PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY OF MOHAMED BOUDIAF-MSILA

FACULTY OF MATHEMATICS AND INFORMATICS
COMPUTER SCIENCE DEPARTEMENT

N° :……..

THESIS

Submitted in Partial Fulfilment of the Requirements for the Degree of 3rd cycle Doctorate in Computer science

Speciality: Computer science
Option: Computer science

By: Anwar Noureddine Bahache

Entitled as:

Security of Health Applications in The Internet of Things Environment

Publicly defended on: 25 /07 /2024

Board of Examiners:

M. Lamri Sayad	Prof	University of M'sila	President
M. Noureddine Chikouche	Prof	University of M'sila	Supervisor
M. Saber Benharzallah	Prof	University of Batna 2	Examiner
M. Noureddine Chaib	MCA	University of Laghouat	Examiner
M. Alloua Hemmak	Prof	University of M'sila	Examiner
M. Debbi Hicham	Prof	University of M'sila	Examiner

Academic Year : 2023 /2024

Acknowledgements

First of all, I thank **ALLAH**, the almighty, for giving me the patience and the will to carry out this work.

I cannot forget the kind efforts and continuous support provided by my wonderful supervisor, **Pr. Noureddine Chikouche**, who has been a constant aid and guide throughout the preparation of the thesis. He has truly been an unparalleled companion in every step I took on this scientific journey.

And of course, I must thank **Dr. Fares Mezrag**, who offered me advice and guidance with sincerity and care, and contributed greatly to the success of this extensive research work.

I dedicate the fruits of this effort to my dear **Parents**, for without their constant presence and limitless support, I would not have been able to achieve this great accomplishment. To whom Allah Almighty has said about them: "And your Lord has decreed that you not worship except Him, and to parents, good treatment. Whether one or both of them reach old age [while] with you, say not to them [so much as], "uff," and do not repel them but speak to them a noble word." Their continuous presence and support have been the cornerstone of my success.

To my brothers, sisters, and all **Bahache** family.

To all my friends.

To all my colleagues at the University of M'sila.

In conclusion, I extend my heartfelt thanks to everyone who contributed in any way, whether near or far, negatively or positively, as their sincere efforts were the true motivation behind achieving this accomplishment.

Abstract

A biosensor serves as a conduit for transmitting diverse physiological data, including body temperature, electrocardiogram (ECG), pulse, blood pressure, electroencephalogram (EEG), and respiratory rate. This transmission occurs through Wireless Body Area Networks (WBANs) within the realm of remote patient diagnosis via the Internet of Medical Things (IoMT). However, the transfer of sensitive IoMT data via WBANs over insecure channels exposes it to numerous threats, underscoring the need for robust security measures against potential adversaries. This dissertation presents a new classification for authentication schemes based on architecture, further enhancing the landscape of secure healthcare communications. Additionally, it seeks to address security apprehensions associated with patient monitoring in healthcare systems, ensuring the requisite security and privacy standards during communication by introducing a resilient authentication framework. Consequently, it introduces a versatile and resilient post-quantum authentication framework tailored for cloud-based healthcare applications, this framework is suitable for various medical scenarios and applications, effectively countering vulnerabilities identified in recent scholarly works. Specifically crafted to thwart quantum attacks utilizing Kyber cryptosystem, this framework undergoes formal security validation using AVISPA tool, supplemented by an informal evaluation. Moreover, it includes a comparative analysis of performance and security vis-à-vis previous endeavors, showcasing the strengths and advantages of the proposed framework in both dimensions.

Key Words:

Authentication framework, Wireless body area network, Internet of Medical Things, Lattice-based cryptography, Security

Résumé

Un biosenseur sert de conduit pour la transmission de diverses données physiologiques, notamment la température corporelle, l'électrocardiogramme (ECG), le pouls, la pression artérielle, l'électroencéphalogramme (EEG) et le rythme respiratoire. Cette transmission se fait par le biais de réseaux de capteurs corporels sans fil (WBAN) dans le domaine du diagnostic à distance des patients via l'Internet des objets médicaux (IoMT). Cependant, le transfert de données sensibles de l'IoMT via les WBAN sur des canaux non sécurisés les expose à de nombreuses menaces, soulignant la nécessité de mesures de sécurité robustes contre les adversaires potentiels. Cette dissertation présente une nouvelle classification des schémas d'authentification basée sur l'architecture, améliorant ainsi le paysage des communications sécurisées en santé. De plus, elle cherche à répondre aux préoccupations en matière de sécurité associées à la surveillance des patients dans les systèmes de santé, en garantissant les normes de sécurité et de confidentialité requises lors de la communication en introduisant un cadre d'authentification résilient. Par conséquent, elle introduit un cadre d'authentification post-quantique polyvalent et résilient conçu pour les applications de santé basées sur le cloud, adapté à divers scénarios et applications médicaux, contrecarant efficacement les vulnérabilités identifiées dans les travaux de recherche récents. Spécifiquement conçu pour déjouer les attaques quantiques en utilisant le cryptosystème Kyber, ce cadre fait l'objet d'une validation formelle de la sécurité à l'aide de l'outil AVISPA, complétée par une évaluation informelle. En outre, il comprend une analyse comparative des performances et de la sécurité par rapport aux travaux antérieurs, mettant en évidence les forces et les avantages du cadre proposé dans les deux dimensions.

Mots Clés :

Framework d'authentification, Réseau corporel sans fil, Internet des objets médicaux, Cryptographie basée sur les réseaux, Sécurité

ملخص

يعمل المستشعر البيولوجي كقناة لنقل البيانات الفسيولوجية المتنوعة، بما في ذلك درجة حرارة الجسم، وتخطيط القلب الكهربائي(ECG) ، والنبض، وضغط الدم، وتخطيط الدماغ الكهربائي(EEG) ، ومعدل التنفس. يحدث هذا النقل من خلال شبكات المناطق الجسدية اللاسلكية (WBANs) في مجال التشخيص عن بعد للمرضى عبر إنترنت الأشياء الطبية .(IoMT) ومع ذلك، فإن نقل بيانات IoMT الحساسة عبر WBANs من خلال قنوات غير آمنة يعرضها للعديد من التهديدات، مما يبرز الحاجة إلى تدابير أمنية قوية ضد الأعداء المحتملين. تقدم هذه الرسالة تصنيفًا جديدًا لآليات المصادقة بناءً على البنية، مما يعزز من مشهد الاتصالات الآمنة في مجال الرعاية الصحية. بالإضافة إلى ذلك، تسعى إلى معالجة المخاوف الأمنية المرتبطة بمراقبة المرضى في أنظمة الرعاية الصحية، وضمان المعايير الأمنية والخصوصية المطلوبة أثناء التواصل من خلال إدخال إطار مصادقة مرن. وبالتالي، يتم تقديم إطار مصادقة ما بعد الكوانتوم متعدد الاستخدامات ومرن مصمم لتطبيقات الرعاية الصحية السحابية، وهذا الإطار مناسب لمختلف السيناريوهات والتطبيقات الطبية، ويعمل بشكل فعال على مواجهة الثغرات المحددة في الأعمال البحثية الأخيرة. مصمم خصيصًا لإحباط الهجمات الكوانتية باستخدام نظام التشفير Kyber ، يخضع هذا الإطار للتحقق الأمني الرسمي باستخدام أداة AVISPA ، مدعومًا بتقييم غير رسمي. علاوة على ذلك، يشمل تحليلًا مقارنًا للأداء والأمان بالمقارنة مع الجهود السابقة، مما يبرز نقاط القوة والمزايا للإطار المقترح في كلا البعدين.

ألكلمات المفتاحية:

إطار المصادقة, شبكة منطقة الجسم اللاسلكية, إنترنت الأشياء الطبية, التشفير المبني على الشبكات, الأمان

Table of Contents

List of Figures

List of Tables

List of Publications

Journals

- – *Title:* **Authentication schemes for healthcare applications using wireless medical sensor networks: A survey.**
  – *Authors:* Anwar Noureddine Bahache, Noureddine Chikouche, Fares Mezrag.
  – *Journal:* Journal of SN Computer Science.
  – *Year:* 2022.
- – *Title:* **Securing cloud-based healthcare applications with a quantum-resistant authentication and key agreement framework.**
  – *Authors:* Anwar Noureddine Bahache, Noureddine Chikouche, Sedat Akleylek.
  – *Journal:* Journal of Internet of Things.
  – *Year:* 2024.

Conferences

International

- – *Title:* **An analysis of user authentication schemes for WBAN in healthcare applications.**
  – *Authors:* Anwar Noureddine Bahache, Noureddine Chikouche.
  – *Conference:* Fourth International Conference on Informatics and Applied Mathematics (IAM).
  – *Location:* Guelma, Algeria.
  – *Year:* 2021.
- – *Title:* **A comparative analysis of RFID authentication protocols for healthcare applications.**
  – *Authors:* Anwar Noureddine Bahache, Noureddine Chikouche.
  – *Conference:* International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP).
  – *Location:* El Oued, Algeria.
  – *Year:* 2021.

National

- – *Title:* **A Survey of RFID authentication schemes for healthcare applications.**
  – *Authors:* Anwar Noureddine Bahache, Noureddine Chikouche.
  – *Conference:* Workshop on Internet of Things (IoT) Security.
  – *Location:* M'sila, Algeria.
  – *Year:* 2021.

Abreviation List

AES:	Advanced Encryption Standard
AVISPA:	Automated Validation of Internet Security Protocols and Applications
CL-ATSE:	Constraint-Logic-based Attack Searcher
CPS:	Cyber-Physical Systems
CU:	Checkup phase
DDoS:	Distributed Denial of Service
DLWE:	Decisional Learning With Errors
DoS:	Denial of Service
ECC:	Elliptic Curve Cryptography
EHR:	Electronic Health Record
EMR:	Electronic Medical Record
FA:	Factor Authentication
GPRS:	General Packet Radio Service
HLPSL:	High-Level Protocol Specification Language
IF:	Intermediate Format
IoMT:	Internet of Medical Things
IoT:	Internet of Things
ITU:	International Telecommunication Union
LWE:	Learning With Errors
MLWE:	Module Learning With Errors
MITM:	Man-In-The-Middle
NAS:	Node Authentication Scheme
NIST:	National Institute of Standards and Technology
OFMC:	On-the-fly Model Checker
OfDA:	Offline Data Access
OnDA:	Online Data Access
PBC:	Pairing-Based Cryptography
PDA:	Personal Digital Assistant
PHR:	Periodic Health Records
PKC:	Public Key Cryptography
PKI:	Public Key Infrastructure
PQC:	Post-Quantum Cryptography
RFID:	Radio-Frequency Identification

RSA:	Rivest-Shamir-Adleman
SATMC:	SAT-based Model Checker
SKC:	Symmetric Key Cryptography
SLWE:	Search Learning With Errors
SPAN:	Security Protocol Animator
TA4SP:	Tree Automata based on Automatic Approximations for the Analysis of Security Protocols
UP:	Upload phase
UAS:	User Authentication Scheme
WBAN:	Wireless Body Area Network
WSN:	Wireless Sensor Network

General Introduction

General Introduction

Ensuring optimal health is pivotal for a fulfilling and prosperous existence, particularly in today's fast-paced world. As articulated by the World Health Organization (WHO), health is not merely the absence of diseases, but a state of complete physical, mental, and social well-being. Healthcare, therefore, encompasses a multifaceted approach aimed at maintaining or improving health through various means, including preventive measures, accurate diagnoses, and effective treatments for ailments and injuries.

However, the conventional healthcare landscape often grapples with challenges inherent in manual management systems. These systems typically involve the laborious handling of patient demographic data, medical records, diagnostic reports, medication schedules, billing processes, and pharmaceutical inventory control. Such reliance on manual procedures not only consumes valuable time but also introduces a considerable margin for error, potentially compromising patient care and safety.

In response to these challenges, the advent of Internet of Things (IoT) technology has revolutionized the healthcare industry. IoT-based smart healthcare solutions leverage interconnected networks of devices and sensors to monitor vital signs, track patient health metrics in real-time, and facilitate seamless communication between healthcare professionals and patients. By automating data collection, analysis, and transmission processes, these systems enable healthcare providers to make more informed decisions and deliver personalized care with greater efficiency and accuracy.

A key aspect of IoT-driven healthcare innovation is the emergence of the Internet of Medical Things (IoMT), which encompasses a wide array of medical devices and wearables capable of wirelessly transmitting health-related data. These devices include wearable fitness trackers, smart insulin pumps, continuous glucose monitors, remote patient monitoring systems, and implantable medical devices. By harnessing the power of IoMT, healthcare practitioners can remotely monitor patient health parameters, detect potential health issues early, and intervene promptly to prevent complications.

Moreover, IoT-enabled smart healthcare systems offer significant benefits beyond individual patient care. They facilitate data-driven insights and population health management strategies, enabling healthcare organizations to identify trends, allocate resources efficiently, and implement targeted interventions to address public health challenges. Additionally, integrating artificial intelligence (AI) and machine learning algorithms with IoT data streams holds the promise of predictive analytics and personalized treatment recommendations, further enhancing healthcare outcomes and patient satisfaction.

In summary, the convergence of IoT technology and healthcare holds immense promise for revolutionizing the delivery of medical services, improving patient outcomes, and advancing

public health initiatives. By embracing innovative IoT solutions, healthcare stakeholders can usher in a new era of proactive, patient-centered care, where precision, efficiency, and accessibility converge to create a healthier world.

Problem statement

The security of Wireless Body Area Networks (WBANs) in Internet-of-Medical-Things (IoMT) applications is crucial due to their deployment in environments susceptible to cyber-attacks and unauthorized access. These networks are utilized in critical sectors such as healthcare services, where ensuring data integrity, confidentiality, and authentication is paramount [1]. However, WBANs face inherent security challenges, especially in hostile environments, making them vulnerable to cyber threats that can compromise sensitive medical data. Additionally, wireless communications within WBANs lack inherent security measures, enabling adversaries to eavesdrop on legitimate node communications. Therefore, there is a pressing need to establish robust security protocols that guarantee authentication, data confidentiality, and integrity while considering the resource constraints of sensor nodes.

Cryptography serves as a fundamental security measure to safeguard communication in open networks like WBANs. Cryptographic techniques, including Symmetric-Key Cryptography (SKC) and Public-Key Cryptography (PKC), play vital roles in ensuring data security in WBANs. While SKC offers efficient performance in terms of computational overhead and energy consumption, it lacks support for non-repudiation and involves complex key distribution processes. On the other hand, PKC addresses these shortcomings but is computationally expensive, posing challenges for resource-constrained sensor nodes. Recent studies have demonstrated the feasibility of implementing PKC in WBANs using elliptic curves, mitigating some of the computational burdens. However, traditional PKI solutions, aimed at ensuring public key authentication, are impractical for WBANs due to their overhead and complexity.

Post-quantum cryptography (PQC) emerges as a promising solution for securing communication in WBANs. Leveraging PQC and specifically the Kyber algorithm presents an alternative approach to address security concerns in WBANs. PQC, exemplified by Kyber, simplifies the process of deriving public keys from known identity information, eliminating the need for complex certificate operations. In this scheme, a trusted authority (TA) in WBANs, serves as a Private Key Generator (PKG) to issue private keys corresponding to sensor nodes' identities. This approach streamlines the key setup process, as sensor node identities and their corresponding keys are generated and embedded by the BS, eliminating the need for a separate secret channel. Consequently, energy-efficient communication is facilitated between sensor nodes, as only identities need to be exchanged without additional public keys and certificates. Additionally, the self-authentication property of public keys in PQC, particularly Kyber, further enhances security without relying on digital certificates.

Goals and contributions

The primary aim of this thesis is to explore the security challenges inherent in IoMT systems leveraging WBANs and to devise innovative security mechanisms to address them effectively. The proposed methodologies are meticulously crafted to accommodate the resource-constrained nature of sensor nodes while also overcoming the shortcomings of existing techniques, thereby enhancing the overall security posture of IoMT. In pursuit of this objective, we present two distinct contributions:

- Contribution 1: proposing a new classification for the existing authentication schemes and performing a security and performance analysis.
- Contribution 2: Presenting a quantum-resistant authentication framework for cloud-based systems, specifically designed to tackle the shortcomings identified in prior literature.

Dissertation outline

The chapters comprising this thesis consist of adaptations of our research articles, which have been formally published in reputable scientific journals or presented at esteemed conference proceedings. The thesis is structured into five distinct chapters, evenly distributed across two primary sections: Background and Contributions.

The Background section furnishes readers with a comprehensive overview of IoMT based on WBANs, delving into various aspects including its architecture, functionalities, and security implications. This section meticulously examines the security landscape of IoMT systems, delineating the constraints, requirements, and potential cyber threats that pose risks to their integrity. Moreover, it conducts a thorough review of existing literature, encompassing prior research efforts and proposed solutions in the domain.

In contrast, the Contributions section delineates our original research contributions aimed at bolstering the security posture of IoMT systems based on WBANs. These contributions encompass novel techniques and methodologies devised to mitigate prevalent security challenges and fortify the resilience of Medical-Enabled Wearable Sensor Networks (MWSNs).

The organizational structure of the dissertation unfolds as follows:

- Chapter 1 defines the principal concepts associated with IoMT, IoT, and WBANS such as architecture and real-world applications. It also highlights the constraints and challenges in IoMT.
- Chapter 2 discusses IoMT security, including security constraints, security requirements, and possible cyber-attacks aimed at WBAN-based IoMT applications. The chapter also reviews cryptographic notions and primitives.
- Chapter 3 reviews existing PKC-based authentication schemes in IoMT, including schemes based on pairings, schemes based on ECC, and schemes based on hash and symmetric encryption.

- Chapter 4 presents our contribution: a novel security framework utilizing the well-known post-quantum cryptographic (PQC) algorithm Kyber to ensure secure data communication, named QR-AKAF. This chapter holds a detailed authentication description for each proposed scheme in the framework.
- Chapter 5 presents the evaluation and discussion of the proposed framework in terms of performance and security.

CHAPTER 1:

Internet of Medical Things

Chapter 1

Internet of Medical Things

1.1 Introduction

The evolution of the Internet of Things (IoT) is poised to revolutionize the entire future internet landscape, ushering in new possibilities for automation and the integration of physical objects into digital ecosystems. This transformative trajectory extends to various domains, with the medical field standing out as an early adopter of innovation. Presently, the medical sector is witnessing a proliferation of IoT applications, including e-Health and m-Health, collectively known as the IoMT. These advancements signify a paradigm shift in healthcare delivery, leveraging interconnected devices and data analytics to enhance patient care, improve diagnostic accuracy, and optimize treatment outcomes. As IoMT continues to evolve, it holds immense potential to reshape medical practices, empower patients, and drive breakthroughs in healthcare research and innovation.

This chapter offers a thorough examination of the Internet of Medical Things (IoMT) and its main enabler devices Wireless Body Area Networks (WBANs), and provides an in-depth overview of its definition, applications, architectures, as well as the associated benefits and challenges. Through this comprehensive exploration of these various aspects, a better understanding of IoMT and its significance in various sectors, particularly within healthcare will be gained.

1.2 Internet of things

The Internet of Things (IoT) represents a modern computing paradigm aimed at transforming ordinary objects into smart entities [2]. Recognized as a disruptive technology of our era, IoT is poised to revolutionize how we perceive and interact with the world around us [3]. This transformation is enabled by advancements in ubiquitous computing, embedded systems, communication technologies, sensor networks, Internet protocols, and web-based applications [4, 5]. These underlying technologies collectively empower everyday devices to exhibit intelligence, thereby realizing the vision of IoT [6].

