against threats of the quantum era, which ensures that the ML-based disease detection process operates securely, efficiently, and resiliently against both classical and quantum adversaries.

III. System Model

In this section, we have discussed the architecture of the designed DT-enabled ML-based disease detection system and discussed its working mechanism. Furthermore, we have analyzed the attacker model and identified potential real-world threats that can target the proposed network framework.

A. Network Architecture

The network architecture designed for ML-based disease detection using DT technology is illustrated in Fig. 1. The proposed network model consists of three main components: the real patient and associated ***IoMT devices***, an ***access point*** acting as the intermediary entity, and the ***digital twin*** of the real hospital patient hosted on the server. The architecture demonstrates how the physiological data and health conditions of the real patient are continuously synchronized in real time with the corresponding digital twin (DT). The DT, equipped with ML-based disease detection capabilities, performs real-time analysis on the synchronized data to identify potential diseases or anomalies. Furthermore, the model incorporates a feedback loop mechanism that allows the digital twin to send analyzed results and medical insights back to the real-world patient via the hospital network, enabling adaptive and intelligent healthcare monitoring.

The proposed network architecture provides a more effective mechanism for digital twin synchronization compared to edge-enabled or purely privacy-preserving digital twin architectures. In the access point-enabled mechanism, data from multiple heterogeneous devices, including multimodal sources, can be aggregated efficiently at a single point before synchronization process. In contrast, edge-enabled architectures mainly maintain only a fragmented or partial view of the data, as each edge node processes limited local information independently.

The access point node facilitates unified and complete synchronization of the digital twin in a single attempt. As a result, it improves consistency and reduces synchronization overhead. Moreover, access point-enabled devices are physically closer to the patient, which helps in enabling timely and reliable real-time data acquisition. For these reasons, the proposed architecture incorporates the access point node as an intermediate synchronization initiation entity. Thus, the proposed architecture ensures efficient, comprehensive, and real-time digital twin updates.

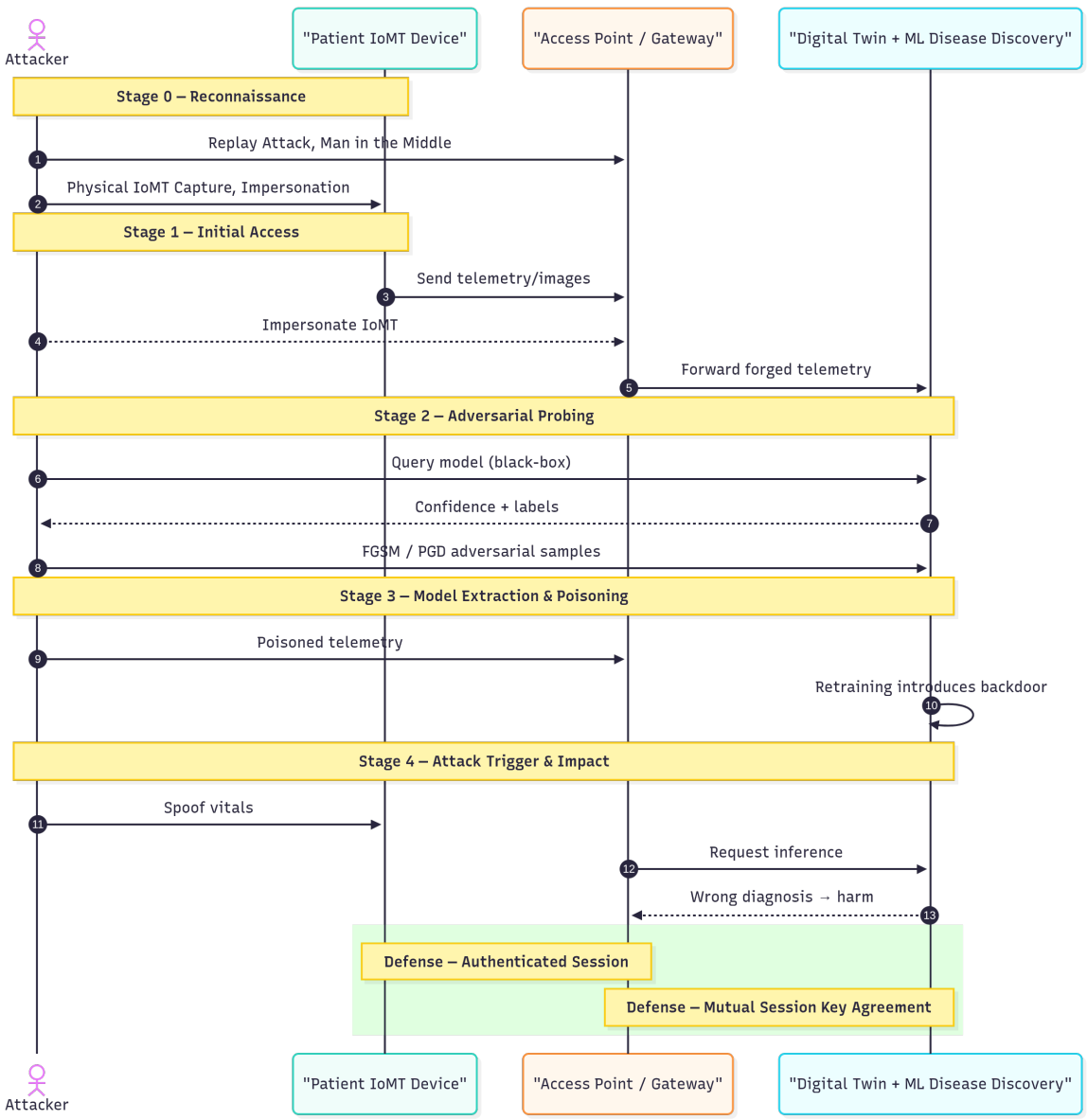


Fig. 2: Attacker model

B. Attack Model

The network architecture is complex and encompasses multiple attack surfaces that adversaries can exploit using various techniques. To clarify the attacker model and its workflow, Fig. 2 shows a sequence diagram that outlines how an adversary can compromise the system and the resulting impacts. Initially, the attacker leverages weak or improperly configured cryptographic authentication through replay, Man-in-the-Middle (MiTM), impersonation attacks, or physically capturing IoMT devices to obtain an entry point into the network. Once initial access is gained, the adversary can compromise sessions, inject tampered or poisoned inputs, and launch white-box or black-box attacks against the disease-discovery server.

These chained exploits are enabled primarily by vulnerable authentication mechanisms that allow unauthorized access to the digital twin synchronization channel. The consequences are severe: an attacker who hijacks a session can manipulate the digital twin's input data or inject malicious vitals, causing incorrect or dangerous diagnostic outputs. Such integrity and availability breaches undermine the reliability of ML-based disease detection and can lead to harmful clinical decisions.

