Summary

1. Introduction and Problem

The paper addresses the critical need for robust security in modern healthcare systems, especially with the rise of the Healthcare Internet of Things (HIoT).
This interconnected environment involves sensitive Personal Health Records (PHRs) being shared over vulnerable wireless channels.

The primary security threats identified are:

- **Data Breaches:** Unauthorized disclosure or theft of sensitive patient data.
- **Unauthorized Access:** Gaining access to systems due to weak authentication, which can lead to data manipulation or theft.
- **Other Attacks:** Includes eavesdropping, replay attacks, impersonation, and Man-in-the-Middle (MITM) attacks.

---

2. Limitations of Current Systems

The paper argues that existing healthcare security models are insufficient for two main reasons:

1. **Vulnerability to Quantum Computing:**
   Traditional security relies on problems like the Integer Factorization Problem (IFP) and the Discrete Logarithm Problem (DLP).
   However, advancements in quantum computing—especially Shor's algorithm—can solve these problems in polynomial time, making current cryptosystems insecure in the post-quantum era.

2. **Weakness of One-Time Authentication (OTA):**
   Most systems authenticate a user only once at the beginning of a session.
   If an attacker steals a user's credentials or device, they gain full access for that session.
   Static authentication methods such as passwords, PINs, or even physiological biometrics (fingerprints, facial recognition) are vulnerable to attacks like shoulder surfing, smudge attacks, and spoofing.

---

3. Proposed Solution: HPostQCA-VSS

To solve these problems, the authors propose a novel framework called **HPostQCA-VSS** (*Healthcare Post-Quantum Continuous Authentication with Vector Similarity Search*).

This system is built on two key pillars:

1. **Post-Quantum Security:**
   The initial authentication and key exchange are based on the **Ring Learning With Errors (RLWE)** lattice problem—considered secure against both classical and quantum attacks.

2. **Continuous Authentication (CA) with Behavioral Biometrics (BB):**
   After initial login, the system continuously monitors the user in the background by analyzing **behavioral biometrics**, such as **keystroke dynamics** (typing patterns).
   These are highly individualized and difficult to spoof compared to static biometrics.
   The continuous verification process uses **Vector Similarity Search (VSS)** to match new behavioral data with stored templates in a secure database.

---

4. Core Components and Methodology

The **HPostQCA-VSS** protocol is organized into several key phases:

A. System Initialization and Registration

- **Initialization:**
  The medical server (MS) sets up public parameters for the post-quantum cryptographic system, including a prime number, polynomial ring, and hash functions.

- **Registration:**
  The user registers through a secure channel by providing:

  - Identity and password.

  - Initial biometric data (e.g., fingerprint or face scan).

  - Behavioral biometric data (e.g., typing or touch patterns).
    The MS computes secret keys and creates a **Feature Vector Database (FVDB)** that stores each user's behavioral patterns as high-dimensional vectors.

B. One-Time Authentication and Key Agreement (OTAKA)

- **Login:**
  The user logs into their device using password and static biometric verification.

- **Key Exchange:**
  The device and server perform a three-message authentication handshake using the RLWE protocol to establish a **shared, quantum-secure session key**.
  This key is used to encrypt all further communication.

C. Continuous Authentication (CA)

Once the secure session is established, continuous monitoring begins:

1. The user's behavioral biometric data (e.g., keystroke dynamics) is continuously captured.

2. The data is encrypted using the session key and transmitted to the medical server.

3. The server decrypts the data and converts it into a **feature vector** using machine learning techniques (e.g., RNNs).

4. The server compares this vector to stored templates in the **FVDB** using **Vector Similarity Search** (e.g., cosine or Euclidean distance).

5. If the match corresponds to the authenticated user, access continues; if not, the session is terminated immediately.

---

5. Security Analysis

The paper performs both **formal** and **informal** analyses.

A. Formal Security Analysis

- **Real-Or-Random (ROR) Model:**
  The security of the session key is proven under this model, showing that adversarial success probability is negligible and based on the hardness of RLWE.

- **Scyther Tool Verification:**
  Using the Scyther model checker, the authors verified that the protocol is secure against known attack types—no violations were detected for secrecy or authentication.

B. Informal Security Analysis

The system resists a wide range of attacks:

- **Replay Attacks:** Prevented by using fresh timestamps in all messages.

- **Man-in-the-Middle (MITM) Attacks:** Infeasible without access to secret keys.
- **Quantum Lattice Reduction Attacks:** Countered by carefully chosen parameters (e.g., polynomial degree 1024) to maintain 80-bit post-quantum security.
- **Quantum Search Attacks:** SHA-256 remains secure, even against Grover's algorithm.
- **Stolen Device Attacks:** Credentials are protected via hashing—no plaintext data is stored locally.
- **Data Poisoning Attacks:** Prevented as all behavioral data is encrypted before being transmitted.

---

6. Performance and Experimental Results

A. Experimental Setup

- **Hardware:**
  A **Laptop (Intel i7, 16GB RAM)** acted as the Medical Server (MS), and a **Raspberry Pi 4 (Cortex-A72, 7.6GB RAM)** simulated the user's device.
- **Implementation:**
  The protocol was implemented in Python using socket programming and standard cryptographic libraries.
  Results confirmed successful establishment of a shared session key.

B. Computation and Communication Costs

- **Computation:**
  - User side (Raspberry Pi): ~4.17 ms total time.
  - Server side (Laptop): ~0.47 ms total time.
  - Overall, faster than most comparable post-quantum security schemes.
- **Communication:**
  The OTAKA phase requires three messages totaling **9985 bits**, which is significantly lower than other robust post-quantum protocols.

C. Proof of Concept: VSS and FastAPI

- **Dataset:**
  The **BioIdent** touchstroke biometric dataset (71 users, 15 features per stroke) was used.

- **Vector Search:**
  Implemented using **Milvus** (vector database) and **ANNOY** (Approximate Nearest Neighbors).

  1. **Accuracy:** 100% match with legitimate users.

  2. **Robustness:** Fake users were correctly rejected (statistically significant difference, $p < 0.001$).

  3. **Speed:** Average query time ≈ 0.0017 seconds — suitable for real-time use.

- **FastAPI Integration:**
  A working FastAPI backend was developed with endpoints for:

  1. Creating the vector database.

  2. Registering new users' behavioral biometrics.

  3. Checking similarity for continuous authentication.

---

7. Conclusion

The paper presents **HPostQCA-VSS**, a secure, post-quantum-ready authentication framework for healthcare environments.
It effectively combines **lattice-based cryptography (RLWE)** for quantum resistance with **continuous behavioral biometric verification** for real-time user authentication.

Through theoretical proof, Scyther validation, and experimental results on lightweight devices (Raspberry Pi), the authors demonstrate that **HPostQCA-VSS** is secure, efficient, and practical for real-world healthcare applications.