The concept of the Internet of Things (IoT) traces back to 1999 when researchers affiliated with the Auto-ID Center at the Massachusetts Institute of Technology first proposed the idea [7]. This concept aimed to imbue everyday objects with intelligence and connect them to the Internet, enabling pervasive communication between any real-world objects. The formal recognition of IoT came in 2005 at the World Summit on Information Society in Tunisia, where

the International Telecommunication Union (ITU) released two reports outlining key enabling technologies, market opportunities, and emerging challenges, describing IoT as a paradigm that would create a dynamic network of networks [8].

Since the inception of the ARPANET in the 1960s, the precursor to the modern Internet, the number of connected devices has steadily grown, accelerating after the liberalization of the Internet in the late 1980s [9]. Factors such as ubiquitous connectivity and the advent of IPv6 with an abundance of IP addresses have facilitated the evolution of IoT [10]. Projections indicated that the number of connected devices would surpass 25 billion by 2020, up from 10 billion in 2014, and exceed 100 billion by 2050 [11]. Figure 1.1 illustrates the growth of connected devices on the Internet from the 1950s to 2050, as forecasted by IBM in 2015.

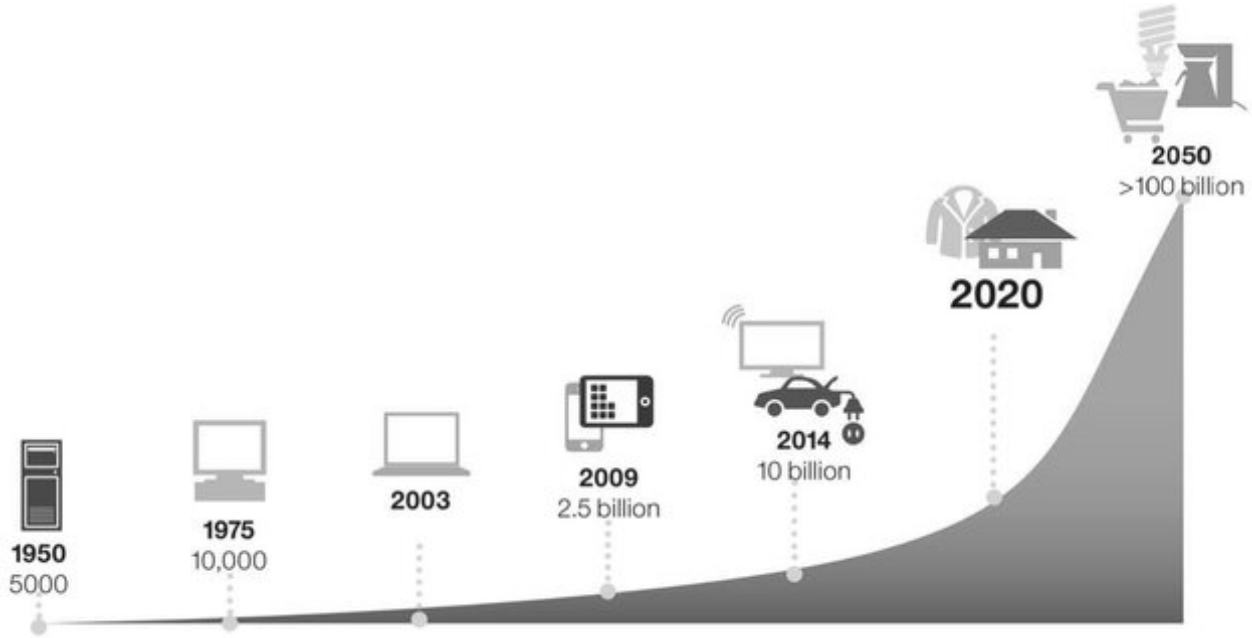


Figure 1.1: Growth of Connected Devices from 1950 to 2050 [10]

1.2.1 Architecture

Research on IoT has been extensive, with researchers examining various issues from different perspectives. As a result, different architectures have been proposed to address specific requirements. Consequently, no universally accepted architecture satisfies every researcher or user, nor one that is suitable for all situations [12]. In the early stages of IoT development, a three-layer architecture consisting of Application, Network, and Perception Layers, from top to bottom, was proposed by Wu et al. [13]. This model was quite basic, as it combined many different functions, which are now categorized under different domains, within a single layer. Later, Tan and Wan [14] expanded this architecture into a five-layer model. The five-layer architecture splits the Application Layer of the three-layer model into three distinct layers: middleware, application, and business layers while retaining the perception and network layers as they are. Figure 1.2 illustrates both the three-layered and five-layered models proposed in

the literature.

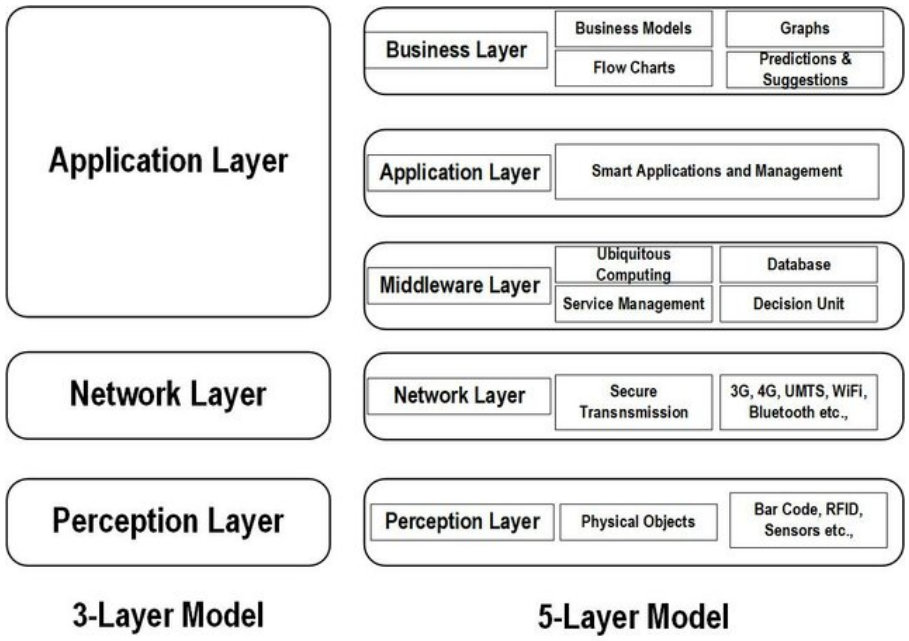


Figure 1.2: IoT Layered Architectures Proposed in Literature [14]

1.2.2 Communication technologies

Numerous communication technologies are currently available for use with IoT, each with its own set of advantages and inherent limitations. This diversity of benefits and drawbacks means that no single technology is universally suitable for every situation, requirement, or application. Therefore, it is essential to assess each technology against the specific requirements of the application in order to determine the most suitable option.

Below we present a summary of a comparative study conducted on a range of communication technologies reported in the literature.

Bluetooth

Bluetooth is a widely recognized wireless technology known for its versatility in handling large amounts of data. It facilitates ad-hoc connections and boasts universal standardization, making it accessible across various devices. However, Bluetooth suffers from relatively low data rates, high power consumption, and vulnerability to external attacks [15, 16].

ZigBee

ZigBee stands out for its ease of setup and decentralized control, enabling load distribution across multiple nodes without a central authority. It offers low power consumption, cost-effectiveness, and low latency. Nonetheless, ZigBee lacks robust security measures and may face compatibility issues with devices from different manufacturers [17, 15].

WiMax

WiMax excels in supporting high-speed voice and data transfers over long distances, with a single base station capable of serving numerous users. Despite its advantages, WiMax requires line-of-sight connections and can suffer from bandwidth limitations under heavy user loads [18, 15, 19].

Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) prioritizes energy efficiency, making it suitable for IoT applications with limited power resources. It offers a balance of low power consumption and moderate data rates but is constrained by limited data handling capacity and susceptibility to attacks [20, 21, 22].

Wi-Fi

Wi-Fi is renowned for its high data rates and widespread adoption, making it suitable for various IoT applications. However, it faces challenges such as increased power consumption with more users, vulnerability to attacks, and limitations in outdoor and obstructed environments [23, 24, 16].

LoRa and LoRaWAN

LoRa and LoRaWAN provide extensive coverage and support for a large number of devices, making them ideal for IoT deployments spanning vast areas. However, their point-to-point nature and reliance on gateways can introduce bottlenecks, and they may experience packet loss during congestion [18, 25, 19].

Wi-Fi HaLow

Wi-Fi HaLow, or IEEE 802.11ah, extends Wi-Fi's reach with enhanced propagation and low power consumption, making it suitable for IoT deployments in challenging environments. Nonetheless, variable data rates and the lack of frequency standards pose potential drawbacks [26, 21].

MiWi and MiWi P2P

MiWi and MiWi P2P offer low power consumption and medium-range communication at zero licensing costs, making them cost-effective solutions for IoT deployments. However, their proprietary nature and susceptibility to interference may limit interoperability and reliability [27].

ISA100.11a

ISA100.11a prioritizes reliability and security, making it suitable for industrial IoT applications. Despite its benefits, ISA100.11a faces challenges such as complex implementation and limited interoperability with other technologies [17, 28].

WirelessHART

WirelessHART employs a self-organizing mesh architecture and strong security measures, making it resilient to interference and suitable for industrial IoT deployments. However, its use of TDMA technology can introduce latency issues, and it may struggle with simultaneous communication in multi-drop mode [17].

Z-Wave

Z-Wave is lauded for its ability to support a large number of connections, making it ideal for IoT ecosystems with numerous devices. It features mesh networking, ensuring robust communication even in complex environments. With no single points of failure, Z-Wave offers reliability and resilience. Additionally, it's relatively inexpensive and boasts low power consumption, making it suitable for both home and light commercial applications. However, Z-Wave faces challenges such as low data rates, dependence on the line of sight for operation, and reported instability in current implementations [16].

LTE, LTE-M, and LTE-A

Operating on licensed bands, LTE variants increase throughput and reduce interference, ensuring reliable connectivity in crowded environments. Their narrowband operation contributes to lower power consumption, enhancing the longevity of IoT devices. Cost-effectiveness on both end devices and base stations, coupled with the reuse of existing cellular spectrum, fosters the densification of IoT deployments. Nevertheless, cellular data plans may incur usage charges, potentially limiting widespread adoption [21, 19].

Ultra-wideband (UWB)

UWB technology utilizes a license-free spectrum, enabling high data rates and efficient spectrum sharing. With very low power consumption, it's suitable for battery-powered IoT devices. UWB's immunity to multipath propagation effects and non-interfering signals enhance reliability. However, its short range and the complexity of antenna design pose challenges to deployment [29, 30, 21].

Wavenis

Wavenis supports ultra-low power operations and offers extensive communication ranges, making it suitable for IoT deployments covering large areas. With reliable communication and

support for multiple network topologies, Wavenis ensures robust connectivity. However, its low data rates, reliance on a high link budget for long-range communication, and requirement for line-of-sight communication may limit its applicability [29, 24, 16].

Insteon

Insteon combines powerline and wireless communication, facilitating long operational ranges and multi-hop transmission. Its decentralized architecture enhances reliability by avoiding single points of failure. However, Insteon faces challenges such as low supported data rates, high power consumption, and reliance on proprietary technology [29, 16].

Thread

Thread supports a large number of clients and mesh networking, providing scalable and reliable communication for IoT ecosystems. With native IPv6 support and robust security measures, Thread ensures secure and efficient data transmission. However, its short range, complex protocol, and less user-friendly implementation may pose barriers to adoption [21, 16].

EnOcean

EnOcean enables energy harvesting from various sources, supporting batteryless operation for IoT devices. With high data rates and compatibility with both indoor and outdoor environments, EnOcean offers versatility in deployment. However, its limited range, reliance on proprietary technology, and throughput constraints may impact its suitability for certain applications [29, 22].

Li-Fi

Li-Fi technology offers faster communication and high data transfer rates, providing efficient data transmission for IoT applications. With low power consumption, Li-Fi enhances energy efficiency in connected environments. Its implementation typically ensures better security measures compared to other wireless technologies. Additionally, Li-Fi poses lower health risks due to its reliance on light-based communication.

However, Li-Fi faces challenges such as relatively high initial costs, making adoption costly for some applications. It is susceptible to interference from other light sources, potentially affecting signal reliability. Moreover, Li-Fi's operational range is limited, and its signals can be blocked by physical obstacles like walls. As a result, Li-Fi is primarily suitable for indoor applications. Implementing Li-Fi infrastructure may require significant investment in new infrastructure, potentially limiting its widespread deployment [31, 32, 33].

Each technology comes with its own set of advantages and drawbacks. While certain technologies excel in indoor environments, others prove more effective outdoors. Some perform optimally with a small number of users, whereas others maintain performance even with a

large number of users. Thus, it's impractical to find a single technology that meets all the requirements of every application.

1.3 Emergence of IoT into the medical field

The emergence of the Internet of Things (IoT) within the medical field has paved the way for the Internet of Medical Things (IoMT). This evolution represents a transformative shift in healthcare, enabled by interconnected medical devices, sensors, and data analytics. IoMT encompasses a wide array of applications and technologies tailored specifically for medical use, ranging from remote patient monitoring and telemedicine to smart healthcare facilities and personalized medicine. By integrating IoT technologies into healthcare delivery and management, IoMT enhances patient care, improves clinical outcomes, and optimizes healthcare operations. Furthermore, IoMT facilitates real-time monitoring, early detection of health issues, and proactive interventions, thereby revolutionizing healthcare delivery and fostering a more connected and patient-centric healthcare ecosystem.

The integration of Wireless Sensor Networks (WSN) into IoT has played a pivotal role in facilitating the transition to IoMT. WSNs provide a scalable and cost-effective means of collecting data from various medical sensors and transmitting it to IoT platforms for analysis and action. This integration has enabled seamless communication and data exchange between medical devices, enabling real-time monitoring and analysis of patient health data, ultimately leading to the emergence of IoMT.

1.4 Internet of Medical Things(IoMT)

IoMT refers to a cluster of interconnected electronic devices equipped with sensors designed for sensing and monitoring purposes [34, 35]. The sensors utilized in IoMT belong to a specialized subset of WSN known as Wireless Body Area Networks (WBANs). These sensors, often referred to as nodes, communicate and transmit the gathered data via wireless links, typically through gateways. Subsequently, the collected information is relayed to a central location, such as servers or databases, for further utilization.

In this section, we provide an overview of IoMT and the sensors utilized within it along with their architecture. Figure 1.3 represents the architecture of IoMT based on the aforementioned layers.

1.4.1 IoMT Architecture

Numerous academics have delved into the architecture of the Internet of Things (IoT), proposing various frameworks suitable for IoT applications. Among the prominent architectures are the EPC global architecture, Web of Things architecture, sensor network-based architecture, autonomous architecture, and Machine-to-Machine (M2M) architecture. Of these, the M2M

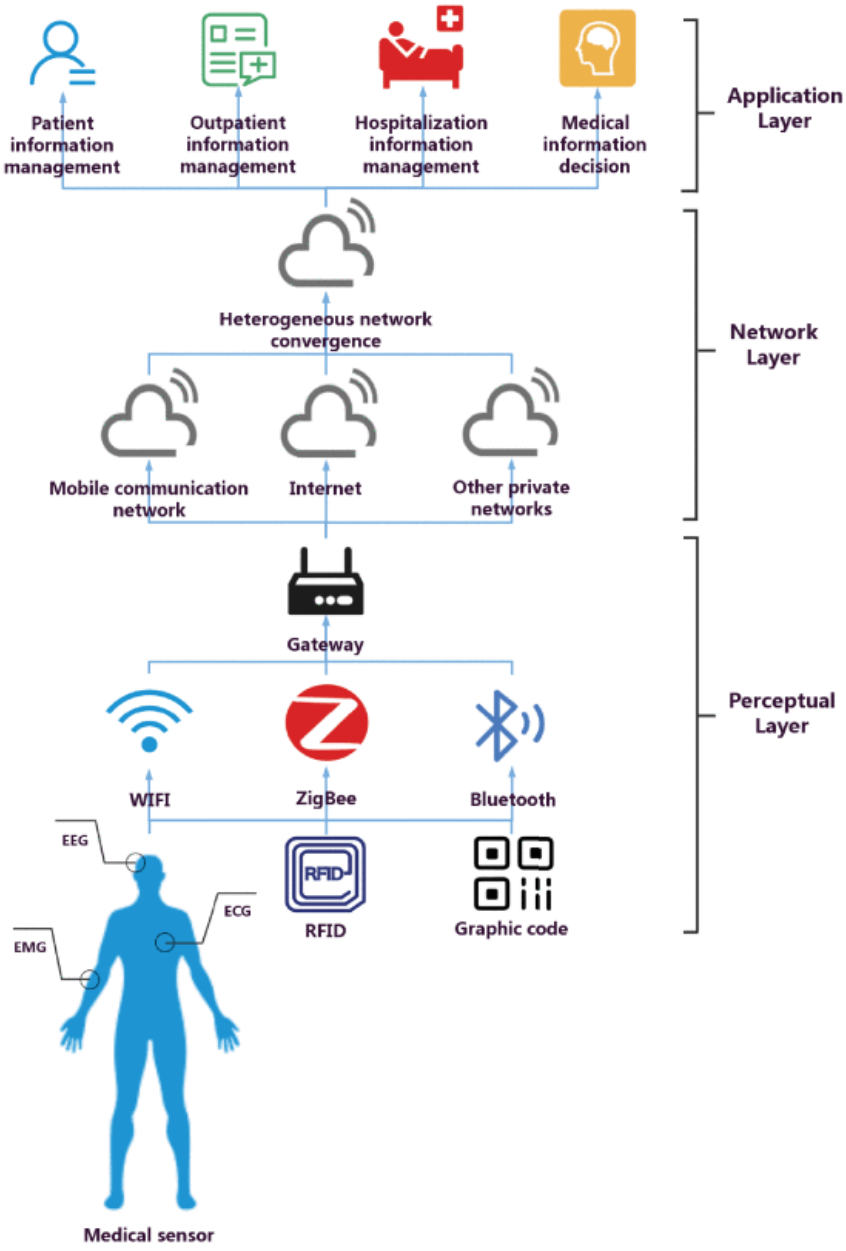


Figure 1.3: Layered IoMT Architecture [36]

architecture stands out as the most widely adopted, encompassing essential elements from EPCglobal and WSN. Within the medical domain, the Internet of Medical Things (IoMT) represents a focused application of IoT technology. Typically, IoMT applications adhere to the general three-tier architecture of IoT, comprising the application layer, network layer, and perception layer [37, 36].

Perception Layer

The focal point and complexity of IoMT lie within the perception layer, which comprises two main sublayers: data access and data acquisition. The data collection sublayer employs various medical perception and signal acquisition equipment to identify nodes in IoMT and gather data about entities. It utilizes signal acquisition techniques such as General Packet Ra-

dio Service (GPRS) technology [38], Radio Frequency Identification (RFID), image recognition, graphic coding, and diverse sensors including physical signal sensors. Physiological signal sensors, chemical sensors, and DNA sensors transform everything and everyone in the network into easily identifiable Cyber-Physical Systems (CPS) nodes [39]. In IoMT, nodes are categorized as passive CPS, active CPS, and Internet CPS based on different objects and requirements [39]. The data access sublayer connects the data collected by the data acquisition sublayer to the network layer through short-distance data transmission technologies like Bluetooth, Wi-Fi, ZigBee, etc. The choice of major access methods depends on the current IoMT environment and the requirements of various objects [40].