After defining the system-level attacker scenario, we ensure that both practical and theoretical security aspects are addressed, which cover threats arising from communication interception, replay, impersonation, and potential post-quantum adversarial capabilities. To ensure comprehensive identification of threat vectors within the authentication scheme, we have included several formal threat models, like the widely-recognized "Dolev-Yao (DY) Threat Model" [14], "Honest-but-Curious (HBC) Model", and "Canetti and Krawczyk's Model (CK-Adversary Model" [15]. A detailed explanation of

these threat models is provided in [16]. These models enable a systematic evaluation of potential attack surfaces, which helps to validate the robustness of the proposed quantum-safe authentication scheme. For the real-world scenario consideration, we assume that the adversary can intercept the communication, harm the integrity of the message exchanges, and exploit insider-authenticated nodes as well. The adversary can also replay messages and manipulate the communication messages exchanged between the users.

IV. Preliminaries

In this section, we discuss the mathematical preliminaries essential for designing the proposed quantum-safe lattice-based authentication scheme. These preliminaries provide the foundational computational hardness assumptions that guarantee the scheme's security against both classical and quantum adversaries. Specifically, this section elaborates on the underlying lattice problems and their mathematical formulations, which form the basis for constructing the secure key exchange and authentication mechanisms utilized in the proposed framework.

Let $\mathbb{R}_q$ denotes a polynomial quotient ring of $\mathbb{R}$ with modulo q and defined as $\mathbb{R}_q = \frac{\mathbb{Z}_q[x]}{<x^n+1>}$, where odd large prime $q \in \mathbb{Z}$, $\mathbb{Z}$ is a set of integers, $\mathbb{Z}_q[x]$ ring polynomial over $\mathbb{Z}_q$, and $< x^n+1 >$ is an irreducible $2n^{th}$ cyclotomic polynomial over $\mathbb{Z}$. We also consider that the function χ_β is a discrete Gaussian distribution over $\mathbb{R}_q$, with $\beta > 0$ being the standard deviation of χ_β. Let a set $S = \{-\lfloor \frac{q-1}{2} \rfloor, \cdots, \lfloor \frac{q-1}{2} \rfloor\}$ and let a subset $\bar{S}$ of S as $\bar{S} = \{-\frac{q}{4}, \cdots, \frac{q}{4}\}$ which is the middle half S. We define a characteristic function $Cha(\cdot)$ as $Cha(x) = 0$ if $x \in \bar{S}$ and 1 otherwise and a modular function $Mod_2 : \mathbb{Z}_q \times \{0,1\} \rightarrow \{0,1\}$, is defined as $Mod_2(x,y) = (x + y \cdot \frac{(q-1)}{2}) \pmod q \pmod 2$ [17].

Ring Learning With Error (RLWE) Problem: Let $\mathbf{D}_{x,\chi_\beta}$ be a distribution of $(x, x \cdot r + e)$ and r be fix sample $\in \mathbb{R}_q$, respectively, where $(x, e) \leftarrow \mathbb{R}_q \times \chi_\beta$. Then, the $RLWE(q, \beta)$ states that it is hard for any probabilistic polynomial time algorithm to distinguish $\mathbf{D}_{x,\chi_\beta}$ from the uniform distribution on $\mathbb{R}_q \times \mathbb{R}_q$ with only polynomial many samples [17].

To substantiate the suitability of RLWE for authentication design in sensitive and security-critical domains, we examine its security properties in relation to the classical Learning With Errors (LWE) hard problem in lattice theory. RLWE extends LWE by introducing an algebraic structure based on polynomial rings rather than vector spaces, which enables more compact representations and efficient arithmetic operations. Moreover, RLWE offers strong worst-case to average-case hardness reductions with tighter security guarantees. Compared to the standard LWE, RLWE also requires significantly smaller key sizes, which leads to reduced computational and communication overheads. These characteristics make the RLWE particularly well-suited for authentication schemes, because it can provide a strong resistance against both classical and quantum adversaries while maintaining practical efficiency. Consequently, RLWE forms a robust and scalable foundation for secure authentication in sensitive application domains like healthcare.

V. The Proposed Authentication

The proposed authentication scheme is divided into multiple phases to establish a secure and structured pipeline that enables the real patient to synchronize real-time data securely with its corresponding digital twin. This synchronization further facilitates a protected ML-based disease detection process. The designed phases are as follows: (i) initialization phase, (ii) registration phase, (iii) secure data collection phase, (iv) secure ML-based disease detection phase, and (v) secure feedback phase. Each of these phases contributes to ensuring a quantum-safe and robust pipeline for real-time digital twin synchronization and secure disease detection.

A. System Initialization Phase

Step 1: The registration authority (RA) selects initial parameters, such as odd large prime $q \in \mathbb{Z}$ and a security parameter $n \in \mathbb{Z}$. Next, the RA selects polynomial rings $\mathbb{Z}_q[x]$ and polynomial quotient ring $\mathbb{R}_q$ with their usual notions.

Step 2: The RA picks a discrete Gaussian distribution χ_β over R_q, where β is the standard deviation of the distribution. The RA selects a one-way cryptographic hash function $h(\cdot)$ as SHA-256 for post-quantum security.

Step 3: The RA generates a secret key $k \in \mathbb{Z}_q$, and public polynomial $\alpha \in \mathbb{R}_q$. Finally, the RA publishes the parameters $\{n, q, \alpha, \chi_\beta, h(\cdot), \mathbb{R}_q\}$.

B. Registration Phase

Step 1: The RA registers through secure channel of offline medical smart devices MD_is, access points APs, and DT server. The RA selects unique and district identity ID_{MD_l}, two 256-bit primary secret keys as $MK_{MD_l} \in \mathbb{Z}_q$ of MD_l and $MK_{MD_{DT}} \in \mathbb{Z}_q$, and a temporal identity TID_i, an identity ID_i for AP_i.

Step 2: The RA stores the registration information $\{ID_i, TID_i, k\}$, where k is the mutual secret between the AP_i and DT, and shares this information with the server DT, where the digital twins of the physical medical devices are installed with proper software.

Step 3: The RA stores MK_{MD_l} in MD_l's memory and also shares MK_{MD_l} to its access point AP_i securely. Further, the RA stores the second primary key $MK_{MD_{DT}}$ to the MD_l and corresponding DT's memory securely. Note that MK_{MD_l} will be used for secure communication between MD_i and AP_i, and $MK_{MD_{DT}}$ will be used for secure communication between the MD_l and DT.

C. Secure Data Collection Phase

In this phase, a secure session key agreement is established among all three entities of the network model through mutual authentication. This process enables the real patient's IoMT devices to transmit real-time data securely to their corresponding digital twin. A detailed description of the proposed authentication scheme is discussed as follows.

1) Secure Data Exchange between IoMT Wearable Devices and Access Point: The following steps are executed for establishing a long-term key LK_{MD_l,AP_i}:

Step 1: The real patient's medical IoMT device MD_l generates a random (secret) nonce $rn_{MD_l} \in \mathbb{Z}_q$ and the current timestamp CT_{MD_l} to calculate $A_l = rn_{MD_l} \oplus h(MK_{MD_l}||CT_{MD_l})$. Next, MD_l sends the message $\langle A_l, CT_{MD_l} \rangle$ to AP_i.