Network Layer

The network layer comprises two sublayers: the service layer and the network transmission layer. The network transmission layer serves as the backbone network of the Internet of Medical Things (IoMT), akin to a person's nerve center and brain. It utilizes the Internet, mobile communication networks, and other specific networks to transmit data information obtained by the perception layer in a real-time, reliable, accurate, and barrier-free manner [41]. Instead of replacing the original network entirely, the objective of IoMT is to explore integration technology of heterogeneous networks tailored for hospitals [42]. The service layer integrates heterogeneous networks and multiple data types, descriptions, data warehouses, and other data. It also develops a support service system with an open interface for different services in the application layer, enabling third parties to construct suitable applications for use by medical professionals and other relevant personnel [43].

Application Layer

The application layer encompasses health data decision-making applications and medical information applications. Medical data management applications include material management and medical equipment, patient data management, inpatient treatment data management, and outpatient data management, among others [44]. Examples of medical data decision-making applications comprise patient data analysis, disease data analysis, pharmaceutical data analysis, diagnosis, and therapy data analysis [45].

1.4.2 IoMT and WBANs

IoMT and WBANs are closely intertwined, playing complementary roles in modern healthcare systems. IoMT encompasses a vast array of interconnected medical devices and sensors, facilitating the collection, transmission, and analysis of health-related data. Within this framework, WBANs serve as a critical component by enabling seamless communication between wearable sensors and other IoMT devices. WBANs allow for the continuous monitoring of individuals' vital signs and physiological parameters, offering real-time insights into their health status. This synergy between IoMT and WBANs empowers healthcare providers to deliver

personalized and proactive care, improve patient outcomes, and enhance overall healthcare efficiency. Additionally, WBANs contribute to the advancement of remote patient monitoring, telemedicine, and other innovative healthcare applications, underscoring their indispensable role in the IoMT ecosystem.

1.4.3 Architecture of WBAN-based IoMT

Various architectures of WBAN-based IoMT can be observed in the literature, depending on the approach and application domain. However, a fundamental three-level architecture similar to the layer-based architecture for IoMT is common among existing works. This basic architecture serves as a foundation for all WBAN-based IoMT applications. Figure 1.4 illustrates the typical architecture of WBAN-based IoMT networks, which comprises three primary levels.

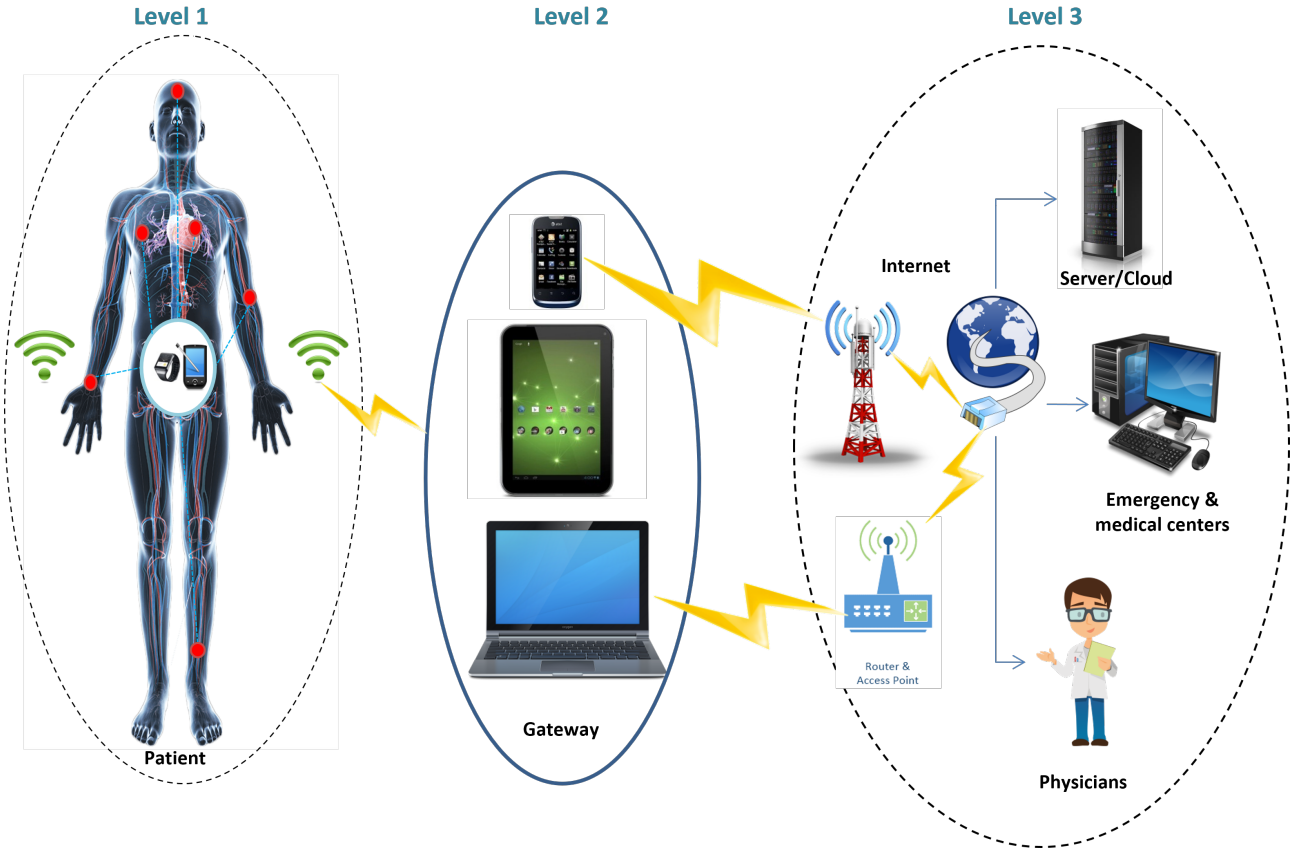


Figure 1.4: Architecture of WBAN-based IoMT

Level 1: This level comprises specialized sensors known as medical sensors. These nodes are designed to continuously measure, monitor, and collect specific biological signals. Subsequently, the gathered data are transmitted to devices at Level 2.

Level 2: Devices at this level primarily function as gateways (e.g., personal digital assistants, PDAs, computers, smartphones, etc.). They serve as an intermediary between Level 1 and Level 3 devices, responsible for transferring the collected data from Level 1 nodes to end-users at Level 3 via open communication channels.

Level 3: At this stage, the data and information received from Level 2 devices are transmitted to end-users via the Internet. These end-users vary depending on the IoMT network design and can include entities such as cloud platforms, emergency physicians, healthcare professionals, service providers, data analysts, family members, or even the patients themselves.

1.4.4 Medical sensors

Wireless medical sensors, integral components of IoMT, serve a specialized role in quantifying physiological metrics such as temperature, blood pressure, heart rate, electrocardiogram (ECG), and respiration [46, 47]. These sensors transmit the measured biological information to a control device worn on the body or positioned in an accessible location. They can be categorized into implant nodes, clothes-attached sensors, and body surface nodes (wearable), each serving distinct purposes [48, 49]. Predominantly used as either implanted or wearable devices, their close association with the human body makes them indispensable in various medical and healthcare applications. Furthermore, medical IoT sensors encompass a diverse array of types tailored to specific functions, including electrocardiogram (ECG), electroencephalogram (EEG), blood pressure, and body temperature sensors [50]. For instance, ECG sensors are utilized to monitor heart rhythm and diagnose abnormal patterns, whereas EEG sensors are employed to test and detect abnormalities in brain electrical activities. More detailed information on the types of medical sensors can be found in [50].

These sensors can be categorized into three classes based on their capabilities:

Class 0: devices that are very constrained in memory and processing capabilities, RAM space is less than 5KB and flash memory is less than 10KB. In addition, the class 0 device cannot be secured in the traditional sense.

Class 1: devices that are quite constrained in code space and processing capabilities, the RAM space is approximately 10 KB, and the flash memory space is approximately 100 KB. It provides support for security functions and is capable enough to use a protocol stack.

Class 2: devices that are less constrained, the RAM space is approximately 50 KB, and the flash memory space can reach up to 250 KB. Class 2 devices can benefit from lightweight energy-efficient protocols and support most protocol stacks.

Additionally, these sensors belong to a specialized category within Wireless Sensor Networks (WSNs) known as Wireless Body Area Networks (WBANs), which are extensively utilized in the realm of IoMT. WBANs are specifically designed to monitor physiological parameters and gather data from the human body. They play a crucial role in IoMT applications, facilitating continuous health monitoring, medical diagnostics, and personalized healthcare solutions.

1.5 Applications of IoMT

Numerous IoMT applications depend on WBANs to achieve the necessary efficiency and quality. Given WBANs' considerable capabilities, a wide array of new IoMT applications in

fields like medicine, home healthcare, and patient monitoring are being extensively embraced. Below, we'll outline and explain some of the most common healthcare applications in use today.

1.5.1 Records

It encompasses various types of health records, and we can categorize the usage of e-health records into three main forms:

- *Electronic Health Record (EHR)*: An electronic version of a patient's comprehensive health records, providing a detailed description of the patient's health status, securely accessible to authorized users [51].
- *Electronic Medical Record (EMR)*: An electronic report compiling the complete medical history of an individual patient within a particular clinic [52].
- *Personal Health Record (PHR)*: A report where the patient securely maintains their health-related data confidentially and privately [53].

1.5.2 Remote health monitoring

Remote health monitoring is an automated medical service that monitors patients' vital signs using WBANs. Various types of sensors can be positioned on or inside the patient's body to monitor physiological indicators such as heart rate, blood pressure, and temperature. The collected data is then stored in a central control unit or transmitted remotely for analysis and further evaluation [1].

1.5.3 Assisted living

The integration of WBANs in IoMT has introduced a novel approach where patients can remain at home while utilizing wearable medical sensors. These sensors continuously monitor the patient's physiological parameters. They can either store and transmit this data at regular intervals or, in certain scenarios, autonomously administer specific medications (for instance, insulin injection when required, as in the case of blood sugar sensors). Moreover, the system can trigger alerts to the nearest healthcare center when necessary [1].

1.5.4 Telecare medicine

Another domain of IoMT leveraging WBANs is telecare medicine. This approach enables the delivery of healthcare services remotely through the utilization of information and communication technologies, including WBANs [54]. By leveraging video and sensor technologies, healthcare providers can remotely assess patients' conditions and prescribe medications based on tele-sensed data, eliminating the need for physical presence.

1.6 Benefits

Integrating IoMT technology into the healthcare domain has ushered in a paradigm shift, resembling the futuristic visions of the 1990s. This revolutionary advancement has not only transformed internet communication but has also significantly impacted various sectors, particularly healthcare. By bridging the gap between doctors, patients, and healthcare services, IoMT offers unparalleled ease, accuracy, and flexibility [55].

One of the primary benefits of IoMT is its ability to enable healthcare professionals to perform their duties more precisely and efficiently, requiring less effort and intelligence. This integration has empowered patients with incredible advantages, as IoMT devices are user-friendly and facilitate seamless access to healthcare services.

The following list represents the major benefits provided by IoMT:

- The integration of IoT devices into healthcare not only makes life more convenient but also significantly reduces healthcare costs. Through real-time disease management, patient outcomes are greatly improved, leading to an overall enhancement in life quality. Additionally, IoMT enhances user experience and increases patient care, while simultaneously reducing costs through efficient resource management.

- Ultimately, the greatest benefit of IoMT is the promotion of healthier and longer lives, achieved through maximum disease management and prevention. With IoMT, the progress of children and elderly parents can be monitored closely, ensuring their well-being.

- A breakthrough of IoMT is its ability to automatically alert relevant parties in the event of significant changes in a patient's health, potentially saving lives and valuable time. Furthermore, the resources of IoMT extend beyond healthcare, facilitating connectivity and interoperability among various IoT devices for enhanced efficiency and effectiveness [55].

- Medication and family members intimation: Ensuring timely medication administration becomes feasible with IoMT, guaranteeing patients receive their medications promptly. Moreover, IoMT systems can automatically notify family members about the status of patient care, fostering better communication and support networks [56].

- Simplicity, affordability, and ease to use: IoMT solutions prioritize simplicity, offering user-friendly interfaces and streamlined processes for enhanced accessibility. Additionally, IoMT technologies strive for affordability, ensuring that cost barriers are minimized, and healthcare remains accessible to all. These systems are designed with ease of use in mind, allowing individuals to navigate them effortlessly for optimal health management [57].

- Doctors can effortlessly manage patient records through IoMT systems, facilitating efficient organization and accessibility of vital medical information [58].

- IoMT systems promote energy efficiency by optimizing various resources, including time and financial investments. Through streamlined processes and automation, IoMT solutions reduce energy consumption, saving both time and money for healthcare providers and patients alike [59].
- IoMT enables doctors to provide off-time medical services efficiently, ensuring round-the-clock access to healthcare through remote monitoring, telemedicine, and automated alerts for timely interventions [60].

In conclusion, IoMT has emerged as a game-changer in the medical field, offering many benefits to individuals, society, the environment, consumers, and businesses alike. From personalized healthcare solutions to improved operational efficiency, IoMT holds the promise of revolutionizing healthcare delivery and enhancing overall wellness.

1.7 Challenges in IoMT

The integration of WBANs in IoMT into healthcare systems has brought forth numerous benefits, but it also faces significant challenges. In this subsection, we represents the major challenges facing IoMT.

1.7.1 Limited resources

Sensor nodes are usually small in size and come with constrained resources such as computational power, storage capacity, communication bandwidth, and battery life. The limited energy reserves of these sensor nodes within the network pose lifespan challenges to WBANs used in IoMT. Addressing the issue of resource limitations necessitates efficient utilization [61]. Consequently, the implementation of energy-efficient protocols becomes imperative to extend the network's lifespan. Examples include energy-conscious routing at the network layer and energy-saving modes at the MAC layer. Additionally, optimizing the use of limited memory in sensors is crucial, considering memory-intensive tasks like routing tables, data replication, and security measures.

1.7.2 Scalability

The scalability of WBANs within the IoMT framework is a critical aspect that determines its effectiveness and widespread adoption. WBANs must be capable of accommodating an increasing number of interconnected devices and sensors seamlessly, without compromising performance or efficiency. Scalability in WBANs enables the network to handle growing volumes of data generated by an expanding array of medical sensors and devices [62]. This scalability extends beyond just the number of devices to encompass factors such as network coverage, data transmission rates, and interoperability with existing healthcare infrastructure [63]. A scalable WBAN infrastructure ensures that IoMT systems can adapt and grow to meet

the evolving needs of healthcare applications, supporting advancements in remote patient monitoring, telemedicine, and personalized healthcare delivery.

1.7.3 Cost of sensor platforms

The high cost of available sensor platforms on the market poses a significant barrier to widespread adoption. Additionally, the challenge of producing cheaper and disposable sensor platforms further complicates the situation [64].

1.7.4 Environmental factors

The environmental conditions within which WBANs operate play a crucial role in their performance and reliability. WBANs are designed to function in diverse environmental settings, ranging from indoor environments to outdoor conditions. Factors such as temperature fluctuations, humidity levels, electromagnetic interference, and physical obstructions can impact the performance of WBANs. Moreover, WBANs deployed in healthcare settings must adhere to stringent regulatory standards and safety requirements to ensure patient well-being and data integrity. As such, robust design considerations and resilient communication protocols are necessary to mitigate the effects of environmental challenges on WBANs, thereby ensuring continuous and reliable operation in various healthcare scenarios.

1.7.5 Inconsistent wireless communication

Communication within Wireless Body Area Networks (WBANs) is often characterized by its unreliability, attributed to the error-prone wireless medium with high bit error rates and variable link capacity. Consequently, for a WBAN to operate effectively, it must exhibit reliability tailored to meet the specific requirements of its intended applications [56]. It is imperative that sensed medical data be transmitted reliably to specialists, ensuring accurate and timely delivery for informed decision-making in healthcare settings.

1.7.6 Susceptibility to node failures

In IoMT networks, nodes are frequently susceptible to unforeseen failures due to various factors, such as depletion of energy or physical damage. Moreover, communication between two nodes may be permanently disrupted. As a result, WBANs in IoMT must exhibit resilience in the face of node failures. Consequently, to enhance fault tolerance, IoMT WBANs may opt to deploy a surplus of nodes beyond what is strictly necessary.

1.7.7 Security

Due to the deployment of sensor devices in typically unprotected environments, many IoMT applications demand a high level of security to meet basic security requirements and

safeguard against various cyber-attacks. This is crucial for preventing intruders from compromising the network's operation by gaining control of sensor nodes [65, 66, 59, 67]. Additionally, communications security poses a significant challenge for WBANs in IoMT. Wireless channels inherently lack security, rendering communications vulnerable to eavesdropping and message tampering by intruders, potentially resulting in severe health issues. Furthermore, the resource-constrained nature of sensor devices makes it impractical to implement conventional security schemes in WBANs, as they often entail high computational, communication, and memory overheads. Consequently, ensuring security in IoMT WBANs remains a challenging endeavor.

1.8 Cloud integration in IoMT

IoMT-based healthcare systems are projected to significantly enhance the quality of life, reduce healthcare costs, and expand users' medical knowledge. From a provider's perspective, the IoMT has the potential to minimize device interruptions through remote monitoring and maintenance. Additionally, IoMT can accurately predict optimal times for replenishing supplies for various medical devices, ensuring their continuous and efficient operation. It also facilitates the effective scheduling of limited resources, optimizing their use and improving service delivery to new patients.

Cloud computing offers a range of services, including databases, servers, software, data analytics, and networking, over the Internet. This infrastructure enables flexible resource allocation, faster deployment of applications, and cost efficiencies through economies of scale. IoMT devices can seamlessly integrate with cloud services, leveraging them for the storage and processing of vast amounts of medical data. This integration supports enhanced data management and analysis, contributing to more informed healthcare decisions and improved patient outcomes [68, 69, 70].

1.8.1 Cloud Computing in Healthcare Systems

Cloud computing is a technology that delivers vast resources and computing services over a network, typically the Internet. Essentially, it involves using online servers for data storage, management, and processing. This technology offers numerous benefits, including virtual hardware, collaboration software, virtual storage, and virtual servers. In this context, the term "cloud" symbolizes the Internet.

Researchers have identified cloud computing as a novel and emerging information and communication technology (ICT) service model [71]. There are multiple descriptions of cloud computing, with one study listing 22 different definitions [72]. Cloud computing services are categorized into three main types: Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS)[73].

Cloud computing can be deployed in four types of clouds [68]:

- *Public Cloud:* Accessible to the general public and provided by companies like Amazon.

- *Private Cloud:* Used exclusively by a single organization.
- *Hybrid Cloud:* A combination of public and private clouds.
- *Community Cloud:* Shared among organizations with similar interests.

In healthcare, cloud computing enables on-demand access to a wide range of information from sources such as claims, electronic medical records (EMRs), laboratory data, and medication records. It can notify doctors about missed or conflicting prescriptions in drug regimens, particularly for chronic conditions like asthma.

The advantages of cloud computing in healthcare include [74]:

- *Customized Service:* Patient requests can be automatically fulfilled without human intervention.
- *Network Access:* Patient applications can operate on various devices, including laptops, tablets, and smartphones.
- *Remote Access:* Patients can access cloud services without needing to know the physical location of the data or the underlying infrastructure.

These features highlight the transformative potential of cloud computing in enhancing healthcare delivery and patient outcomes.

1.9 Conclusion

The integration of WBANs into the IoMT constitutes an emerging technology that has garnered significant attention from researchers and developers due to its unique characteristics. However, WBANs encounter various challenges and limitations due to the nature of the medical sensors used within them, necessitating attention from researchers. This chapter has provided an overview of key concepts related to IoMT and WBANs, including their architecture, applications, and the primary challenges and limitations they face. The subsequent chapter will delve into a detailed examination of security and cryptography in IoMT WBANs.