Step 2: AP_i checks the validity of the message by validating the received timestamp by $|CT^*_{MD_l} - CT_{MD_l}| \leq \triangle T$, where $\triangle T$ is the "maximum transmission delay for a message" and $CT^*_{MD_l}$ denotes the time when the message $\langle A_l, CT_{MD_l} \rangle$ is received by AP_i. If it is valid, AP_i generates a random (secret) nonce $rn_{AP_i} \in \mathbb{Z}_q$ and the current timestamp CT_{AP_i}. AP_i then calculates $rn_{MD_l} = A_l \oplus h(MK_{MD_l}||CT_{MD_l})$, $B_i = rn_{AP_i} \oplus h(MK_{MD_l}||CT_{AP_i})$, long-term key $LK_{AP_i,MD_l} = h(rn_{MD_l}||rn_{AP_i}||MK_{MD_l}||CT_{MD_l}||CT_{AP_i})$ and its verifier $LKV = h(LK_{AP_i,MD_l}||CT_{AP_i})$. Finally, AP_i sends the message $\langle B_i, LKV, CT_{AP_i} \rangle$ to MD_l.

Step 3: After receiving the message $\langle B_i, LKV, CT_{AP_i} \rangle$, MD_l validates the timestamp CT_{AP_i}, and if the timestamp is valid, it proceeds to calculate $rn_{AP_i} = B_i \oplus h(MK_{MD_l}||CT_{AP_i})$, long-term key $LK_{MD_l,AP_i} = h(rn_{MD_l}||rn_{AP_i}||MK_{MD_l}||CT_{MD_l}||CT_{AP_i})$ and its verifier $LKV' = h(LK_{MD_l,AP_i}||CT_{AP_i})$. Now, if $LKV' = LKV$, both MD_l and AP_i share the same long-term key LK_{MD_l,AP_i} $(= LK_{AP_i,MD_l})$ for secure communication of the patient's vitals to AP_i securely.

2) Secure Data Exchange between Access Point and Digital Twin: After a secure session has been successfully established between the MD_i and AP_i, the AP_i proceeds to develop a secure communication session with the corresponding patient's digital twin DT through the following steps.

Step 1: The AP_i selects the random secrets as $r_i, e_i \in \chi_\beta$, current time stamp TS_1, and calculates it corresponding lattice-based public key as $x_i = \alpha \cdot r_i + 2 \cdot e_i$. After this, the AP_i calculates the $V = h(ID_i \,||TID_i \,||TS_1 \,||x_i \,||k)$ and the prepares the message $M_1 = \{x_i, TS_1, TID_i, V\}$ and send it to the DT through an open channel.

Step 2: After receiving the M_1 from the AP_i the DT checks the current timestamp and validate its freshness. If the timestamp validity is active the DT calculates the value $V^* = h(ID_i \,||TID_i \,||TS_1 \,||x_i \,||k)$ and verifies $V = V^*$. If it is valid, the DT selects the random secret as $r_j, e_j \in \chi_\beta$ and its corresponding public key as $y_i = \alpha \cdot r_j + 2 \cdot e_j$ along with the current timestamp TS_2. Then, the DT calculates the value $Z_i = x_i \cdot r_j$, $W_i = Cha(Z_i)$, $U_i = Mod_2(Z_i, W_i)$. After this the DT computes $W^*_i = W_i \oplus h(ID_i \,||TS_2 \,||k)$, and session key $sk = h(k||\, TS_1||\, TS_2||\, U_i||\, TID_i||\, ID_i \,||x_i \,||y_i)$. Thereafter, it selects a new TID^n_i and calculates $TID^* = TID^n_i \oplus h(sk||TID_i \,||TS_1 \,||TS_2)$, and session key verifier $skv = h(sk \,||TID^* \,||ID_i \,||TS_1 \,||y_i \,||W^*_i \,||TS_2)$. After all these calculates the DT prepares the message M_2 as $\{skv, TID^*_i, y_i, W^*_i, TS_2\}$ and sends this M_2 through a open channel.

Step 3: After receiving the M_2 the AP_i first checks $|TS^*_2 - TS_2| < \Delta T$, if the timestamp is fresh then the AP_i compute $Z^*_i = y_i \cdot r_i$, $W_i = W^*_i \oplus h(ID_i \,||TS_2 \,||k)$, $U'_i = Mod_2(Z^*_i, W_i)$. Then computes the session key as $sk' = h(k||\, TS_1||\, TS_2||\, U'_i||TID_i||\, ID_i \,||x_i \,||y_i)$ and calculate the new temporal identity as $TID^n_i = TID^*_i \oplus h(sk||TID_i \,||TS_1 \,||TS_2)$. After all these calculates the AP_i calculates the session key verifier as $skv' = h(sk' \,||TID^* \,||ID_i \,||TS_1 \,||y_i \,||W^*_i \,||TS_2)$ and verify $skv' = skv$, if the condition exist, update TID_i with TID^n_i. Now, the AP_i selects the current timestamp TS_3 and compute $ack = h(sk' \,||TS_3 \,||TID^n_i)$. After this, AP_i prepares the acknowledgment message as $M_3 = \{ack, TS_3\}$.

Step 4: After receiving the M_3, DT verifies $|TS^*_3 - TS_3| < \Delta T$. If yes,compute $ack' = h(sk \,||TS_3 \,||TID^n_i)$. Verify $ack' = ack$. If yes, update TID_i with TID^n_i, and both the devices now share the same session key.

Access Point (AP_i)	Patient's Digital Twin (DT)
Store: $\{ID_i, k, TID_i\}$	Store: $\{ID_i, TID_i, k\}$
Pick $r_i, e_i \in \chi_\beta$, timestamp TS_1, compute $x_i = \alpha \cdot r_i + 2 \cdot e_i$, and $V = h(ID_i \,||TID_i \,||TS_1 \,||x_i \,||k)$	
$\{x_i, TS_1, TID_i, V\}$ →	
	Verify $\|TS^*_1 - TS_1\| < \Delta T$, if yes fetch ID_i and k corr. to TID_i, $V^* = h(ID_i \,||TID_i \,||TS_1 \,||x_i \,||k)$, and verify $V = V^*$. If yes, pick $r_j, e_j \in \chi_\beta$, timestamp TS_2, and compute $y_i = \alpha \cdot r_j + 2 \cdot e_j$, $Z_i = x_i \cdot r_j$, $W_i = Cha(Z_i)$, $U_i = Mod_2(Z_i, W_i)$. Compute $W^*_i = W_i \oplus h(ID_i \,||TS_2 \,||k)$, session key $sk = h(k||\, TS_1||\, TS_2||\, U_i||\, TID_i||\, ID_i \,||x_i \,||y_i)$. Pick a new TID^n_i. Compute $TID^* = TID^n_i \oplus h(sk||TID_i \,||TS_1 \,||TS_2)$, session key verifier $skv = h(sk \,||TID^* \,||ID_i \,||TS_1 \,||y_i \,||W^*_i \,||TS_2)$
Verify $\|TS^*_2 - TS_2\| < \Delta T$. If yes, compute $Z^*_i = y_i \cdot r_i$, $W_i = W^*_i \oplus h(ID_i \,||TS_2 \,||k)$, $U'_i = Mod_2(Z^*_i, W_i)$, $sk' = h(k||\, TS_1||\, TS_2||\, U'_i||TID_i||\, ID_i \,||x_i \,||y_i)$, $TID^n_i = TID^*_i \oplus h(sk||TID_i \,||TS_1 \,||TS_2)$, a verifier $skv' = h(sk' \,||TID^* \,||ID_i \,||TS_1 \,||y_i \,||W^*_i \,||TS_2)$, and verify $skv' = skv$. If yes, update TID_i with TID^n_i. Pick TS_3, $ack = h(sk' \,||TS_3 \,||TID^n_i)$.	← $\{skv, TID^*_i, y_i, W^*_i, TS_2\}$
$\{ack, TS_3\}$ →	
	Verify $\|TS^*_3 - TS_3\| < \Delta T$. If yes, compute $ack' = h(sk \,||TS_3 \,||TID^n_i)$. Verify $ack' = ack$. If yes, update TID_i with TID^n_i

Fig. 3: Summary of authentication between AP_i and DT.