CHAPTER 2:

Security and Cryptography in IoMT

Chapter 2

Security and Cryptography in IoMT

2.1 Introduction

The integration of WBANs in IoMT into healthcare systems has brought forth numerous benefits, but it also faces significant challenges. Researchers have diligently addressed these hurdles to ensure the seamless implementation and efficacy of IoMT solutions. Among the most critical challenges are data security and privacy concerns, as the vast amounts of sensitive medical information transmitted through IoMT devices require robust encryption and authentication mechanisms to safeguard against unauthorized access. Another key issue is interoperability, as IoMT devices from different manufacturers must seamlessly communicate and share data to provide comprehensive patient care. Additionally, ensuring the reliability and accuracy of IoMT devices poses a challenge, as any malfunction or erroneous data could have serious implications for patient health. Moreover, the scalability of IoMT systems to accommodate the growing volume of connected devices and the need for standardization in IoMT protocols and regulations are pressing concerns that researchers have diligently addressed to propel the advancement of IoMT technology.

This chapter provides an introduction to several fundamental concepts that serve as background knowledge for understanding the thesis. The initial section delves into the security aspects of Wireless Body Area Networks (WBANs), covering topics such as security constraints, essential security requirements, and potential cyber-attacks targeting wireless sensor networks. Subsequently, the chapter proceeds to review cryptographic principles and primitives, along with the computational assumptions relevant to the thesis.

2.2 Security Constraints

WBANs are governed by various constraints that render conventional security schemes designed for IoMT unsuitable at their level. Hence, it becomes imperative to tailor these schemes to accommodate the specific characteristics of WBANs. The development of robust security schemes in WBANs necessitates a comprehensive understanding of the following constraints [75, 76].

2.2.1 Resource limitations

To implement any security approach, certain resources are required, including processing power, data storage, code space, and energy to power the sensors. Unfortunately, these resources are severely limited in tiny wireless sensors.

- Limited amount of energy: The most significant constraint in wireless sensor technology is energy availability. Sensor nodes are often unable to be readily replaced or recharged once deployed into a sensor network. Therefore, conserving battery power in the field becomes imperative to extend the life of each sensor node and the entire network. Additionally, it's essential to consider the energy impact of adding security codes to a sensor node when implementing cryptographic functions or schemes.

- Limited processing capability: Sensor node microcontrollers are typically slow and incapable of performing certain arithmetic operations. This limitation makes it challenging to execute very complex security schemes or operations.

- Limited storage capability: Sensor devices possess an extremely limited amount of memory, often just a few kilobytes. Consequently, any security scheme designed for sensor networks should consume minimal memory to ensure efficient operation.

2.2.2 Unreliable communication

Unreliable communications pose a significant threat to sensor security within a network. The effectiveness of security schemes in a sensor network is heavily reliant on wireless communication. However, the inherently insecure nature of wireless channels makes any transmission vulnerable to interception, alteration, or re-transmission by adversaries. Malicious nodes can also disrupt data packets by causing collisions and interference in the communication channel[77]. Moreover, wireless communications incur high energy costs, with transmitting a single bit requiring approximately 1,000 microcontroller operations. As a result, implementing complex security schemes involving multiple message exchanges between sensor nodes becomes impractical.

2.2.3 The unguarded environment

WBANs face significant risks due to their deployment in unguarded environments. These risks stem from potential physical tampering, unauthorized access, and exposure to environmental hazards. Such unguarded environments increase the susceptibility of WBANs to malicious attacks, data breaches, and device tampering, compromising the integrity and security of medical data and patient privacy. Therefore, safeguarding WBANs against these risks is paramount to ensure the reliability and security of healthcare services.

2.3 Security and privacy requirements

Given the nature of deploying sensor devices, often in unprotected environments, the majority of IoMT applications demand a high-security level. This ensures that basic security requirements are met, rendering these applications resilient against various cyber-attacks. Such measures prevent intruders from disrupting the network's operation and gaining control of sensor nodes. The fundamental security requirements for WBANs include[78, 1, 79, 80]:

2.3.1 Anonimity

Anonimity encompasses the safeguarding of a user's true identity, prioritizing their privacy and shielding them from exposure. This entails ensuring that no method or avenue exists through which the user's actual identity can be discerned, thus maintaining their anonymity intact.

2.3.2 Untraceability

Untraceability serves to thwart any attempts by adversaries to backtrack communication pathways to the user, be it a sensor node or any other participant engaged in the session. It ensures that the origin of communication remains obscure, preventing any tracing back to its source by external parties.

2.3.3 Data Confidentiality

Data confidentiality is a fundamental security requirement in any sensor network, ensuring that information remains undisclosed and accessible only to authorized parties. Cryptographic techniques are commonly employed as countermeasures against confidentiality threats.

2.3.4 Data Integrity

This requirement pertains to ensuring that messages remain unaltered while traversing the network, whether intentionally or inadvertently. In such scenarios, the receiver can verify that the received message aligns with the one sent by the sender.

2.3.5 Authentication

It is crucial to consistently verify the sender's identity for any message exchanged within the network. Ensuring communication with the correct node is essential to uphold the confidentiality and integrity of exchanged messages. A compromised authentication process could enable adversaries to infiltrate the network and inject false information.

2.3.6 Availability

Network services should remain available even in the face of cyber-attacks or malfunctions in a portion of the network. WBANs are service-oriented networks, specifically engineered to deliver well-defined and often critical medical services. Consequently, even if a sensor network becomes the target of an attack, it should strive to withstand such threats and uphold the availability of its resources and services to the greatest extent possible.

2.3.7 Freshness

Data freshness refers to the timeliness of data, ensuring that it is recent and preventing adversaries from re-transmitting old messages. To meet this security requirement, a nonce or another time-related counter can be included in the packet.

2.3.8 Non-repudiation

In cybersecurity, non-repudiation denotes the capability to verify that both the sender and receiver are indeed the parties claiming to have sent or received the message. Hence, non-repudiation of data origin establishes that the data was indeed sent by the claimed sender. Conversely, non-repudiation of receipt confirms that the data was indeed received by the claimed recipient.

2.4 Cyber-attacks in IoMT

Network security encompasses the suite of policies, mechanisms, and services implemented to safeguard a network from cyber-attacks and unauthorized access [81]. Security within IoMT WBANs presents numerous challenges, particularly in applications requiring heightened security levels, such as emergency response and healthcare [82, 83]. Sensor devices are commonly deployed in unprotected environments, rendering them susceptible to increased cyber-attacks that can compromise sensitive data and impede network performance [75, 84]. Cyber-attacks targeting IoMT WBANs can be categorized into three main types: attacks on confidentiality, attacks on the reliability of traffic data, and attacks on availability. Figure 2.1 illustrates the classification of cyber-attacks in WBAN-based IoMT applications.

2.4.1 Attacks on confidentiality

This relates to the passive adversary, who can intercept messages exchanged between sensor nodes via a communication channel, thereby gaining access to the message contents circulating in the network. If the exchanged messages are encrypted, the adversary endeavors to decrypt them by testing numerous potential keys until the correct secret key is identified.

- Eavesdropping: Among all attacks targeting data confidentiality, this cyber-attack is the simplest to execute. The adversary can eavesdrop on messages exchanged between nodes,

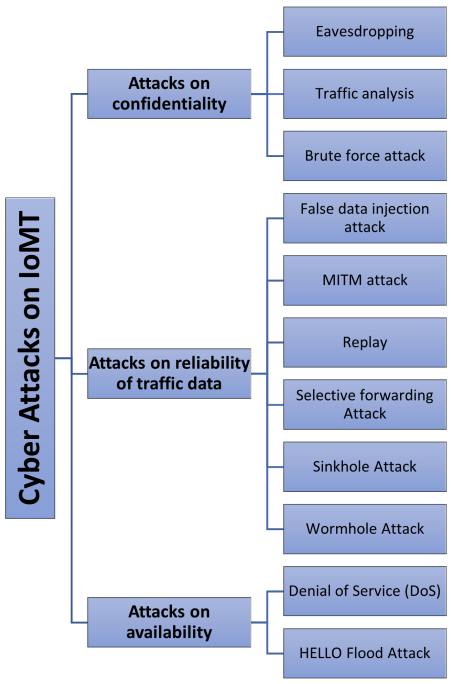


Figure 2.1: Taxonomy of cyber-attacks on IoMT

enabling them to intercept strategic information that could be exploited to launch more damaging attacks.

- Traffic analysis: Through traffic analysis, the adversary can identify sensor nodes with specialized and crucial roles within the network. For instance, an uptick in the volume of messages exchanged between sensors indicates the occurrence of specific activities and events warranting monitoring. Moreover, the adversary can pinpoint level 2 nodes without necessarily deciphering the message contents[75, 85].

- Brute force attack: To decrypt messages exchanged during data transmission, an adversary engages in a process of trial and error, testing a multitude of potential keys in an attempt to ascertain the correct ones.

- Node capture attack: in this attack, the adversary gains access to a node within the network. This breach affords the adversary a comprehensive view of the authentication protocol's current state. Moreover, the captured node grants the adversary possession of the cryptographic keys and primitives utilized within the network infrastructure. This enables the adversary to replicate and introduce malicious nodes into the network, thereby compromising its integrity and security.

2.4.2 Attacks on reliability of traffic data

The adversary may attempt to compromise the integrity of the network by injecting erroneous data, replaying previous messages, and altering messages transmitted by sensor nodes. This manipulation is aimed at distorting the final outcome or result.

- False data injection attack: During the aggregation process, a malicious node deliberately sends random false data to the intended level 2 to distort the aggregation outcome. Consequently, the level 2 node unknowingly accepts and aggregates the data transmitted by the malicious node, leading to an erroneous final result, as depicted in Figure 2.2. To mitigate this attack, countermeasures such as node authentication [86] or end-to-end encryption can be implemented. These measures prevent the injection of fake data packets or modification of packet contents.

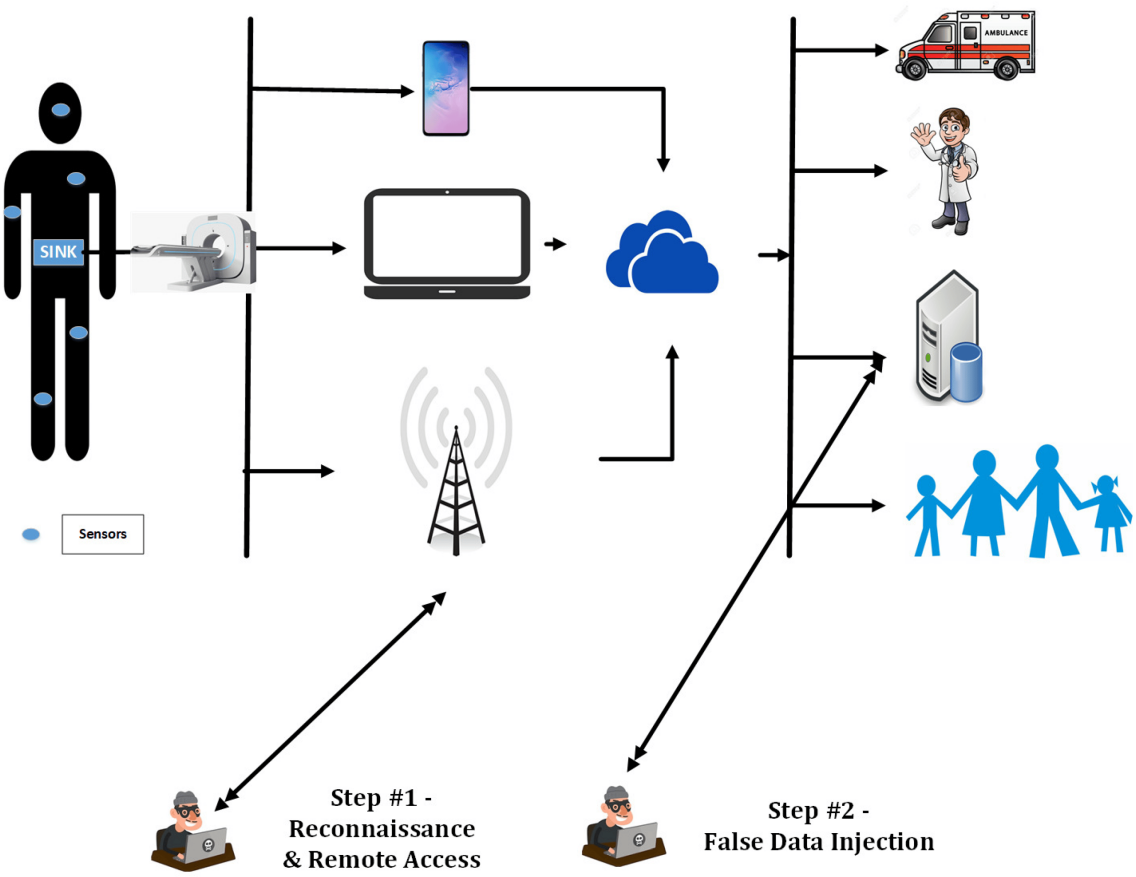


Figure 2.2: Conceptual view of False Data Injection in the IoMT

- MITM attack: The adversary clandestinely modifies communication and intercepts messages exchanged between two or more parties (e.g., user, server, and sensor node). In this scenario, the adversary has the capability to alter or impersonate one of the entities, while also pilfering authentication data. Additionally, the adversary can initiate communication with one of the parties, enabling them to send or receive critical data.

- Replay: After successfully eavesdropping on the communication channel, the adversary utilizes the captured data, primarily authentication messages, for malicious purposes. They may replay the captured data to gain unauthorized access to the system or masquerade as a legitimate entity.

- Sinkhole Attack: In this attack, a malicious node manipulates the routing metrics to divert

all traffic from a specific area. Consequently, neighboring nodes are misled into believing that a high-quality path exists and begin forwarding packets to the malicious node. This tactic, known as a sinkhole attack, involves the gathering of traffic to compromise the integrity and reliability of data collected by the network's sensor nodes [87].

- Wormhole Attack: This attack occurs when an adversary intercepts messages being transferred in a specific location and tunnels them to another location, where a second adversary replays them in a different area.

2.4.3 Attacks on availability

- Denial of Service (DoS): The adversary inundates the network with numerous captured or counterfeit messages aimed at the server or sensor, thereby impeding its ability to offer services and compromising its availability. In this attack, the replayed messages tend to exhaust all the resources of the server or sensor, including storage, computational power, and energy, rendering it incapable of processing any additional requests.

- Distributed Denial of Service (DDoS): These attacks pose a significant threat to WBANs, where interconnected wearable devices monitor physiological parameters. In the context of WBANs, DDoS attacks involve flooding the network infrastructure with an overwhelming volume of illegitimate traffic, aiming to disrupt communication between wearable devices and the central monitoring system. Such attacks can severely impact the reliability and real-time monitoring capabilities of WBANs, potentially endangering the health and safety of individuals relying on these networks for medical monitoring and emergency response. As WBANs typically operate within constrained resources and bandwidth, mitigating DDoS attacks requires robust security measures, including intrusion detection systems, authentication mechanisms, and traffic filtering techniques, to ensure uninterrupted and secure communication within the network.

- HELLO Flood Attack: Sending HELLO packets is a common method for identifying neighboring nodes. When a sensor node receives such a packet, it assumes that the transmitter is within its communication range. Exploiting this, a laptop-class adversary equipped with a high-powered antenna floods sensor nodes with HELLO messages. Upon receiving these messages, the remote node perceives the adversary as a neighbor within communication range and attempts to transmit messages directly to it. This results in message transmission failures and disrupts network operations by preventing the exchange of other messages.

2.5 Cryptographic techniques in IoMT

Cryptography serves as a vital security measure for safeguarding communication in open IoMT networks. It ensures security requirements such as data confidentiality, integrity, authen-

tication, and non-repudiation. Selecting suitable cryptographic primitives is crucial in IoMT, considering the resource constraints of sensor nodes. Cryptography-based schemes in IoMT need to be evaluated for their impact on energy consumption, processing time, code size, and data size [88].

There are two main categories of cryptographic techniques: Symmetric-Key Cryptography (SKC) and Public-Key Cryptography (PKC). SKC offers good performance in terms of computational overhead and energy consumption but lacks support for non-repudiation and requires complex key distribution. PKC addresses these issues by providing a more flexible interface and eliminating the need for key pre-distribution and pairwise key sharing. However, PKC is computationally expensive for resource-constrained sensor nodes [88, 89].

2.5.1 Symmetric-Key Cryptography

SKC, also referred to as symmetric-key cryptography, involves the sender and receiver sharing a secret key at the outset of communication. Subsequently, they utilize this shared key to encrypt and decrypt messages exchanged between them. One of the most widely recognized symmetric algorithms is the Advanced Encryption Standard (AES) [90]. We define an SKC scheme in the following Definition 2.5.1.

Definition 2.5.1 *(SKC scheme). A secret-key cryptography (SKC) scheme with an input security parameter k is defined by a pair of deterministic algorithms (Enc, Dec) as follows:*

- *$Enc(K, M) \rightarrow C$. This represents the encryption algorithm, where K is a key from the set $\mathcal{K}$, and M is a message from the set $\mathcal{M}$ of plaintexts. It produces an encrypted message C from the set of ciphertexts $\mathcal{C}$.*
- *$Dec(K, C) \rightarrow M$. This denotes the decryption algorithm, where K is the same secret key, and C is the ciphertext. It outputs the original message M.*

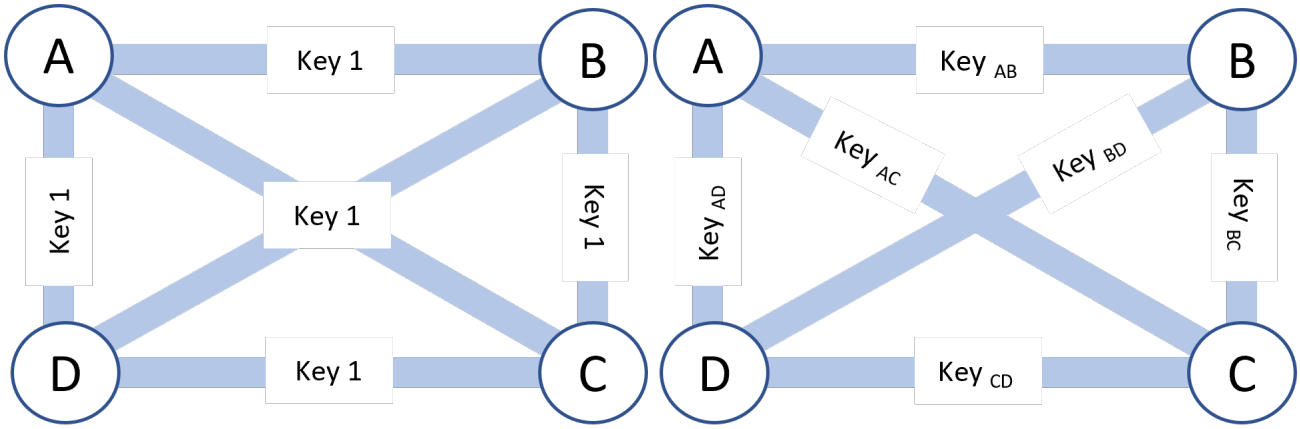
It is essential that the equation $Dec(K, Enc(K, M)) = M$ holds for every $K \in \mathcal{K}$ and $M \in \mathcal{M}$.