D. Secure ML-Based Early Disease Detection Phase

After establishing a secure session among the entities in the network, the following steps are executed to ensure a secure ML-based disease detection process:

Step 1: The MD_i transmits the input medical data to the AP_i. The AP_i aggregates all incoming data from multiple medical devices into a transaction set defined as $TX = \{T_{MD_1}, T_{MD_2}, T_{MD_3}, \ldots, T_{MD_n}\}$.

Step 2: Once the transactions TX are prepared, the AP_i encrypts them as $TX' = Enc_{sk'}[TX]$ using the established secure session key between the AP_i and the corresponding digital twin (DT). Here, $Enc_k(.)$ represents the encryption using the symmetric key k. The AP_i then transmits the TX' data to the DT.

Step 3: Upon receiving the encrypted transactions TX', the DT decrypts the data using $Dec_{sk}[TX']$ using the shared session key sk', where $Dec_k(.)$ represents the decryption using the symmetric key k. After successful decryption, the DT initiates the ML-based disease detection module, which pre-processes the decrypted input data, executes the disease

classification model in real time, and generates the diagnostic report based on the model's results.

E. Secure Feedback Phase

After finalizing the model's results, the DT server prepares a disease detection report and transmits it securely and directly to the corresponding real patient through the following steps:

Step 1: The DT prepares the disease detection report $Rep_{DD_{DT}}$ and encrypts it using the established shared secret key $MK_{MD_{DT}}$, as $EREP_{DT} = Enc_{MK_{MD_{DT}}}[Rep_{DD_{DT}}]$. After encryption, the DT sends the $EREP_{DT}$ to the real patient's device MD_l.

Step 2: Upon receiving $EREP_{DT}$, the MD_l decrypts the encrypted report using the shared key as $Rep_{DD_{DT}} = Dec_{MK_{MD_{DT}}}[EREP_{DT}]$. If the report is successfully decrypted, the real patient can then utilize the decrypted report for further medical analysis or diagnosis.

F. Real-life Applicability

If we consider the real-life deployment and daily secure operation of the proposed digital twin-based early disease detection framework, its workflow can be described as follows:

Step 1: Initially, all medical devices attached to the patient's body establish a secure session with the nearest access point node deployed within the hospital environment. This secure session is established using the proposed hybrid PQC-based authentication scheme.

Step 2: After the successful start of the secure session between the patient's medical sensors and the access point node, the access point further establishes a secure session with the patient's corresponding digital twin server hosted by the hospital. This session establishment follows the hybrid PQC-based authentication process proposed in this work, which leverages the resource-rich computational capabilities of the server.

Step 3: Once all post-quantum secure sessions are established, the medical devices start transmitting real-time patient data to the access point node. The data is encrypted using the established session keys, and the access point aggregates the received information into a unified multimodal dataset collected from heterogeneous sensors.

Step 4: The access point node securely transmits the aggregated multi-modal data to the authenticated digital twin server. Using the data, the digital twin simulates the physiological condition of the real patient. The integrated ML-based disease detection model analyzes the simulated environment and generates an analytical report indicating the presence or absence of disease.

Step 5: Finally, the analyzed disease detection report is securely transmitted back to the real patient side for further evaluation. Based on physician observations, appropriate medical decisions and treatments can be applied. Any subsequent updates or feedback follow the same secure synchronization process, which ensure continuous, time-to-time secure communication between the real patient and the digital twin.

VI. Security Analysis

For the security analysis, we follow the attack (threat) model described in Section III-B. Other ML-related attacks are explained for the proposed scheme through the experiments discussed in Section VII.

Proposition 1: The proposed scheme is resilient against replay attacks.

Proof: A replay attack on a digital twin will enable a malicious wearable device or access point to re-execute its commands to the digital twin, leading to inaccurate data processing. Our scheme prevents this scenario by enforcing freshness of every message using timestamp checks on CT_{MD_l}, CT_{AP_l}, TS_1, and TS_2, within the permissible delay $\triangle T$. In this way, all the old messages can be easily filtered by the respective recipients to discard them. ■

Proposition 2: The proposed scheme is resilient against man-in-the-middle (MiTM) attacks.

Proof: A malicious adversary may capture the messages exchanged between the wearable devices and the access point or the access point and the digital twin. For a MiTM attack, the adversary tries to modify the message and resend it to the destination. For example, an adversary may modify skv, y_i, or W_i sent by the DT before it reaches AP_i. However, in our scheme, AP_i verifies the correctness of skv, y_i, and W_i on receipt using one-way cryptographic hash $h(\cdot)$, which detects and discards any such modifications. ■

Proposition 3: The proposed scheme is secure against impersonation attacks.

Proof: To impersonate the digital twin, an adversary needs to fabricate the registration information k, x_i computed with AP_i's random secrets, and y_i computed with DT's random secrets. U_i in skv is computed from the Diffie-Hellman-type parameter Z_i at DT and Z_i^* at AP_i, which requires solving the lattice-based RLWE hard problem to be fabricated. Thus, our scheme is secure from impersonation of digital twins. Moreover, due to the post-quantum security of $h(\cdot)$, our scheme is also secure against impersonation of wearable devices. ■

Proposition 4: The proposed scheme is resilient against a physical IoMT wearable device capture attack.

Proof: The wearable devices, being small and highly mobile, are vulnerable to loss or theft. As such, an adversary can easily gain access to the physical wearable device and extract the primary secret MK_{MD_l} from its memory using the power analysis attacks. However, since every device has its unique primary secret, the lost wearable can be easily replaced. For completing the secure data collection phase with AP_i, the lost device generates the timestamp CT_{MD_l} and random rn_{MD_l}, and establishes a secure session key to send the wrong patient data and corrupt the digital twin analyses process. Thus, only the compromised wearable devices will be able to communicate with the AP_i. However, all other non-compromised wearable devices can still communicate with 100% security with their AP_i. In this way, the proposed scheme provides the *unconditional security against wearable device capture attack.* ■

Proposition 5: The proposed scheme supports the properties of anonymity and untraceability.

Proof: The identities of the wearable devices and the corresponding digital twins are not required for the secure data collection and secure data exchange phases in our scheme, and thus, are never revealed. This strategy of not using their real identities preserves their anonymity and keeps them untraceable. ■

Proposition 6: The proposed scheme is secure against Ephemeral Secret Leakage (ESL) attack under the CK-adversary model.

Proof: AP_i provides long-term secrets k to DT and MK_{MD_l} to the wearable device during registration. DT and MD_l generate their short-term secrets r_j, e_j and rn_{MD_l} during the session. The session keys in both phases are constructed using both the provided long-term secrets and session-alive secrets. Thus, compromise of only long-term secrets or only short-term secrets cannot compromise the session key. As a result, the ESL attack is protected in the proposed scheme under the CK-adversary model. ■

Proposition 7: The proposed scheme is resilient against quantum attacks.

Proof: The proven security of the one-way cryptographic hash function $h(\cdot)$ against quantum attacks ensures that secure data collection from wearable devices remains protected against such attacks. Moreover, the data exchange with the digital twin is secured against quantum attacks, since any such attack would require solving the RLWE problem, which is considered hard for quantum computers. Thus, our proposed scheme is post-quantum secure. ■

VII. Experimental Results

To demonstrate the effectiveness of the proposed authentication scheme, we conducted experiments using an ML-based early disease detection process in two distinct scenarios. In the first scenario, the secure authentication mechanism was used to transmit the data from its source to the digital twin, after which the data was processed using a machine learning classifier. In the second scenario, the same process was executed without the authentication scheme, exposing the system to potential adversarial threats. To evaluate the resulting vulnerabilities, we applied the Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD) attacks on the unsecured data and trained model. This comparative analysis highlights the detrimental impact of unsecured data aggregation in digital twins-based early disease detection.

For the experimental evaluation, the authors have used the dataset [18], which is a chest X-ray image collection from multiple patients categorized into four distinct classes: *"COVID-19"*, *"Normal"*, *"Pneumonia"*, and *"Tuberculosis"*. The dataset contains a total of 4,028 images distributed across these classes, providing a diverse and representative collection for the classification and evaluation tasks. The core idea of the experiment is to simulate a real-time healthcare scenario in which chest X-ray images represent patient data collected and synchronized with a digital twin system. Once the images are securely stored within the digital twin, the ML-based disease detection process is initiated. This setup effectively models how real-world medical data flows from patient acquisition to intelligent diagnosis, highlighting the critical role of secure authentication in preserving data integrity throughout the process.

A. Experimental Configurations

In ML-based early disease detection, such tasks are typically formulated as classification problems, where the objective is to distinguish between different medical conditions. In this experiment, chest X-ray images (we take the data from the public dataset [18]) collected from patients serve as the input data, and the model is trained to classify these images into corresponding disease categories. The DenseNet-121 architecture is employed for this classification task due to its proven efficiency and high accuracy in medical image analysis. The detailed step-by-step experimental configuration is presented as follows.

1) Dataset Prepossessing: As discussed earlier, the dataset consists of four primary classes: *"COVID-19"*, *"Normal"*, *"Pneumonia"*, and *"Tuberculosis"*. To ensure compatibility with the network's expected input dimensions, all images were resized to 224×224 pixels. The images were then converted to floating-point format and normalized using the ImageNet statistics with mean values $[0.485, 0.456, 0.406]$ and standard deviations $[0.229, 0.224, 0.225]$.

For dataset partitioning, an $80/20$ split was primarily used for training and testing. However, in certain attack-based experiments, a $70/15/15$ split was adopted for training, validation, and testing, respectively. To further enhance the model's robustness, data augmentation techniques, such as random horizontal flipping and minor rotations, were applied. These pre-processing and augmentation steps collectively contribute to efficient model training and improved generalization.

2) Used Model Architecture and Training: In this experiment, we utilized the DenseNet-121 model, which consists of a series of convolutional and dense blocks followed by a single fully connected classification layer. Using transfer learning, we employed the pretrained weights from ImageNet. For the classification head, the original 1000-way linear layer was replaced with a 4-class linear layer corresponding to the categories in the selected dataset. For fine-tuning, all DenseNet-121 layers were kept trainable, and no layers were frozen. This configuration enables efficient feature reuse through dense connectivity, a characteristic that has shown strong performance in medical imaging tasks.

The model was trained with an input size of 224×224, using the *Adam* optimizer. The learning rate was set to 1×10^{-4}, and the loss function used was cross-entropy. The batch size was set to 16, and the model was trained for 10 epochs. These training configurations help achieve a balance between model convergence and computational efficiency.

B. ML-based Disease Detection Using Secure Data

In this experimental setup, we have trained and tested images aggregated over the digital twin using the proposed secure authentication scheme. The model receives input from an authenticated twin in the digital twin environment, ensuring that the associated ML-based disease detection mechanism

processes the data securely and performs detection using the trained model. The training and testing results obtained through the secure data transmission are illustrated in Fig. 4.

As shown in Fig. 4(a), the training and validation accuracies are notably high, demonstrating the robustness and generalization capability of the model during the training phase. Furthermore, the model loss, depicted in Fig. 4(b), indicates that the learning rate and convergence behavior are well-aligned with the dataset, confirming stable learning dynamics. In the testing phase, the confusion matrix presented in Fig. 4(c) reveals that the model achieves an accuracy of nearly 99%, which is exceptionally impressive in a healthcare context, where disease detection is a highly sensitive and critical task.

C. ML-based Disease Detection in Adversarial Attacks

In this experimental setup, we consider two white-box adversarial scenarios that arise when communication is unsecured and the server (or its model parameters) can be compromised. This compromised situation arises when the actual device and twin server communicate without any secure and robust authentication, and the attacker can hijack the twin server to extract the ML-model parameters. Under the white-box assumption, the adversary has full knowledge of the model architecture and parameters and can therefore compute gradients and craft targeted perturbations to input samples. The two attacks used to evaluate the unsecured setting are described below.

1) Fast Gradient Sign Method (FGSM) Adversarial Scenario: The FGSM is a single-step white-box attack that constructs a small, undetectable perturbation to an input image to induce a misclassification [19]. Let x denote a correctly classified input (e.g., a chest X-ray) with true label y, and let $J(\theta, x, y)$ be the loss of the model parameterized by θ. FGSM computes the input gradient $\nabla_x J(\theta, x, y)$ and perturbs x in the direction that increases the loss. The perturbed adversarial example x' is formed as [19]:

$$x' \;=\; x \;+\; \varepsilon \cdot \operatorname{sign}\big(\nabla_x J(\theta, x, y)\big),$$

where $\operatorname{sign}(\cdot)$ denotes the sign function and $\varepsilon > 0$ controls the perturbation magnitude (attack strength). In our experiments, we evaluate FGSM across multiple perturbation magnitudes, specifically $\varepsilon \in \{0.005,\ 0.010,\ 0.020,\ 0.030,\ 0.050\}$, to measure the model robustness under increasing adversarial intensity. A detailed attack performance over the trained disease detection model is shown in Table I and the results are plotted in the Fig. 5 and 6.