Advanced Encryption Standard (AES): is one of the most known and most used symmetric encryption functions nowadays. It is a subset of the Rijndael block cipher. It was developed Vincent Rijmen and Joan Daemen. AES was designed and based around substitution-permutation network which supersedes the Data Encryption Standard(DES). AES-x uses x-bit key length to encrypt and decrypt a block of messages. Each type encrypts and decrypts data in blocks of x-bits using cryptographic keys of x, where x can be 128, 192, 256 respectively. AES is widely used due to its great performance and high security where it can be improved by increasing the key size. However, it doesn't support key exchange.

To SKC in the IoMT, a shared-key distribution mechanism is essential. Key distribution methods can be categorized into three main groups:

- **A Global key (or network key):**A global key, or network key, refers to a straightforward method of distributing keys by using the same key for all sensor nodes (as depicted in

Figure 2.3a). In this scenario, all sensor nodes are pre-configured with the global key, allowing secure communication between any two nodes. However, if an adversary obtains the global key, they can gain control over the entire network.



(a) (b)

Figure 2.3: Cases of using a global key and pairwise key.

- **A pairwise key:** Another technique involves using a secret key shared by pairs of nodes (as illustrated in Figure 2.3b). If one node is compromised, the security of the other nodes remains intact. Employing this technique enhances the network's resilience against attacks. However, in an IoMT network comprising n nodes, each node would need to store $n-1$ keys, and the entire network would require storage for $n(n-1)/2$ keys. As a result, this approach demands a considerable amount of memory, especially when n is large.
- **A group key:** A group key is a secret key shared among a specific group of nodes. If an adversary manages to obtain the group key, they can compromise all the nodes within that group.

2.5.2 Public-Key Cryptography

Public-key cryptography (PKC), also known as asymmetric cryptography, enables two parties to exchange data securely over an insecure channel while ensuring data confidentiality, non-repudiation, and authenticity. Unlike symmetric encryption, which relies on a shared secret key between two parties, PKC utilizes a pair of keys for data protection. This key pair consists of a public key and a private key, which are related by a mathematical equation. Solving this equation involves breaking a hard mathematical problem, such as the Discrete Logarithm Problem (DLP). Each party shares its public key while keeping its corresponding private key confidential. Definition 2.5.2 represents the the PKC formalities.Figure 2.4 illustrates the encryption process in PKC. Mature public-key cryptographic algorithms such as ECC, PBC, and RSA have been extensively researched by the academic community. RSA was designed by Rivest, Shamir, and Adleman in 1977 [91], while ECC was independently proposed by Koblitz and Miller in 1985 [92, 93].

Definition 2.5.2 *A PKC scheme with an input security parameter k is defined by a tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ as follows:*

- *$\mathcal{E}(pk, m) \rightarrow c$. This represents the encryption algorithm, where pk is the public key from the set $\mathcal{K}$ of public keys and m is a message from the set $\mathcal{P}$ of plaintexts. It produces an encrypted message c from the set of ciphertexts $\mathcal{C}$.*
- *$\mathcal{D}(sk, c) \rightarrow m$. This denotes the decryption algorithm, where sk is the corresponding private key from the set $\mathcal{K}$, and c is the ciphertext. It outputs the original message m.*

It is essential that the equation $\mathcal{D}(sk, \mathcal{E}(pk, m)) = m$ holds for every $(pk, sk) \in \mathcal{K}$ and $m \in \mathcal{P}$.

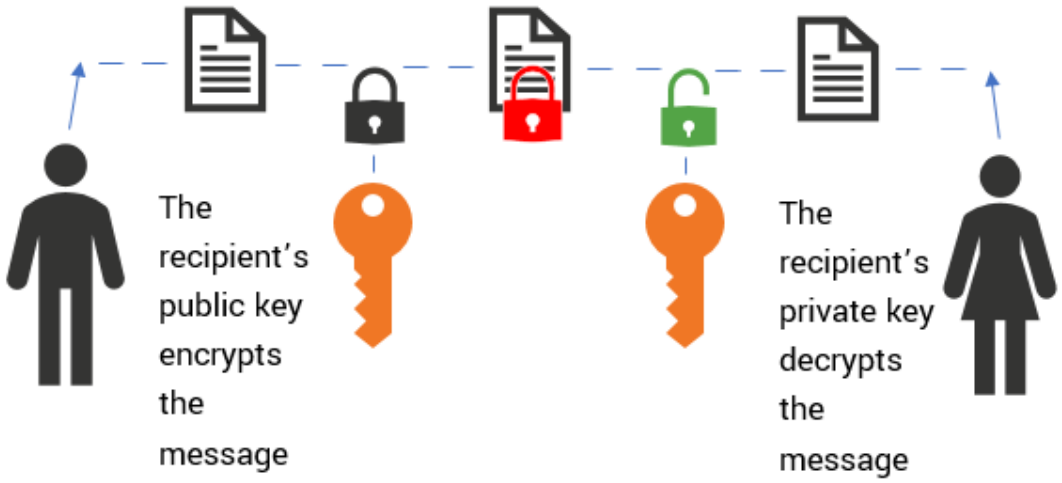


Figure 2.4: Public key cryptography

Elliptic curve cryptography (ECC)

ECC is a public key cryptography approach proposed by Kobleitz [92] and Miller [93] in 1985. ECC is considered security alternative to RSA for resource-constrained devices. This is due to the 160-bit key provides an equivalent security 1024-bit RSA key. Therefore, ECC saves the storage space and reduces the computational overhead and energy consumed by the device. Table 2.1 represents a comparison of the key sizes between RSA and ECC while ensuring the same level of security. The description of elliptic curves is similar to ellipses due to the use of cubic equations in both. It is based on the algebraic structure of elliptic curves over finite fields. We can define it as follow:

Definition 2.5.3 *Consider F_p a finite field with prime order p based on a non singular elliptic curve E defined as follow: $E: \ y^2 = x^3 + ax + bx$ Let O be the point at infinity then O and other points on E make an additive elliptic curve group G having order q and generator P [94].*

Table 2.1: RSA and ECC key length equivalence for the same security level [92]

Security level	80	112	128	256
RSA key length (bits)	1024	2024	3072	15360
ECC key length (bits)	160	224	256	512

ECC depends mainly on point addition and scalar multiplication in additive groups.

The addition in additive groups is defined as:

Definition 2.5.4 *Let P and S be two randomly chosen points on the elliptic curve E such that $(P, S) \in G$, where P generates the group G with a large prime order q. If $P = S$, then $R = P+S$ can be computed, where R represents the intersection point of E and the line connecting P and S. If $P = S$, then $R = P + S$, and if $P = -S$, then $P + S = O$.*

The scalar multiplication on the elliptic curve E is defined as:

Definition 2.5.5 *$mP = P + P + P + \cdots + P$ for m times where $m \epsilon \mathbb{Z}^*$.*

Pairing Based cryptography (PBC)

The PBC is a related mathematical mechanism to elliptic curve cryptography. The main goal of the PBC mechanism is to construct a mapping between two elliptic curve groups of points, called a bilinear pairing function.

Definition 2.5.6 *Let G_1, G_2 denote two additive groups of prime order q, and G_T is multiplicative group of order q. The bilinear pairing is a map*

$$\hat{e} : G_1 \times G_2 \longrightarrow G_T$$

That satisfies the following properties:

- *Bilinearity: $\forall a, b \in F_q^*,\ \forall P \in G_1,\ Q \in G_2 : e(aP, bQ) = e(P, Q)^{ab}$.*
- *Non degeneracy: there exists $P \in G_1, Q \in G_2$ such that $\hat{e}(P, Q) \neq 1$.*
- *Computability: for all $P \in G_1$ and $Q \in G_2$ an efficient algorithm exists to compute $\hat{e}(P, Q)$.*

2.5.3 Post Quantum Cryptography (PQC) Emergence

In this section, we will present the differences between classical cryptography, quantum cryptography, and post-quantum cryptography, highlighting their unique characteristics and applications. Additionally, we will delve into the emergence of post-quantum cryptography (PQC) within the IoMT. As IoMT continues to evolve, the integration of PQC becomes crucial to counteract the potential threats posed by quantum computing. We will explore how PQC is enhancing data security, protecting patient information, and ensuring the reliability of medical devices in this connected healthcare landscape.

Definitions

Classic Cryptography

"Classic cryptography" encompasses the traditional cryptographic methods that have been employed for centuries to secure communication. These methods use mathematical algorithms and keys to encrypt and decrypt information, ensuring data confidentiality and integrity. Classic cryptographic systems are categorized into two main types: symmetric-key algorithms and asymmetric-key algorithms.

Symmetric-key algorithms described in the sections above, such as the DES and the AES, use the same key for both encryption and decryption. This means that both the sender and the receiver must possess the shared secret key. DES, once widely used, has largely been replaced by AES due to the latter's higher security standards and efficiency. AES is now a global standard for data encryption, widely used in various applications, including government and financial services.

Asymmetric-key algorithms described in sections above, on the other hand, utilize a pair of keys: a public key and a private key. Notable examples include RSA and the Diffie-Hellman key exchange. In RSA, the public key is used to encrypt data, while the private key is used to decrypt it, providing a secure way to exchange information even if the public key is openly shared. The Diffie-Hellman algorithm, meanwhile, allows two parties to securely share a secret key over an insecure communication channel, which can then be used for symmetric encryption.

Classic cryptography has laid the foundation for modern cryptographic practices, evolving to meet the increasing demands for security in the digital age. Despite advancements in cryptographic techniques, the principles of classic cryptography remain integral to understanding and developing robust security systems today.

Quantum Cryptography

Quantum cryptography is a cutting-edge field of cryptography that harnesses the principles of quantum mechanics to create secure communication channels. Unlike traditional cryptography, which depends on the computational complexity of mathematical algorithms, quantum cryptography relies on the fundamental laws of physics to safeguard information.

One of the most notable applications of quantum cryptography is Quantum Key Distribution (QKD). QKD enables the secure sharing of encryption keys using quantum properties like entanglement and the uncertainty principle. In QKD, keys are transmitted as quantum bits (qubits), which are delicate and easily disrupted by any attempt at eavesdropping. This ensures that any interception of the key can be detected, providing an unparalleled level of security.

The use of entanglement in QKD allows for the creation of pairs of qubits that are intrinsically linked, so that the state of one qubit instantaneously influences the state of its entangled partner, no matter the distance between them. This phenomenon enables the detection of any interception attempts, as any eavesdropping would disturb the entangled states, revealing the presence of an intruder.

The uncertainty principle, another cornerstone of quantum mechanics, asserts that certain pairs of physical properties, such as position and momentum, cannot both be precisely measured

simultaneously. In the context of QKD, this principle ensures that any measurement of the quantum key by an eavesdropper will inevitably alter its state, thus signaling an intrusion.

Quantum cryptography represents a significant advancement in the field of secure communications, offering a level of security based on the immutable laws of physics. As research and technology in this domain continue to evolve, quantum cryptography is poised to play a crucial role in the future of data security, providing robust protection against increasingly sophisticated cyber threats.

Post Quantum Cryptography (PQC)

"Post-quantum cryptography" is a field of cryptography dedicated to developing encryption methods that remain secure against adversaries equipped with quantum computers. Quantum computers pose a significant threat to current cryptographic algorithms, especially asymmetric ones. Presently, all 10 widely used asymmetric cryptographic methods—including RSA, ECC, Diffie-Hellman (DH), and the Digital Signature Algorithm (DSA)—can be broken by a sufficiently powerful quantum computer. This vulnerability arises because these methods rely on the Prime Factoring Problem or the Discrete Logarithm Problem, both of which can be efficiently solved using Shor's Algorithm [95].

The development and implementation of post-quantum cryptographic techniques are crucial to ensure data security in the impending era of quantum computing. These new methods are designed to withstand the computational power of quantum algorithms, thereby maintaining the confidentiality and integrity of information in a post-quantum world.

PQC Families

In this section, we provide a concise overview of the primary families for which post-quantum primitives have been suggested. These families encompass those founded on lattices, codes, and multivariate polynomials, among a few others. For more detailed information.

Lattice-based cryptography

"Lattice-based" cryptosystems have garnered renewed attention due to several compelling reasons. These include the emergence of exciting new applications like fully homomorphic encryption, code obfuscation, and attribute-based encryption, all made feasible through lattice-based cryptography. Moreover, many lattice-based key establishment algorithms boast simplicity, efficiency, and high parallelizability. Additionally, the security of certain lattice-based systems is provably guaranteed under worst-case hardness assumptions, rather than relying on average-case scenarios. However, accurately estimating the security of lattice schemes against known cryptanalysis techniques remains challenging [96].

Code-based cryptography

"The McEliece cryptosystem", introduced in 1978, remains unbroken to this day, establishing a robust foundation for code-based cryptography. Despite its resilience, subsequent systems based on error-correcting codes have been developed. Although generally efficient, many code-based primitives are burdened with notably large key sizes. Recent variants have aimed to mitigate this issue by incorporating more structure into the codes, albeit at the risk of suscep-

tibility to attacks. While code-based signatures have been proposed, encryption schemes have seen greater success within the realm of code-based cryptography [96].

Multivariate polynomial cryptography

"Multivariate cryptography" relies on the challenge of solving systems of multivariate polynomials over finite fields. Over the past few decades, numerous multivariate cryptosystems have been put forward, although several have been compromised. Despite this, multivariate cryptography has found greater success as a method for creating signature schemes, with fewer proposals focusing on encryption schemes [96].

Hash-based signatures

"Hash-based signatures" are digital signatures created through hash functions, offering robust security even in the face of quantum attacks. However, some efficient hash-based signature schemes come with certain limitations. For instance, signers must accurately maintain a record of previously signed messages, as any error in this record could compromise security. Additionally, these schemes are often restricted in the number of signatures they can produce. While it's possible to increase the number of signatures, doing so typically results in larger signature sizes [96].

Classical vs Quantum Computing

Classical computing operates on binary bits, which can exist in one of two states: 0 or 1. In contrast, quantum computing harnesses the power of quantum bits, or qubits, which possess the unique ability to exist in a superposition of states, meaning they can simultaneously represent both 0 and 1. This fundamental distinction enables quantum computers to execute specific computations exponentially faster than their classical counterparts [97].

To illustrate the difference between classical bits and qubits, consider their respective representations:

A classical bit is described by two distinct states:

$$0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad 1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2.1}$$

Here, 0 signifies the state where the classical bit is in state 0, and 1 denotes the state where the classical bit is in state 1.

On the contrary, a qubit can exist in a superposition of the 0 and 1 states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.2}$$

Here, α and β are complex amplitudes satisfying $|\alpha|^2 + |\beta|^2 = 1$. Upon measurement, the probability of observing the qubit in the 0 state is $|\alpha|^2$, and in the 1 state is $|\beta|^2$.

Moreover, quantum computing introduces the concept of entanglement, where multiple qubits can become correlated such that the state of one qubit is dependent on the state of another, even when physically separated. This entanglement property empowers quantum com-

puters to tackle specific computations more efficiently than through superposition alone.

While quantum computing offers unparalleled advantages in terms of computational speed and efficiency for certain tasks, it also presents a formidable challenge to classical cryptographic systems. Quantum algorithms, such as Shor's algorithm, have the potential to efficiently factor large numbers, threatening conventional public-key cryptography schemes like RSA. Hence, there is a critical need to develop and adopt post-quantum cryptographic techniques to safeguard against potential attacks from quantum computers.

Shor's and Grover's Algorithms

In the field of factorization, the General Number Field Sieve (GNFS) is currently the most efficient classical algorithm for factoring large numbers. The complexity of GNFS is subexponential, approximately given by $O\left(\exp\left(\left(\frac{64}{9}\right)^{\frac{1}{3}} \cdot (\ln N)^{\frac{1}{3}} \cdot (\ln \ln N)^{\frac{2}{3}}\right)\right)$, where N is the number being factored. Despite its efficiency, the runtime of GNFS increases rapidly with the size of the input number, making it impractical for factoring extremely large numbers [98].

In stark contrast, Shor's algorithm [99] revolutionizes factorization by leveraging quantum computing principles. Unlike classical algorithms, Shor's algorithm uses quantum parallelism and quantum entanglement to achieve an exponential speedup. The complexity of Shor's algorithm is $O\left((\log N)^3\right)$, where N is the number to be factored. This represents a significant breakthrough, as it allows quantum computers to factorize large numbers exponentially faster than classical computers, highlighting the profound potential of quantum computing to disrupt fields like cryptography and number theory.

In the domain of unstructured search problems, classical algorithms generally exhibit linear time complexity, requiring an average of $O(N)$ steps to locate a specific item within an unsorted database of size N. However, Grover's algorithm [100] provides a remarkable quadratic speedup when run on a quantum computer, reducing the complexity to $O(\sqrt{N})$. This makes Grover's algorithm substantially more efficient than the best-known classical search algorithms, underscoring the power of quantum computing in solving a wide range of problems more efficiently.

Table 2.2 represents a brief comparison between classical, quantum, and PQC in terms of security, implementation, key exchange, and performance.

PQC in IoMT

PQC has emerged as a promising solution for enhancing authentication security in the IoMT in recent years. With the advent of quantum computing technology, traditional cryptographic algorithms face the risk of being broken by quantum computers, posing significant threats to the security of sensitive medical data exchanged within IoMT networks. PQC offers cryptographic algorithms that are resistant to attacks from both classical and quantum computers, ensuring long-term security for IoMT systems. By leveraging mathematical problems that are believed to be computationally hard even for quantum computers, such as lattice-based cryptography or code-based cryptography, PQC provides robust security guarantees for authentication mechanisms in IoMT applications. As IoMT devices continue to proliferate and handle increasingly sensitive medical data, the adoption of PQC holds immense promise for safeguarding patient

Aspect	**Classic Cryptography**	**Quantum Cryptography**	**Post-Quantum Cryptography**
Security	Vulnerable to quantum attacks	Offers unconditional security based on quantum principles	Provides long-term security against quantum attacks
Implementation	Well-established and widely understood	Practical implementation challenges due to specialized quantum hardware	Compatible with classical computing infrastructure
Key Exchange	Depends on mathematical algorithms and key distribution	Secure key exchange through quantum properties (QKD)	Secure key exchange using quantum-resistant algorithms
Performance	Efficient encryption and decryption processes	Practical implementation challenges and performance considerations	Performance and efficiency considerations compared to classic algorithms

Table 2.2: Comparison of Classical, Quantum and Post-quantum cryptography approaches

privacy and maintaining the integrity of healthcare systems against emerging threats from quantum computing technologies.

2.6 Conclusion

Cryptographic primitives, including SKC and PKC, play a vital role in ensuring the security and privacy of data transmitted within IoMT. SKC, with its efficient and fast encryption and decryption processes, is commonly utilized for securing communication between devices within the IoMT ecosystem. It ensures the confidentiality and integrity of sensitive medical data exchanged between medical sensors, wearable devices, and healthcare infrastructure. On the other hand, PKC provides a robust mechanism for authentication and secure key exchange in IoMT environments. Public-key infrastructure (PKI) enables devices to authenticate each other and establish secure communication channels without the need for pre-shared secrets. This is particularly crucial in IoMT, where devices may join or leave the network dynamically, and maintaining secure communication channels is essential. Furthermore, public-key cryptography facilitates the implementation of digital signatures and non-repudiation mechanisms, ensuring the authenticity of transmitted medical data and preventing unauthorized alterations. Overall, cryptographic primitives are fundamental in IoMT to protect patient privacy, ensure data integrity, and establish secure communication channels, thereby fostering trust and reliability in healthcare systems.

PQC emerges as a promising solution to address the evolving security landscape within the IoMT. With recent advancements in quantum computing posing potential threats to tradi-

tional cryptographic algorithms used in IoMT, the adoption of PQC offers several advantages. PQC provides cryptographic algorithms that are resistant to attacks from quantum computers, ensuring the long-term security of sensitive healthcare data in IoMT environments. Moreover, PQC solutions offer better performance and protection against a wide range of attacks faced by both SKC and PKC. By integrating PQC into IoMT systems, healthcare organizations can enhance security measures and mitigate the risks associated with emerging threats, thereby safeguarding patient privacy and data integrity effectively.

CHAPTER 3:

Authentication protocols for IoMT: State of art

Chapter 3

Authentication protocols for IoMT: State of art

3.1 Introduction

A secure WBAN-based IoMT application needs to address privacy, confidentiality, integrity, and authentication. However, implementing these security measures encounters challenges due to the limited energy and infrastructure of WBAN systems. Authentication holds paramount importance in interconnected device networks. Nonetheless, WBAN users often lack security expertise, necessitating user-friendly authentication processes with seamless transparency [101]. Authentication schemes in WBANs play a crucial role in fulfilling privacy and security requirements. However, the constrained capabilities of WBAN devices introduce stability and performance issues during the deployment of these schemes. The primary challenge arises from the utilization of traditional cryptographic primitives such as ECC-based and RSA cryptosystems for authentication security. This dependence imposes significant computational overhead on the devices, leading to excessive energy consumption [1].

Current authentication schemes rely on cryptographic primitives to maintain security services, primarily focusing on authentication and confidentiality. These schemes utilize key primitives like encryption (ECC and PBC), digital signatures, and hash functions to ensure information security, reduce the trust required among involved entities, and mitigate security breaches in scenarios where these services may be unavailable.

In this chapter, we will examine the current authentication schemes designed for WBAN-based IoMT applications, providing an overview of their key features. Additionally, we will present different taxonomies to classify these existing schemes. All of these measures we have conducted in our research papers [102, 1].

3.2 Literature review

Numerous proposals have emerged to enhance security in WBANs, particularly within medical contexts involving sensor networks. These security mechanisms can be broadly categorized into cryptographic and non-cryptographic authentication methods.

This section focuses on cryptographic schemes chosen for their relevance in medical settings within sensor network architectures. Many of these schemes leverage cryptographic tools to offer security services like authentication, confidentiality, and integrity.

In 2012, Kumar et al. [103] introduced a sensor-centric WBAN architecture, which was later criticized by He et al. [104], who proposed an improved version. Subsequently, Wu et al. [105] addressed vulnerabilities in He et al.'s work, focusing on mitigating various types of attacks.

Chen et al. [106] and Chen et al. [107] introduced cloud-assisted data exchange and a secure authentication framework for cloud-based healthcare, respectively. However, Chiou et al. [108] identified shortcomings in Chen et al.'s framework, leading to the development of an enhanced key agreement framework by Mohit et al. [109].

Srinivas et al. [110] detected security flaws in Wu et al.'s work [105] and proposed their symmetric key-based authentication scheme. Meanwhile, Wazid et al. [111] addressed privacy and security concerns, and Li et al. [112] tackled flaws in He et al.'s scheme [104]. Das et al. [113] developed a new scheme building upon previous work, highlighting vulnerabilities in both.

Mao et al. [114] introduced a trusted authority-guided authentication scheme. Liu and Chung [115] proposed user authentication using bilinear pairing, later criticized by Challa et al. [116], who introduced an ECC-based authentication scheme, further improved by Soni et al. [117]. Ali et al. [118] criticized both approaches, with Xu et al. [119] improving Soni et al.'s work.

Amin et al. [120] designed an authentication scheme for mobile devices, but Jiang et al. [121] identified security drawbacks. Ali et al. [122] later improved Amin et al.'s scheme. Ever et al. [123] proposed a scheme to enhance healthcare infrastructure security.

In 2018, Wazid et al. [124] introduced a user-based authentication scheme involving the cloud. Sharma et al. [125] proposed an authentication scheme for remote patient monitoring, later improved by Alzahrani et al. [126]. Liu et al. [127] introduced a robust authentication scheme with dynamic passwords, and Aghili et al. [128] proposed a lightweight scheme.

Chandrakar et al. [129] presented a cloud-guided authentication framework for healthcare monitoring systems. However, flaws were found by Kumari et al. [130]. Shuai et al. [131] presented a remote patient monitoring authentication scheme using WBANs.

Fotouhi et al. [132] introduced a hash-chain-based authentication scheme for WBAN, criticized by Chen et al. [133] for vulnerabilities, leading to an alternative scheme. Similarly, Masud et al. [134] focused on user anonymity preservation, and Khalid et al. [135] proposed a cloud-based authentication scheme.

Recently, Delgado et al. [136] devised a cryptographic scheme with keyless sensor authentication, while Lee et al. [137] introduced a scheme to prevent various attacks. Kim et al. [138] introduced a lightweight authentication scheme focusing on preserving anonymity and protecting against replay attacks in healthcare systems.

In 2016, Ibrahim et al. proposed a two-tier WBAN authentication scheme, marking the initial focus on this architecture but without including user authentication [139]. However, later findings revealed vulnerabilities in this approach. Li et al. introduced an authentication and key agreement scheme suitable for WBAN sensor nodes, considering node anonymity and two-hop centralized WBAN architecture [140].

Subsequently, Almuhaideb and Alqudaihi addressed the lack of node anonymity, key man-

agement, and size in existing schemes by proposing a new authentication scheme consisting of two protocols for authentication and re-authentication [141]. Similarly, Gupta et al. presented a scheme focusing on security and privacy requirements in WBAN-based healthcare systems, while also reviewing and highlighting flaws in existing schemes [142].

Kompara et al. focused on proposing a new authentication scheme providing anonymity, untraceability, confidentiality, and mutual authentication for sensor nodes [143]. However, subsequent findings revealed vulnerabilities, leading to improvements by Rehman et al. to protect against various cyber-attacks [144].

To address resource-saving needs, Xu et al. introduced a lightweight authentication scheme based on a two-hop centralized architecture, departing from previous resource-intensive methods [145]. Kumar and Chand leveraged the cloud environment to propose an identity-based anonymous authentication and key agreement protocol for WBAN, addressing inherent security challenges [146].

Furthermore, Wan et al. proposed a continuous authentication scheme based on physiological signals to overcome impersonation and sensor node capture attacks [147]. Koya and Deepthi proposed improvements to Li et al.'s scheme using physiological signals, albeit with increased computational costs [148].

3.3 Classification of authentication schemes

Researchers have embraced diverse classification methods to assess the efficacy of authentication schemes and categorize them effectively. In our study, we particularly concentrated on authentication schemes tailored for healthcare WBANs. Figure 3.1 showcases several potential classification approaches utilized in categorizing WBAN authentication schemes.

Meanwhile, Table 3.1 outlines our categorization of surveyed schemes, organized according to three primary criteria: authentication factors, cryptographic primitives, and architecture-based considerations. It's worth mentioning that in the literature, some studies have tackled the entire IoMT environment by presenting various scenarios and multiple schemes within a single work [129, 106, 107, 108, 130, 109].

3.4 Comparison

In this section, we employ two distinct comparison approaches based on architectural classification criteria and security requirements and attacks.

3.4.1 Architectural Comparison

Each of the addressed literature schemes comes with its own set of cryptographic primitives and goals. Below, we outline various studied schemes based on their architectural classification as presented in[1] which is illustrated in 3.2. Also, we present a comparison between the different schemes studied in this chapter according to the following criteria:

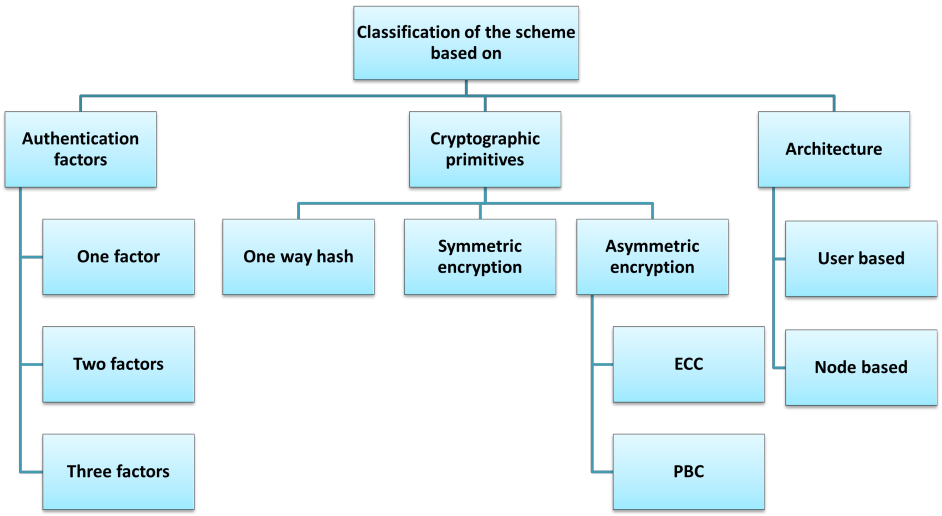


Figure 3.1: Classification of authentication schemes in WBANs

Table 3.1: Classification of the survied schemes

Classification		Scheme
Authentication factor	Two factor	[120] [123] [104] [121] [115] [110] [111] [105] [134]
	Three factor	[128] [122] [118] [126] [116] [113] [112] [127] [114] [125] [131] [117] [124] [119] [135] [149]
Cryptographic primitives	Hash function	[128] [122] [118] [141] [126] [120] [116] [113] [123] [142] [104] [139] [121] [143] [148] [146] [140] [112] [115] [114] [144] [125] [131] [117] [110] [111] [124] [105] [119] [145] [135] [134] [149] [147]
	Symmetric cryptography	[122] [126] [113] [104] [112] [110] [105] [149]
	Asymmetric cryptography	[118] [116] [123] [146] [115] [114] [117] [111] [119] [135] [147]
Architecture	Node authentication schemes	[141] [142] [139] [143] [148] [146] [140] [144] [145] [147]
	User authentication schemes	[128] [122] [118] [126] [120] [116] [113] [123] [104] [121] [112] [115] [127] [114] [125] [131] [117] [110] [111] [124] [105] [119] [135] [134] [149]

- Architecture that was used to design the scheme.
- Cryptographic primitives that were used to achieve a certain security level.
- Goals of each scheme that were the main reason for proposing it.

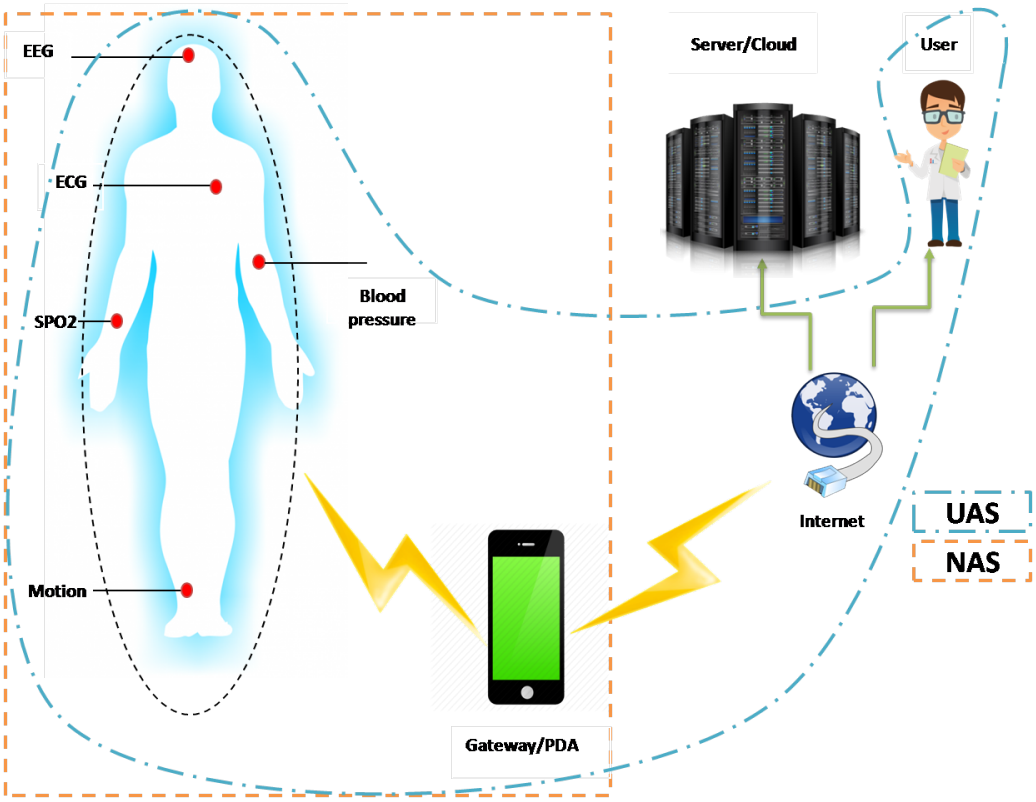


Figure 3.2: NAS and UAS architectures [1]

- Verification tools used to prove the security of the scheme.

User authentication schemes (UAS)

In this classification, we identify three primary system components: the user, gateway node, and sensor node. Authentication occurs mutually between each pair of entities within the scheme: user-gateway, gateway-sensor, and user-sensor, as well as vice versa. Users have the option to authenticate using either a smart card/mobile device or solely a password. However, due to the open and insecure nature of the communication channels between entities, they are susceptible to various attacks. Many researchers have incorporated authentication factors into UAS to enhance security and ensure the legitimacy of users. Authentication factors vary depending on the specific application and preferences of the authors, ranging from one factor (1FA) such as a password, to two factors (2FA) like a password and smart card/mobile device, or even three factors (3FA) which include all mentioned factors plus biometrics. Typically, UAS falls into two main categories: 2FA and 3FA, each aimed at elevating the security level of user authentication. To facilitate the presentation of the surveyed UAS, we have categorized the schemes into two groups: UAS with 2FA and UAS with 3FA.

- **UAS with two-factor authentication**: Here we compared all the studied UAS that rely on 2FA based on their goals that lead to developing the scheme, cryptographic primitives, and verification tools. Table 3.2 represents summary of UAS with two-factor authentication.

- **UAS with three-factor authentication**: Table 3.3 presents the main goals of each 3AF UAS scheme and the crypto-primitives that were used in its design.

Table 3.2: Summary of UAS with 2FA

Scheme	Year	Method	Goal	Tools
He et al. [104]	2015	Symmetric encryption, Hash	• Lightweight scheme • Improving the flaws of [103]	BAN-Logic
Wu et al. [105]	2017	Symmetric Encryption, Hash	• Improving the flaws of [104]	Proverif
Wazid et al. [111]	2017	ECC, Hash	• Preventing leakage of health data • Mutual secure authentication	AVISPA
Liu and Chung [115]	2017	Bilinear pairing+Hash	• Establishing secure communication between a user and a sensor node	
Srinivas et al. [110]	2017	Symmetric Encryption, hash	• Ensuring privacy • Ensure secure and authorised communication • Overcoming the flaws of [105]	AVISPA
Jiang et al. [121]	2017	Quadratic residues, Fuzzy verifiers, Hash	• End-to-end mutual authentication • Overcoming the flaws of [120]	
Amin et al. [120]	2018	Hash	• Minimising the transmission distance • Saving more power consumption • Session key negotiation protocol	AVISPA, BAN-Logic
Masud et al. [134]	2021	Hash	• Preserving the anonymity of users • Permitting the registered and verified users to access the medical networks through secure sessions	AVISPA

Table 3.3: Summary of UAS with 3FA

Scheme	Year	Method	Goals	Tools
Li et al. [112]	2016	Symmetric Encryption, Hash, Bio Hash	• Overcoming the flaws in[104] • A new wrong password detection mechanism	AVISPA, BAN-Logic
Das et al. [113]	2017	Symmetric Encryption, Hash, Bio Hash	• Overcoming the flaws in [104, 112] • Enhancing the security of [112]	AVISPA, BAN-Logic
Ever et al. [123]	2018	ECC, Symmetric Encryption, Hash	• Protecting healthcare infrastructures • Minimizing overheads	AVISPA, ROM
Challa et al. [116]	2018	ECC, Hash, Bio Hash	• Overcoming the flaws found in [115] • Adopting a low bio-hash function • Providing a lightweight three factor authentication	AVISPA, BAN-Logic, ROR
Wazid et al. [124]	2018	Hash, Bio Hash	• Using the could in the authentication • Reducing the overheads by adopting cloud • Providing essential management process for secret keys establishment	ROR
Mao et al. [114]	2018	ECC, Hash, Fuzzy verifier	• Overcoming the flaws found in [111] • Introducing the fuzzy verifier to prevent offline guessing attacks • Secure local login • Secure biometric template	ROM, ROR
Ali et al. [122]	2018	Symmetric encryption, Hash	• Overcoming the flaws found in [120]	AVISPA, BAN-Logic

Table 3.3: Summary of UAS with 3FA (Continued)

Scheme	Year	Method	Goals	Tools
Liu et al. [127]	2019	Hash, fuzzy extractor	• Providing a lightweight scheme • Dynamicity and randomness based approaches • Dynamic secure passwords • Continuously updated pseudo identities	AVISPA, BAN-Logic
Sharma et al. [125]	2019	Hash	• Providing a lightweight scheme • Adopting mobiles in the authentication process	AVISPA
Soni et al. [117]	2019	ECC, Hash	• Overcoming the flaws found in [116] • New secure mechanism for developing a three-factor authentication • Providing support for revocation and re-registration of users	AVISPA, BAN-Logic
Aghili et al. [128]	2019	Hash	• Overcoming the flaws found in [150] • Providing access control liability for users • Considering ownership transfer possibility	Proverif
Shuai et al. [131]	2019	Hash	• Providing protection against forward secrecy and desynchronisation • Providing a low cost scheme • Pseudo-identities to achive anonymity	BAN-Logic
Ali et al. [118]	2020	ECC, Hash	• Overcoming the found flaws in [116, 115] • Providing a suitable lightweight scheme for WMSNs	AVISPA, BAN-Logic

Table 3.3: Summary of UAS with 3FA (Continued)

Scheme	Year	Method	Goals	Tools
Xu et al. [119]	2020	Chebyshev, Hash	• Securing the session establishement using Rabin cryptosystem and chaotic maps • Overcoming the flaws found in [117] • Reducing the costs in [117]	BAN-Logic, ROM
Alzahrani et al. [126]	2020	Symmetric Encryption, Hash, Bio Hash	• Overcoming the flaws found in [125] • Adopting a cloud based environment	BAN-Logic, ROM, Proverif
Khalid et al. [135]	2021	ECC, Hash	• Adopting cloud environment • Providing a scheme that supports multi-server environments • Protection against the well-known attacks	BAN-Logic
Shadi Nashwan [149]	2021	Symmetric Encryption, Hash	• Providing simultaneous anonymity • Providing perfect forward secrecy services	BAN-Logic

Node authentication schemes (NAS)

In this category, the user does not play a central role; instead, the primary participants are gateway nodes and sensor nodes. Mutual authentication occurs between various pairs of entities, including gateway-gateway, gateway-sensor, sensor-gateway, and sensor-sensor, depending on the architecture's number of hops. Communication among these participants is considered insecure, leaving them vulnerable to various attacks. This classification may encompass different types of sensor nodes and gateways, with sensors also being able to authenticate with each other. For instance, authentication may be required between controller sensor nodes (super-nodes that facilitate communication with various types of WBAN implants/wearables and collect or receive data from them) and sensor nodes (the implantable or wearable WBAN devices). Below, we provide descriptions of the surveyed schemes falling within this classification.