2) Projected Gradient Descent (PGD) Adversarial Scenario: PGD [20] is an iterative, white box adversarial attack that generalizes FGSM by performing multiple small gradient steps while projecting the perturbed example back into a feasible perturbation set. Starting from a correctly classified input $x^0 = x$, PGD computes, at each iteration i, the gradient of the loss with respect to the current adversarial example x^i and performs a step in the loss direction [20]:

$$\tilde{x}^{\,i+1} \;=\; x^i \;+\; \alpha \cdot \operatorname{sign}\big(\nabla_x J(\theta, x^i, y)\big),$$

where $\alpha > 0$ is the step size (typically $\alpha = \varepsilon/T$ with T iterations). The intermediate result $\tilde{x}^{\,i+1}$ is then projected back to ensure the perturbation remains bounded. Finally, the result is clipped to the valid input range (e.g., $[0, 1]$ for our experiment). After T iterations the adversarial example x^T is returned; in our experiment, we set $T = 10$ (can be evaluated up to $T = 40$ for robustness analysis) and examine multiple ε values (same as FGSM in this experiment) to measure model resilience against strong, multi-step perturbations. A detailed attack performance over the trained disease detection model is shown in Table I, and the results are plotted in Figs. 5, 6 and 7.

TABLE I: Model performance under adversarial attacks

Attack	ε Value	Accuracy	Macro Precision	Macro Recall	Macro F1
FGSM	0.005	0.533	0.556	0.533	0.530
FGSM	0.010	0.285	0.294	0.285	0.267
FGSM	0.020	0.225	0.203	0.225	0.179
FGSM	0.030	0.253	0.236	0.254	0.173
FGSM	0.050	0.254	0.272	0.254	0.140
PGD	0.005	0.023	0.019	0.023	0.021
PGD	$\geq$ 0.010	0.000	0.000	0.000	0.000

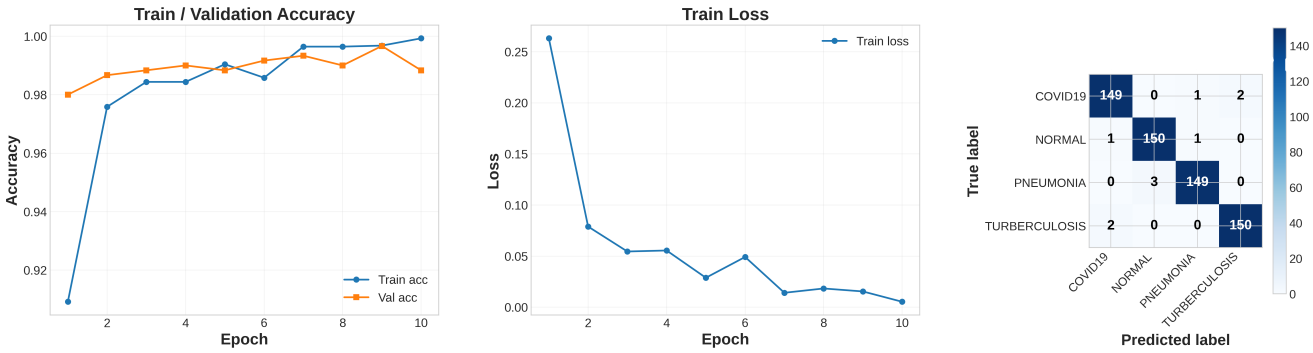
3) Result Discussion: We evaluated the ML-based disease detection security under two operational conditions. The model achieves excellent training and validation performance in the secure scenario where the proposed authentication scheme protects data aggregation (see Fig. 4). The secure channel ensures that only authenticated digital twins contribute data, preventing tampering during collection and transmission; as a result, the classifier achieves near ideal accuracy and stable loss behavior under clean conditions.

In the unsecured scenario, the server and model parameters are assumed to be exposed, and adversaries can inject crafted perturbations. We assessed two white-box attacks, FGSM and PGD, across perturbation values as $\varepsilon \in \{0.005,\ 0.010,\ 0.020,\ 0.030,\ 0.050\}$. Results in Table I and Figs. 5–6 demonstrate that even very small perturbations substantially degrade performance. FGSM produces a noticeable accuracy drop beginning at $\varepsilon = 0.005$, indicating that the classifier is vulnerable to simple one-step perturbations, although it retains partial resilience at lower strengths. PGD, being an iterative and stronger method, causes a far more significant impact: the model tolerates $\varepsilon = 0.005$ in some cases but fails catastrophically for larger ε values, confirming that multi-step attacks severely compromise inference.

These findings have serious implications: compromised devices and unsecured aggregation can enable adversaries to (i) disrupt critical ML-driven services, (ii) produce misleading diagnostic outputs that may result in harmful clinical decisions, and (iii) precipitate system-wide failures in automated monitoring. Collectively, the results underscore the necessity of the proposed authenticated data synchronization: secure device authentication and protected parameter exchange substantially mitigate adversarial impact and preserve the integrity of ML-based disease detection.

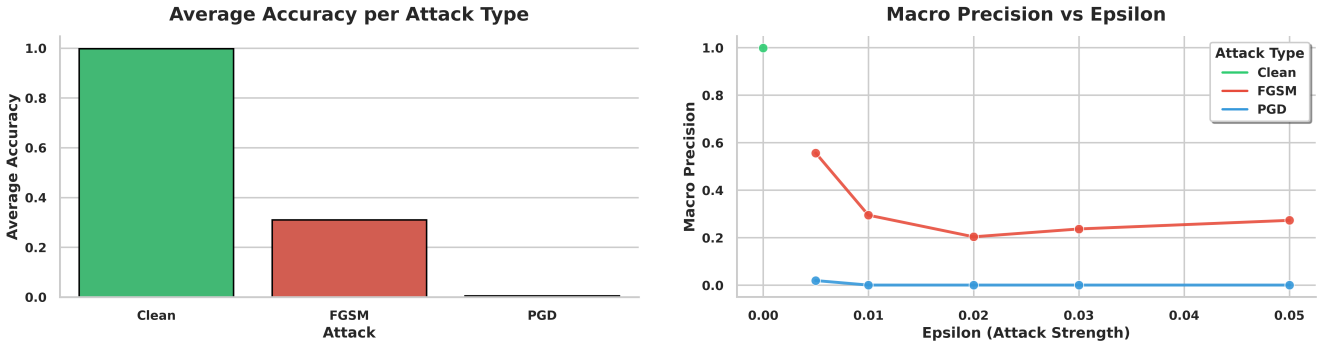
VIII. Comparative Study

In this section, we conduct a comparison analysis of the proposed scheme with the existing schemes of Chaudhary et al. [9], Rewal et al. [10], Cui et al. [11], Khalid et al. [12], and Ahmad and Jagatheswari [13].