Table3.4 presents the main goals of each NAS scheme and the crypto-primitives that were used in its design.

Table 3.4: Summary of the studied NAS

Scheme	Year	Method	Goals	Tools
Ibrahim et al. [139]	2016	Hash	• Two-tier WBAN authentication • Providing a lightweight scheme	BAN-Logic
Li et al. [140]	2017	Hash	• Providing a lightweight scheme • Preserving node anonymity	AVISPA, BAN-Logic
Koya & Deepthi [148]	2018	Hash	• Overcoming the flaws found in [140] • Using physiological signals to provide extra security features	AVISPA, BAN-Logic
Xu et al. [145]	2019	Hash	• Saving the resources in WBAN • Two-hop centralised architecture • Providing a lightweight scheme	Proverif
Kompara et al. [143]	2019	Hash	• Overcoming the flaws found in [140] • Providing nodes anonymity and untraceability • Providing a lows cost scheme	AVISPA, BAN-Logic, Scyther
Gupta et al. [142]	2020	Hash	• Overcoming the flaws found in [140] • Providing a lightweight scheme	AVISPA, BAN-Logic, ROR
Kumar and Chand [146]	2020	ECC	• Adopting the cloud environment to facilitate the storage and computation	ROM
Rehman et al. [144]	2020	Hash	• Overcoming the flaws in [143] • Protecting against base station compromise attack and sensor node impersonation attack • Providing a low cost scheme	AVISPA, BAN-Logic

Table 3.4: Summary of the studied NAS (Continued)

Scheme	Year	Method	Goals	Tools
Almuhaideb & Alqudaihi [141]	2020	Hash	• Providing nodes anonymity • Key management, and size	BAN-Logic
Wan et al. [147]	2021	ECC, Hash	• Continuous authentication scheme • Protecting against impersonation and sensor node capture attacks • Using physiological signals that are hard to imitate	BAN-Logic
Rehman et al. [151]	2021	Hash	• Improving the previous work[144] • Combining physiological signs and lightweight cryptographic primitives for extra protection	AVISPA, BAN-Logic

3.4.2 Security and privacy comparison

Each of the discussed literature schemes has successfully met privacy requirements and mitigated various attacks. However, they may fall short in certain aspects. Below, we outline several studied schemes based on their privacy and security requirements. Additionally, we provide a comparison between the different schemes studied in this chapter according to different security requirements and attacks.

Table 3.5 presents various attacks and identified failures in the surveyed schemes. These attacks were identified by other researchers who proposed improvements or new schemes (see the "Ref." column). A blank cell in the "Ref." column indicates that no work has identified flaws in that particular scheme. Notably, none of the schemes succeeded in ensuring or proving all security and privacy requirements. Below, we discuss the observed results, their underlying reasons, and offer important recommendations.

- Several surveyed schemes fail to preserve anonymity and compromise process integrity, as evidenced by [143, 148, 125, 134]. To address this, it's crucial to: 1) Avoid passing IDs in plaintext over insecure channels, 2) Utilize the collision-resistant property of one-way hash functions for ID transmission when necessary (e.g., as demonstrated in [131]), 3) Employ pseudo-random IDs for authentication.

- A notable presence of replay attacks is observed in schemes such as [143, 113]. Countermeasures for this attack include using random numbers and timestamps.

- Many surveyed schemes are vulnerable to impersonation attacks, where adversaries can impersonate communication parties (nodes, users, gateways). Causes for this vulnerability include: - Theft of secret user information and node identity, emphasizing the need for anonymous communication parties. - Replay attacks enabling adversaries to replay communications between parties undetected, leading to false assumptions about direct communication.

  Countermeasures include: - Continued use of access control lists (ACLs) focusing on MAC addresses. - Generation of bio-keys to mitigate IoT sensor node impersonation attacks [151, 144, 147]. - Authentication factor combinations like passwords, smart cards, and biometrics [126, 116]. - Adoption of techniques to protect against replay attacks and preserve anonymity.

- Some schemes are susceptible to node capture attacks, as seen in [113, 148]. This vulnerability arises from compromised cryptographic keys exposed by adversaries. Mitigations include regular updates of keys used for securing communication in WMSNs, detection mechanisms for cloned nodes, and detection of compromised keys.

- Notably, the table indicates the prevalence of guessing attacks, particularly on the node side, where adversaries attempt to recover critical data. To mitigate such attacks, robust security mechanisms are essential.

Table 3.5: Security analysis of the surveyed schemes

Scheme	Class	FA	FT	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	Ref
Ibrahim et al. [139]	NAS		1	Y	Y	Y	-	Y	N	Y	N	Y	-	-	-	N	[148]
Li et al. [140]	NAS		2	N	Y	N	-	N	Y	N	N	N	N	-	Y	Y	[142] [141]
Koya & Deepthi [148]	NAS		2	N	N	N	-	Y	Y	N	Y	N	N	-	-	Y	[143] [145]
Xu et al. [145]	NAS		1	N	-	N	-	N	Y	N	N	N	N	-	-	N	[152] [141]
Kompara et al. [143]	NAS		3	N	Y	N	-	Y	-	Y	N	N	-	-	-	-	[142] [144]
Gupta et al. [142]	NAS		3	Y	Y	Y	-	Y	-	Y	Y	Y	N	-	Y	-	[141]
Kumar and Chand [146]	NAS		1	Y	N	N	-	N	-	-	Y	-	-	-	-	Y	[153]
Rehman et al. [144]	NAS		2	Y	Y	Y	-	Y	N	Y	Y	-	-	-	-	-	[151]
Almuhaideb et al. [141]	NAS		1	Y	Y	-	-	-	-	Y	Y	-	Y	-	-	-	
Wan et al. [147]	NAS		1	Y	Y	-	-	Y	-	Y	Y	Y	-	-	-	-	
Rehman et al. [151]	NAS		2	Y	Y	Y	-	Y	Y	Y	Y	-	-	-	-	-	
He et al. [104]	UAS	2	1	Y	-	-	-	N	-	-	N	N	N	Y	Y	Y	[112] [105]
Li et al. [112]	UAS	3	2	N	-	-	N	N	-	Y	N	N	Y	Y	N	Y	[113]
Wu et al. [105]	UAS	2	1	Y	-	-	N	N	Y	-	N	Y	N	N	Y	-	[110]
Wazid et al. [111]	UAS	2	1	Y	Y	Y	Y	N	-	Y	N	Y	N	Y	Y	Y	[114]
Das et al. [113]	UAS	3	2	Y	N	-	N	N	N	N	N	-	N	Y	Y	Y	[154]
Liu and Chung [115]	UAS	2		N	-	-	-	N	-	Y	N	-	N	N	N	Y	[116]
Srinivas et al. [110]	UAS	2	1	Y	N	-	Y	N	-	Y	Y	N	Y	Y	Y	N	[123]
Jiang et al. [121]	UAS	2		Y	Y	Y	N	Y	Y	Y	Y	-	-	Y	N	-	[155]
Ever et al. [123]	UAS	2	2	Y	Y	-	-	Y	-	Y	Y	Y	Y	Y	Y	Y	
Amin et al. [120]	UAS	2	2	N	Y	Y	N	Y	N	Y	Y	-	Y	N	N	N	[156] [121]
Challa et al. [116]	UAS	3	3	N	N	-	Y	N	-	Y	Y	N	N	Y	Y	-	[117] [118]
Wazid et al. [124]	UAS	3	1	Y	-	Y	Y	Y	-	Y	Y	-	Y	-	Y	-	
Mao et al. [114]	UAS	3	2	Y	Y	Y	Y	Y	-	Y	-	N	Y	Y	N	Y	[127]
Ali et al. [122]	UAS	3	2	Y	N	Y	-	-	N	Y	Y	Y	N	Y	N	-	[157]
Liu et al. [127]	UAS	3	2	Y	-	Y	-	-	-	Y	Y	Y	Y	Y	Y	-	
Sharma et al. [125]	UAS	3	1	N	Y	Y	Y	N	-	Y	N	-	N	N	Y	Y	[126]
Soni et al. [117]	UAS	3	2	Y	N	Y	Y	Y	-	Y	Y	N	Y	Y	Y	-	[119]
Aghili et al. [128]	UAS	3	1	Y	N	Y	Y	-	N	Y	N	-	Y	Y	Y	-	[158]
Shuai et al. [131]	UAS	3	1	Y	Y	-	-	-	Y	Y	Y	-	N	Y	N	Y	[157]
Xu et al. [119]	UAS	3	2	Y	Y	-	-	Y	Y	Y	-	Y	Y	-	Y	-	
Alzahrani et al. [126]	UAS	3	3	Y	Y	Y	-	Y	-	Y	Y	-	Y	Y	Y	Y	
Ali et al. [118]	UAS	3	2	Y	-	-	Y	Y	-	Y	Y	-	Y	Y	Y	-	
Masud et al. [134]	UAS	2	1	N	Y	Y	Y	Y	N	Y	N	-	N	-	N	-	[159]
Khalid et al. [135]	UAS	3	1	Y	Y	-	-	Y	-	Y	Y	-	Y	Y	Y	Y	
Shadi Nashwan [149]	UAS	3	1	Y	Y	Y	-	Y	Y	Y	Y	-	Y	Y	-	Y	

FA: Authentication factors, 2/3 FT: Number of security verification techniques used

A1: Achieve anonymity of communication parties, A2: Achieve perfect forward secrecy, A3: Achieve untraceability, A4: Resist DoS attack

A5: Resist MITM attack, A6: Resist desynchronization attack, A7: Resist replay attack, A8: Resist impersonation attack A9: Sensor node capture

A10: Resist guessing attacks, A11: Resist smart card/mobile stolen A12: Resist insider attack, A13: Resist stolen verifier attack

In summary, insider, password guessing, replay, impersonation, node capture, and smart card loss attacks are among the most common risks in authentication schemes identified in the surveyed literature. Many of these attacks cannot be formally verified.

3.4.3 Performance comparison

This section provides an assessment of the performance of the analyzed schemes across four key metrics: computational cost, communication cost, storage overhead, and energy consumption.

Table 5.3 displays the cryptographic primitives utilized in the surveyed schemes, along with their respective computational times and energy consumption, as observed in [1]. Additionally, the lengths of various primitives and data are provided as follows:

- L_{ID}: Length of ID is 8 bytes.
- L: Length of the hash function, symmetric key, the modulus operation result and the nonce are 32 bytes.
- L_{ECC}: Length of ECC point is 40 bytes.
- L_{TS}: Length of timestamp is 4 bytes.
- L_{SES}: Length of session number is 4 bytes.

Table 3.6: Experimental results of cryptographic primitives in sensors

Operation	Notation	Computational time (Second)	Energy consumption (mJ)
Hash function (SHA-256)	T_H	0.013	0.086
Symmetric decryption (AES-256)	T_S	0.015	0.099
Scalar point multiplication (160 bits)	T_{ECM}	1.049	6.923
ECC Addition (160 bits)	T_{ECA}	0.007	0.046
Bilinear pairing operation	T_{pair}	8.142	53.74

Table 3.7 illustrates a theoretical comparison of the performance of the surveyed schemes. The data presented in this table will serve as the basis for calculating various costs.

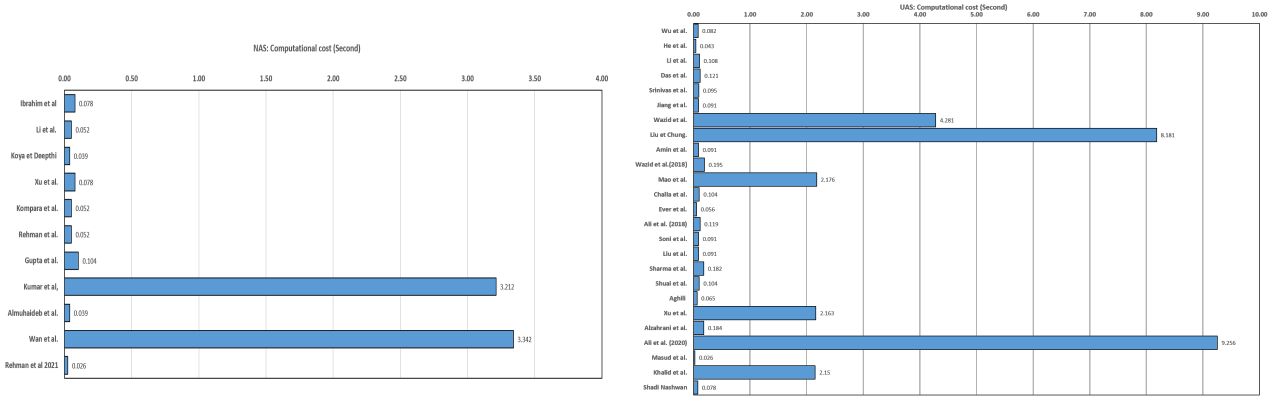
The costs comparison for the surveyed schemes using the metrics and simulations presented in our paper [1] can be seen in Figures 3.3, 3.4, 3.5 and 3.6 .

Here, we present the calculated costs for various aspects of the studied schemes:

- **Computational Cost**: Figures 3.3 (a-b) depict the computational cost (in seconds) of the studied schemes for both NAS and UAS classes on the sensor side. Notably, Rehman et al.'s scheme [151] requires only 0.026 seconds for NAS class, while Masud et al.'s scheme [134] requires the same for UAS class. These results demonstrate significantly lower computational costs compared to other schemes. For instance, Wan et al.'s scheme [147] takes 3.342 seconds for NAS, and Ali et al. [118] and Liu et Chang [115] schemes take 9.256 seconds and 8.181 seconds, respectively, for UAS class.

Table 3.7: Theoretical evaluation of the surveyed schemes

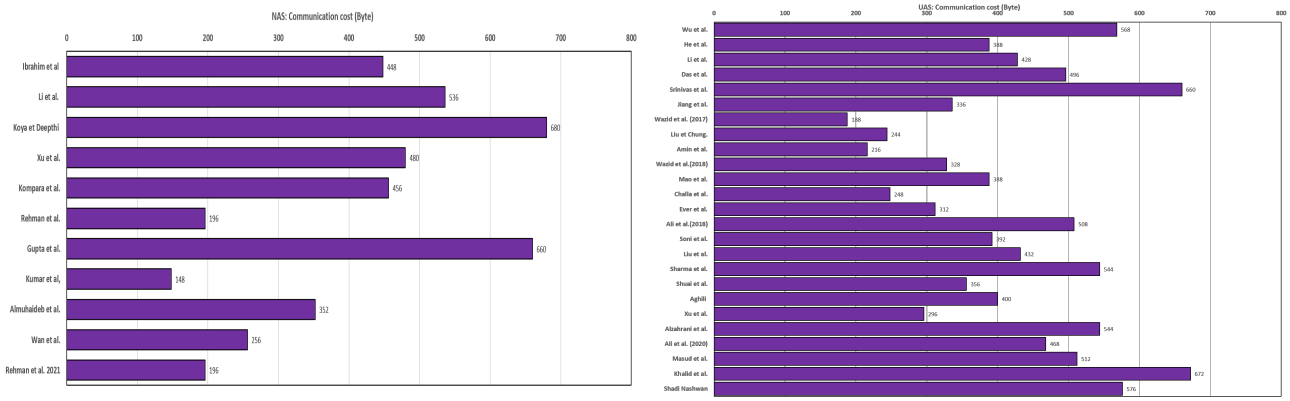
Scheme	Class	Computational cost	Communication cost	Storage cost
Ibrahim et al. [139]	NAS	$6T_H$	14L	$2L+L_{ID}$
Li et al. [140]	NAS	$4T_H$	$2L_{ID}+16L+2L_{TS}$	$L_{ID}+2L$
Koya & Deepthi [148]	NAS	$3T_H$	$21L+3L_{TS}$	$L_{ID}+2L$
Xu et al. [145]	NAS	$6T_H$	$2L_{ID}+14L+4\ L_{TS}$	$L_{ID}+3L$
Kompara et al. [143]	NAS	$4T_H$	$14L+2L_{TS}$	$2L+L_{ID}$
Rehman et al. [144]	NAS	$4T_H$	$6L+1L_{TS}$	$3L+L_{ID}$
Gupta et al. [142]	NAS	$8T_H$	$20L+5L_{TS}$	$L_{ID}+4L$
Kumar et al. [146]	NAS	$5T_H+3T_{ECM}$	$2L_{ECC}+2L+L_{TS}$	$LID+2L_{ECC}$
Almuhaideb & Alqudaihi [141]	NAS	$3T_H$	$10L+4L_{TS}+\ 2_{ID}$	$3L_{ID}+2L+L_{SES}$
Wan et al. [147]	NAS	$15T_H+3T_{ECM}$	$3L_{ECC}+4L+2L_{TS}$	$3L+L_{ECC}$
Rehman et al. [151]	NAS	$2T_H$	$6L+1L_{TS}$	$3L+L_{ID}$
He et al. [104]	UAS	$T_H+2\ T_S$	$10L_{ID}+9L+5L_{TS}$	$L_{ID}+L$
Li et al. [112]	UAS	$6T_H+2\ T_S$	$10L_{ID}+10L+7\ L_{TS}$	$L_{ID}+L$
Wu et al. [105]	UAS	$2T_S+4\ T_H$	$7L_{ID}+16L$	$L_{ID}+L$
Das et al. [113]	UAS	$7T_H+2\ T_S$	$11L_{ID}+12L+6L_{TS}$	$L_{ID}+L$
Srinivas et al. [110]	UAS	$5T_H+2$ TS	$9L_{ID}+18L+3L_{TS}$	$L_{ID}+2L$
Jiang et al. [121]	UAS	$7T_H$	$L_{ID}+10L+2\ L_{TS}$	$L_{ID}+2L$
Wazid et al. [111]	UAS	$6T_H+4T_{ECM}+1T_{ECA}$	$2L_{ECC}+3L+3L_{TS}$	$3L+L_{ECC}$
Liu et Chung [115]	UAS	$3T_H+1T_{pair}$	$2L_{ECC}+4L+\ 3L_{ID}+3L_{TS}$	$2L_{ECC}+L$
Amin et al. [120]	UAS	$7\ T_H$	$2L_{ID}+12L$	$L_{ID}+2L$
Wazid et al. [124]	UAS	$15T_H$	$10L+3\ L_{TS}$	$3L+L_{ECC}$
Mao et al. [114]	UAS	$6T_H+2T_{ECM}$	$3L_{ECC}+8L+3\ L_{TS}$	$L_{ID}+L+2L_{ECC}$
Challa et al. [116]	UAS	$8T_H$	$L_{ECC}+6L+4\ L_{TS}$	$L_{ID}+L$
Ever et al. [123]	UAS	$2T_H+2T_S$	$7L_{ID}+8L$	$L_{ID}+L$
Ali et al. [122]	UAS	$8T_H+T_S$	$14L+6L_{ID}+3L_{TS}$	$2L+L_{ID}$
Soni et al. [117]	UAS	$7T_H$	$9L+2L_{ECC}+6\ L_{TS}$	$L_{ID}+2L$
Liu et al. [127]	UAS	$7T_H$	$13L+4\ L_{TS}$	$L_{ID}+2L$
Sharma et al. [125]	UAS	$14T_H$	$L_{ID}+16L+6\ L_{TS}$	$L_{ID}+2L$
Shuai et al. [131]	UAS	$8T_H$	$11L+L_{TS}$	$2L+L_{ID}$
Aghili et al. [128]	UAS	$5T_H$	$12L+4L_{TS}$	$L_{ID}+L$
Xu et al. [119]	UAS	$5T_H+2T_{cheb}$	$9L+2L_{TS}$	$L_{ID}+L$
Alzahrani et al. [126]	UAS	$13T_H+T_S$	$L_{ID}+16L+6\ L_{TS}$	$2L+L_{ID}$
Ali et al. [118]	UAS	$5T_H+T_{pair}+T_{ECM}$	$4L_{ECC}+2L_{ID}+9L+L_{TS}$	$L_{ID}+2L_{ECC}$
Masud et al. [134]	UAS	$2T_H$	16L	$3L+L_{ID}$
Khalid et al. [135]	UAS	$4T_H+2T_{ECM}$	$16L+4L_{ECC}$	$2L+\ L_{ECC}$
Shadi Nashwan [149]	UAS	$6T_H$	$4L_{ID}\ +\ 17L$	$2L+L_{ID}$



(a) (b)

Figure 3.3: Sensor computation cost of NAS and UAS

- **Communication Cost**: Figure 3.4 (a-b) illustrates the communication cost of the studied schemes for both NAS and UAS classes. Comparison in Figure 3.4a highlights Kumar and Chand's scheme [146] offering better performance in communication cost for NAS class. Meanwhile, in Figure 3.4b, Wazid et al.'s scheme [111] demonstrates the lowest overhead, while Khalid et al. [135] show the highest for NAS.