(a) Accuracy (b) Model loss (c) Confusion matrix

Fig. 4: Accuracy, model loss, and confusion matrix of detection over secure data



(a) (b)

Fig. 5: Comparison of model performance in an adversarial attack scenario: (a) Accuracy (b) Precision

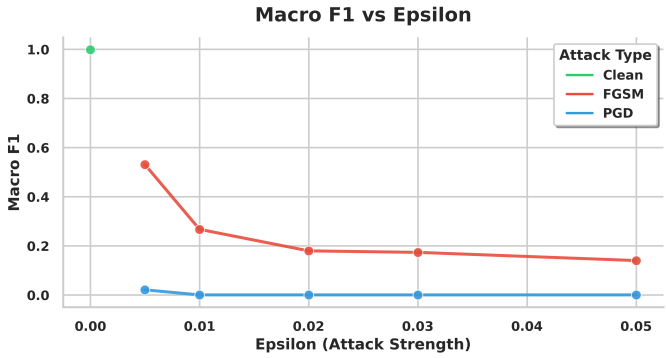


Fig. 6: Comparison of model performance in an adversarial attack scenario: F1-score

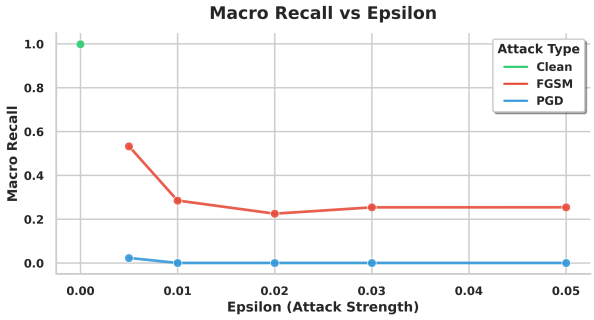


Fig. 7: Comparison of model performance in an adversarial attack scenario: Recall

A. Communication Cost Comparison

In this section, we compute the communication costs of the proposed scheme among other existing schemes. To do so, we consider the sizes of random nonce are 160 bits, timestamps are 32 bits, polynomials in $\mathbb{R}_q$ are 4096 bits, hash output with SHA-265 are 256 bits, and signal function is 1 bit. In this proposed scheme, three messages are transmitted for authentication and key establishment, such as MSG_1, MSG_2, and MSG_3. The message $MSG_1 = \{x_i, TS_1, TID_i, V\}$ needs (4096 + 32 + 160 + 256) = 4544 bits, $MSG_2 = \{skv, TID_i^*, y_i, W_i^*, TS_2\}$ requires (256 + 256 + 4096 + 256 + 32) = 4896 bits, and the message $MSG_3 = \{ack, TS_3\}$ needs (256 + 32) = 288 bits, respectively. Totally, they need 9728 bits. Table II shows the comparison results, and it is evident that the proposed scheme incurs lower communication costs compared to other schemes, except Khalid et al. [12]. However, [12] does not satisfy all the security requirements, as this scheme is vulnerable to key reuse attacks and has design flaws.

TABLE II: Comparative analysis on communication cost

Scheme	No. of messages	Total costs (in bits)
Chaudhary et al. [9]	5	19490
Rewal et al. [10]	4	18626
Cui et al. [11]	4	26977
Khalid et al. [12]	3	5696
Ahmad and Jagatheswari [13]	4	18210
Proposed scheme	3	9728

B. Computation Cost Comparison

For computation costs analysis, we calculate the execution times of the primitives based on our real-time testbed experiment using laptop as a server configuration 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 Raspberry Pi 4 Model B is considered as AP_i and 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".

The primitive T_h is denoted as "one-way hash function using Secure Hash Algorithm (SHA-256) algorithm" and requires 0.183935 ms for AP_i and 0.021616 for the server; T_g. Similarly, for lattice-based operations, the primitives T_g, T_{sm}, T_{pm}, T_{pa}, and T_{cha} represents the time for sampling from χ_β and requires 0.020706 ms and 0.004361 ms, a "component-wise multiplication with a scalar in $\mathbb{R}_q$" and needs 0.017586 ms and 0.003971 ms, a "component-wise polynomial multiplication in $\mathbb{R}_q$" and requires 1.53777 ms and 0.153038 ms, a "component-wise polynomial addition in $\mathbb{R}_q$" and needs 0.0607048 ms and 0.007114 ms, and the "characteristic function in $\mathbb{R}_q$" and requires 0.312965 ms and 0.034375 ms, for AP_i and for server, respectively.

The computation costs for the AP_i of the proposed scheme is $6T_h + 2T_g + T_{sm} + 2T_{pm} + T_{pa} \approx 4.2988$ ms and for the DT_i in server environment is $6T_h + 2T_g + T_{sm} + 2T_{pm} + T_{pa} + T_{cha} \approx 0.4899$ ms. Table III shows the comparison of the proposed scheme with other schemes, and it is worth noticing that the proposed scheme incurs lower computation costs compared to other schemes.

C. Security and Functionality Features

Table IV presents the security and functionality features of the proposed scheme, along with those of other schemes. It is noticed that the proposed scheme satisfies all security features, whereas the other schemes do not fulfill these features, which shows the superiority of the proposed scheme.

D. Summarized Assessment

As the authentication schemes are evaluated based on computational, communication, and security feature parameters, the results obtained from the experiments demonstrate that the proposed approach provides superior and more robust security compared to the existing schemes. However, the computational cost of the proposed scheme is slightly higher. Still, when considering the enhanced security features and reduced communication overhead, the proposed method effectively compensates for this cost through the diversity and strength of its security mechanisms (see Table IV). This signifies the practical applicability of the proposed authentication approach and provides comprehensive evidence that the scheme offers a significant contribution in terms of overall security performance.

TABLE III: Comparative analysis on computation costs

Scheme	SM/smart device/AP_i	Server
Chaudhary et al. [9]	$12T_h + 4T_g + 2T_{sm} + 4T_{pm} + 2T_{pa} + 4T_{cha}$ ≈ 6.7740 ms	$10T_h + T_g + 2T_{pm}$ ≈ 0.5266 ms
Rewal et al. [10]	$8T_h + 4T_g + 2T_{sm} + 4T_{pm} + 2T_{pa} + T_{cha}$ ≈ 8.1749 ms	$6T_h$ ≈ 0.1296 ms
Cui et al. [11]	$5T_h + 3T_g + 2T_{sm} + 2T_{pm} + 2T_{pa}$ ≈ 4.2139 ms	$10T_h + 3T_g + 2T_{sm} + 2T_{pm} + 2T_{pa} + T_{cha}$ ≈ 0.5918 ms
Khalid et al. [12]	$8T_h + 2T_g + T_{sm} + 2T_{pm} + T_{pa}$ ≈ 4.6667 ms	$7T_h + T_g$ ≈ 0.1556 ms
Ahmad and Jagatheswari [13]	$4T_h + 4T_g + 2T_{sm} + 4T_{pm} + 2T_{pa} + T_{cha}$ ≈ 7.4391 ms	$5T_h$ ≈ 0.1081 ms
Proposed scheme	$6T_h + 2T_g + T_{sm} + 2T_{pm} + T_{pa}$ ≈ 4.2988 ms	$6T_h + 2T_g + T_{sm} + 2T_{pm} + T_{pa} + T_{cha}$ ≈ 0.4899 ms

TABLE IV: Comparative analysis on various FS attributes

Attribute (FS)	[9]	[10]	[11]	[12]	[13]	Proposed scheme
FS_1	×	✓	✓	✓	×	✓
FS_2	✓	✓	✓	✓	✓	✓
FS_3	✓	✓	✓	✓	✓	✓
FS_4	✓	✓	✓	✓	✓	✓
FS_5	✓	✓	✓	✓	✓	✓
FS_6	✓	✓	✓	✓	✓	✓
FS_7	✓	✓	✓	✓	✓	✓
FS_8	✓	×	×	×	×	✓
FS_9	✓	✓	✓	✓	✓	✓
FS_{10}	✓	✓	✓	✓	✓	✓
FS_{11}	×	×	×	×	×	✓
FS_{12}	✓	✓	✓	×	✓	✓

Note: FS_1: Replay attack; FS_2: MITM attack; FS_3: Mutual authentication; FS_4: Key Agreement; FS_5: Device impersonation attack; FS_6: Device physical capture attack; FS_7: ESL attack; FS_8: Untraceability; FS_9: Privileged-insider attack; FS_{10}: Quantum attack; FS_{11}: Key reuse attacks, FS_{12}: Design flow. ✓: A scheme is secure, or it supports an attribute; ×: A scheme is insecure, or it does not support an attribute; N/A: means Not applicable in a scheme."

IX. Conclusion and Limitations

The current medical sector is highly dependent on smart services, where major diagnoses and healthcare discoveries are achieved through intelligent operations such as disease detection and smart drug diagnosis. In such a scenario, preserving patients' data privacy and maintaining the integrity of their health information requires critical technological solutions. To address this need, we have utilized the digital twin technology for secure ML-based disease detection, which enables healthcare organizations to efficiently process patients' data without directly compromising their privacy or health. Furthermore, to enhance security robustness, a lattice-based post-quantum secure authentication mechanism has been integrated, ensuring the designed authentication scheme remains resilient even against quantum-era threats. To evaluate

the system's performance, we conducted a comprehensive technical assessment of ML-based disease detection using authenticated data transmitted through the proposed secure authentication, and compared it with results obtained from insecure, unauthenticated data. The conducted white-box adversarial attack experiments demonstrate that insecure data handling can severely compromise the system and potentially collapse the entire smart healthcare service. The results of this study highlight that a secure data collection and processing pipeline is essential for modern healthcare organizations.

In order to understand the limitations of this study, we have utilized the publicly available chest X-ray images to demonstrate the experimental evaluation. However, in real-life ML-based disease detection systems, data is often multi-modal in nature, encompassing textual vitals, imaging data, and other heterogeneous forms. Thus, a key limitation of this study lies in its reliance on a single data modality. In the future, incorporating multi-modal datasets and conducting corresponding experiments may show more realistic and significant results. Furthermore, to mitigate the impact of white-box attacks, this study primarily adopts a network security-oriented approach by securing the communication through authenticated session establishment. Although this provides a robust defense mechanism, integrating adversarial training and other ML-based defensive strategies against white-box attacks can further enhance the system's resilience and performance.

Acknowledgments

The authors would like to thank the associate editor and the anonymous reviewers for providing their valuable feedback on the paper, which has improved the presentation and technical quality of the work. This paper was edited for grammar using "Grammarly".

References

[1] S. Padinjappurathu Gopalan, C. L. Chowdhary, C. Iwendi, M. A. Farid, and L. K. Ramasamy, "An Efficient and Privacy-Preserving Scheme for Disease Prediction in Modern Healthcare Systems," *Sensors*, vol. 22, pp. 1–17, 2022.

[2] Y. Ren, A. A. Pieper, and F. Cheng, "Utilization of precision medicine digital twins for drug discovery in Alzheimer's disease," *Neurotherapeutics*, vol. 22, no. 3, p. e00553, 2025.

[3] S. Amofa, Q. Xia, H. Xia, I. A. Obiri, B. Adjei-Arthur, J. Yang, and J. Gao, "Blockchain-secure patient Digital Twin in healthcare using smart contracts," *PLoS One*, vol. 19, no. 2, pp. 1–28, 2024.

[4] A. Alqahtani, S. Alsubai, and M. Bhatia, "Digital-Twin-Assisted Healthcare Framework for Adult," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 14 963–14 970, 2024.

[5] C. L. Stergiou, M. P. Koidou, and K. E. Psannis, "IoT-Based Big Data Secure Transmission and Management over Cloud System: A Healthcare Digital Twin Scenario," *Applied Sciences*, vol. 13, pp. 1–28, 2023.

[6] A. K. Jameil and H. Al-Raweshidy, "A digital twin framework for real-time healthcare monitoring: leveraging AI and secure systems for enhanced patient outcomes," *Discover Internet of Things*, vol. 5, no. 1, pp. 1–27, 2025.

[7] Z. Z. Zhao, F. Guo, G. Wu, W. Susilo, and B. Wang, "Secure Infectious Diseases Detection System With IoT-Based e-Health Platforms," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22 595–22 607, 2022.

[8] P. R. Babu, S. A. Kumar, A. G. Reddy, and A. K. Das, "Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges," *Computer Science Review*, vol. 54, p. 100676, 2024.

[9] D. Chaudhary, U. Kumar, and K. Saleem, "A Construction of Three Party Post Quantum Secure Authenticated Key Exchange Using Ring Learning With Errors and ECC Cryptography," *IEEE Access*, vol. 11, pp. 136 947–136 957, 2023.

[10] 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.

[11] J. Cui, J. Liu, L. Wei, I. Bolodurina, J. Li, and H. Zhong, "Post-quantum Secure Authenticated Key Agreement Scheme for Vehicular Digital Twin," *IEEE Transactions on Mobile Computing*, pp. 1–16, 2025, doi: 10.1109/TMC.2025.3618752.

[12] H. Khalid, S. Jahari Hashim, F. Hashim, W. Ameen Mahmoud Al-Jawher, M. Akmal Chaudhary, and H. H. M. Altarturi, "RAVEN: Robust Anonymous Vehicular End-to-End Encryption and Efficient Mutual Authentication for Post-Quantum Intelligent Transportation Systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 11, pp. 17 574–17 586, 2024.

[13] A. Ahmad and S. Jagatheswari, "Lattice-Based Three Party Authenticated Key Agreement Scheme in Medical IoT for Post-Quantum Environment," *IEEE Access*, vol. 12, pp. 157 247–157 259, 2024.

[14] 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.

[15] 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.

[16] A. K. Pandey, A. K. Das, M. Wazid, K. Kaur, Y. Park, and M. M. Hassan, "Uncrewed Aerial Vehicles Empowering Secure Authentication in Cognitive IoMT for Transformative Knowledge Discovery in Data," *IEEE Internet of Things Journal*, vol. 12, no. 9, pp. 11 329–11 346, 2025.

[17] 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.

[18] V. K. Omtri, S. C. Kurupati, V. S. Palla, and I. A. K, "Chest X-ray images for Multiple diseases," *IEEE Dataport*, 2024. [Online]. Available: https://dx.doi.org/10.21227/mece-sa87

[19] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples," *arXiv*, pp. 1–11, 2015, https://arxiv.org/abs/1412.6572.

[20] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards Deep Learning Models Resistant to Adversarial Attacks," *arXiv*, pp. 1–28, 2019, https://arxiv.org/abs/1706.06083.