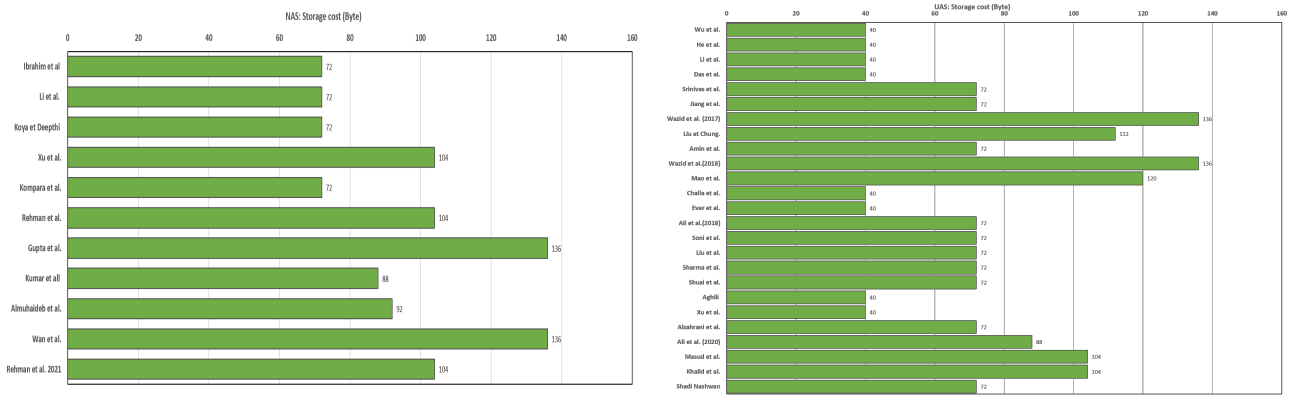


(a) (b)

Figure 3.4: NAS and UAS Communication cost

- **Storage Cost**: Figure 3.5 (a-b) displays the memory space required by the sensor in the studied schemes for both UAS and NAS. Several schemes share the same storage cost, such as [139, 143, 148, 140] requiring 72 Bytes for NAS, and [128, 116, 113, 123, 104, 112, 105, 119] requiring 40 Bytes for UAS. This efficient storage allocation is crucial for sensor devices constrained by storage capacity.

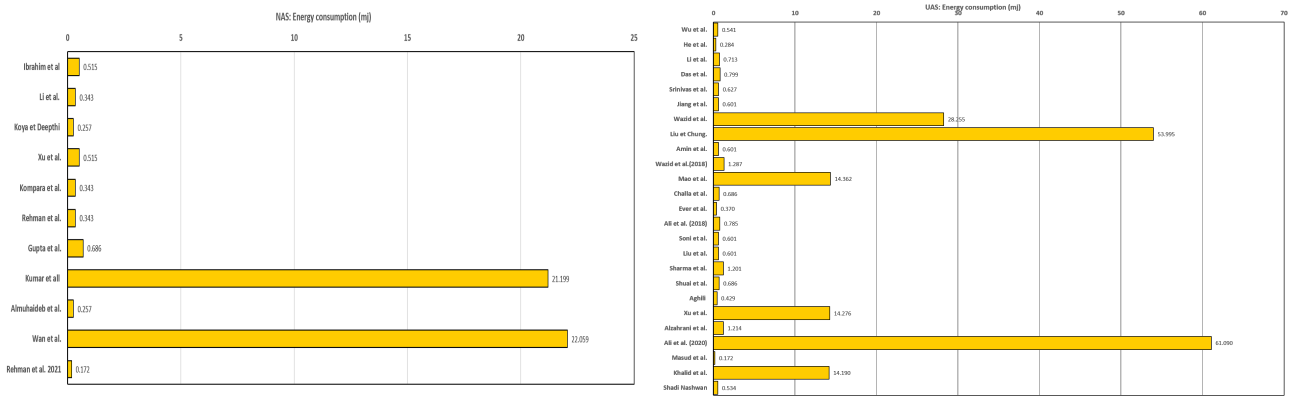
- **Energy Consumption Cost**: Figure 3.6 (a-b) shows the energy consumption in the sensor node for the studied schemes. Energy consumption estimation is based on the equation $W = V \times I \times t$, where W, V, I, and t denote the consumption power in millijoules (mJ), voltage in volts (V), current draw in active mode in milliamps (mA), and time in seconds (s), respectively [160]. According to the WiSMote platform, the current draw is 2.2 mA, and the supply voltage is 3V.



(a) (b)

Figure 3.5: NAS and UAS storage cost

Comparison in Figure 3.6a reveals Wan et al.'s [147] scheme consumes more energy than others, with Rehman et al.'s scheme [151] being the lowest (0.172mJ) in NAS class. Additionally, comparison between UAS-schemes in Figure 3.6b indicates [118, 115, 114, 111, 119] require more energy consumption, while Masud et al.'s scheme [134] requires less (0.172mJ).



(a) (b)

Figure 3.6: UAS and NAS Energy cost

3.5 Conclusion

In this chapter, we conducted a survey and analysis of WBAN authentication schemes recently proposed in the literature, aiming to enhance security in WBANs. Additionally, we compared the studied schemes based on various criteria.

In the following chapters, we will introduce our proposed methods aimed at enhancing the security and performance of WBANs. These methods will take into account the advantages and limitations observed in the related works we have reviewed.

CHAPTER 4:

QR-AKAF: Quantum resistant framework for IoMT

QR-AKAF: Quantum resistant framework for IoMT

Chapter Overview: This chapter introduces a novel security framework utilizing the well-known post-quantum cryptographic (PQC) algorithm Kyber to ensure secure data communication. Named QR-AKAF, this framework adopts a multi-constrained criteria approach, combining various cryptographic primitives to establish shared keys, encrypt sensed data, and compute session key values.

4.1 Introduction

In recent years, the emergence of post-quantum cryptography has marked a significant advancement in the field, providing compelling solutions in contrast to older cryptosystems like RSA, PBC, and ECC. Traditional algorithms, while effective in the past, are now facing challenges from the rapid development of quantum computing, prompting the need for more resilient solutions [161]. Post-quantum cryptography offers algorithms and protocols specifically designed to withstand attacks from powerful quantum computers, ensuring the enduring security of encrypted data.

Post-quantum cryptography presents a more efficient alternative to traditional methods, reducing computational and energy costs while maintaining strong security against quantum threats [162]. As quantum computing advances, the importance of efficient cryptography grows, enabling secure and energy-conscious encryption of sensitive data. These new systems offer promising solutions for WBAN authentication, improving security efficiency and addressing performance issues.

Kyber, distinguished as a finalist among post-quantum cryptosystems by the National Institute of Standards and Technology (NIST) [163], emerges as a potential replacement for traditional cryptosystems. This chapter aims to emphasize the significance of Kyber in this context, particularly in our WBAN authentication framework. We utilize the robustness and security of the Kyber post-quantum cryptosystem to enhance authentication within WBANs.

Using kyber we have introduced a new authentication framework for WBAN-based healthcare systems in [164]. this framework will be introduced in detail in this chapter.

4.2 MLWE-based scheme

The Learning with Errors (LWE) problem, originally proposed by Regev [165], serves as a cornerstone lattice problem extensively employed in developing efficient lattice-based post-quantum cryptographic schemes. Regev [165] introduced a novel approach that reduces complex worst-case lattice problems like GAPSVP and SIVP to LWE problems, providing evidence that solving LWE implies a quantum algorithm's capability to solve GAPSVP and SIVP.

The LWE problem entails solving a linear system where an unknown vector with small errors is introduced. While Gaussian elimination could easily solve this system in the absence of errors, the presence of these unknown errors makes the problem challenging to resolve, as discussed in [166]. Formally, LWE is defined as follows:

Given a secret vector s and a vector a, both randomly chosen from $\mathbb{Z}_q^n$, and an error e sampled from a distribution D, we define the following problems:

4.2.1 Search LWE

Definition 4.2.1 (Search LWE) *Given a collection of m samples, each in the form $(a, < a, s > +e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, the primary objective is to recover the secret vector s from these sample sets.*

4.2.2 Decisional LWE

Definition 4.2.2 (LWE) *When provided with a set of m samples represented as $(a, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, the task is to determine whether these samples conform to the format $(a, < a, s > +e)$ or if they are drawn from a uniform distribution across $\mathbb{Z}_q^n \times \mathbb{Z}_q$.*

4.2.3 Module Learning with Error (MLWE)

Module Learning with Error (MLWE) centers around sampling a vector comprising k polynomials within $\mathbb{R}_q^k$. This vector, termed a "module," has a rank of k. The challenge posed by MLWE is similar to solving module lattice problems. The formal definition for MLWE is as follows:

In the context of MLWE, a secret module element $s \in \mathbb{R}_q^k$ and a module element $a \in \mathbb{R}_q^k$ are considered. The coefficients of each polynomial are uniformly and randomly chosen from $\mathbb{Z}_q$ within $\mathbb{R}_q$. Additionally, an error $e \in \mathbb{R}_q$ with coefficients drawn from a distribution denoted as D is introduced. The ensuing problems are defined as follows:

Definition 4.2.3 (Search MLWE) *Given a set of m samples, each in the form of $(a, a \cdot s + e) \in \mathbb{R}_q^k \times \mathbb{R}_q$, the primary goal is to retrieve the secret value s.*

Definition 4.2.4 (Decisional MLWE) *When provided with a set of m samples represented as $(a, b) \in \mathbb{R}_q^k \times \mathbb{R}_q$, the task is to determine whether all these samples adhere to the format $(a, a \cdot s + e)$ or if they are drawn from a uniform distribution across $\mathbb{R}_q^k \times \mathbb{R}_q$.*

Table 4.1: Comparison of Kyber, RSA, and ECC [171]

Security Level	Encryption (ms)		Decryption (ms)		
	RSA	ECC	RSA	ECC	Kyber
128-bit	1150	70	304	131	6
256-bit	1358	78	369	147	13

4.3 Kyber PKC

Bos et al. introduced Kyber [167, 168] as a lattice-based Key Encapsulation Mechanism (KEM). Kyber utilizes modular lattices due to their effective balance between security and performance considerations. Its security is rooted in the hardness assumptions associated with Module Learning with Errors (MLWE), making it resilient to quantum attacks. A distinguishing characteristic of Kyber is its utilization of polynomial multiplication within a polynomial ring.

The key parameters defining Kyber's characteristics include the degree of the polynomial ring, denoted as n, a prime number q establishing the fundamental ring structure, a positive integer η employed in a binomial distribution, and an integer k where $k{\cdot}n$ signifies the dimension relevant to the corresponding LWE problem [169, 170].

In this section, we explore the Kyber public-key encryption scheme (Kyber-PKE). Kyber.PKE is defined by integers n, k, q, η_1, η_2, d_u, and d_v, where n remains fixed at 256 and q at 3329. It consists of three algorithms: key generation ($KeyGen$), encryption (Enc), and decryption (Dec).

- **KeyGen()**: Initially, Alice generates a random matrix of polynomials $A \in R_q^{k\times k}$. Then, she samples $s \in R_q^k$ and error $e \in R_q^k$ from B_{η_1}. Subsequently, she calculates the vector of polynomials $t = As + e$. Finally, the algorithm returns $(pk = t, sk = s)$.
- **Enc(m,pk)**: Bob generates the matrix $A \leftarrow gen(pk) \in R_q^{k\times k}$. Then, it samples $r \in R_q^k$ from B_{η_1} and samples $e_1 \in R_q^k$ and $e_2 \in R_q$ from B_{η_2}. After that, it calculates two vectors u and v where $u = A^T r + e_1$ and $v = t^T r + e_2 + Decomp_q(m, 1)$. Finally, it returns the ciphertext $c = (c_1, c_2)$ where $c_1 = Comp_q(u, d_u)$ and $c_2 = Comp_q(v, d_v)$.
- **Dec(c,sk)**: Alice recalculates $u := Decomp_q(c_1, d_u)$ and $v := Decomp_q(c_2, d_v)$. Alice finds the plaintext m by calculating $= Comp_q(v - s^T u, 1))$.

Table 4.1 represents a comparison of the encryption and decryption between Kyber and ECC while ensuring the same level of security.

4.4 QR-AKAF: the proposed framework

The proposed framework comprises three primary phases: registration, upload, and login/authentication. Additionally, the scheme includes five distinct types of authentication, each tailored to specific

Table 4.2: Notations and their description.

Notation	Description
CS	Cloud server
TA	Trusted authority
GW	Gateway
U	User
S	Sensor node
$\mathcal{A}$	Adversary
SK_x	Secret key of x
MK	Master Key of Trusted Authority
SK	Session key
PK_x	Public key of x
TS_n	Time stamp n
$\mathcal{A}$	Adversary
$\|\|$	Two inputs concatenated
$\oplus$	xor operator
$h(.)$	One-Way hash function
$Kyber.enc_{PK_x}$	Kyber encryption with the public key of x
$Kyber.dec_{SK_x}$	Kyber decryption with the secret key of x

scenarios. In this section, we will detail the various phases of the proposed scheme and outline the authentication processes for each scenario. Table 4.2 presents all the used notations in this process.

4.4.1 System Architecture

This section outlines the system architecture adopted in our proposed framework. The system consists of five distinct entities: trusted authority (TA), cloud server (CS), user (U), gateway (GW), and sensor. In our framework, all patients (represented by sensors) are required to register with the trusted authority (TA). Similarly, users U register with TA to obtain their pre-shared values. Each patient maintains a personal health record securely stored on a cloud service. Both cloud servers (CS) and gateways (GW) are registered with TA and are provided with pairs of keys used for encrypting health data.

Our framework introduces five schemes tailored to different scenarios in medical environments divided into three different phases. Figure 4.1 illustrates the proposed system architecture. The five authentication schemes are as follows:

- **Upload phase (UP)**: In this phase, the trusted authority authenticates with the cloud server to upload new users' and patients' information for future authentication.
- **Online data access ($OnDA$)**: This scenario involves three entities: sensor, gateway, and user. Users can access real-time data captured by sensors, typical in healthcare applications like Tele-monitoring.
- **Offline data access ($OfDA$)**: Here, users can access stored medical data periodically

captured by sensors and uploaded to the cloud. This scenario includes updating personal health records and prescriptions, relevant for treatments and health record management.

- **Periodic health records** (PHR): Sensors periodically capture and send health data to the cloud server, accessible by professionals (users) later on.
- **Check up** (CU): In this scenario, the patient can review new prescriptions and health condition observations uploaded by doctors using gateways represented by mobile devices and cloud servers.

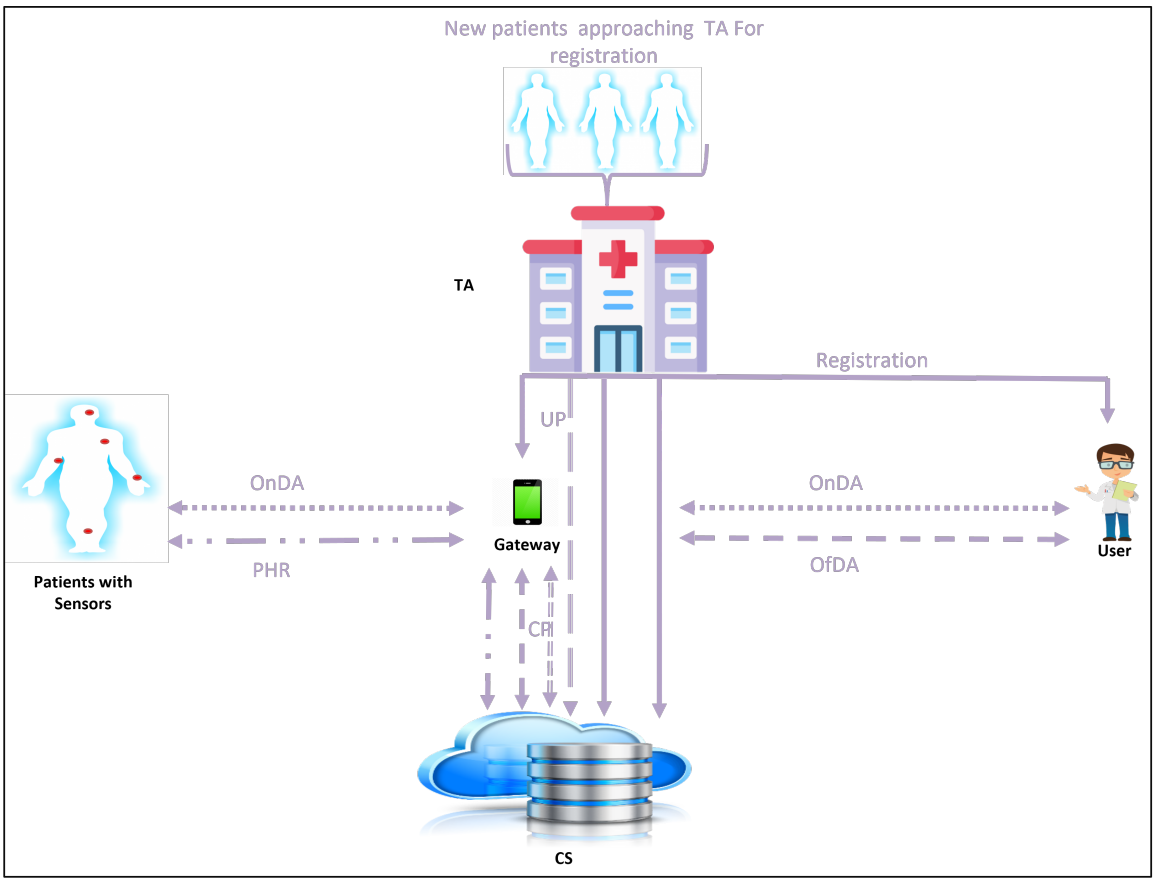


Figure 4.1: The proposed Framework System architecture model

Registration Phase

During the registration phase, system setup parameters are generated via a secure trusted third party known as the trusted authority (TA) or the registration center. In this phase, a master key (MK) is generated for use in registering the Cloud Server (CS), Gateway (GW), User (U), and Sensors (S). Additionally, parameters for the post-quantum cryptographic system Kyber are generated.

Four distinct registrations occur in this phase: Cloud Server (CS) registration, Gateway (GW) registration, User (U) registration, and Sensor (S) registration.

Cloud Server/Gateway Registration

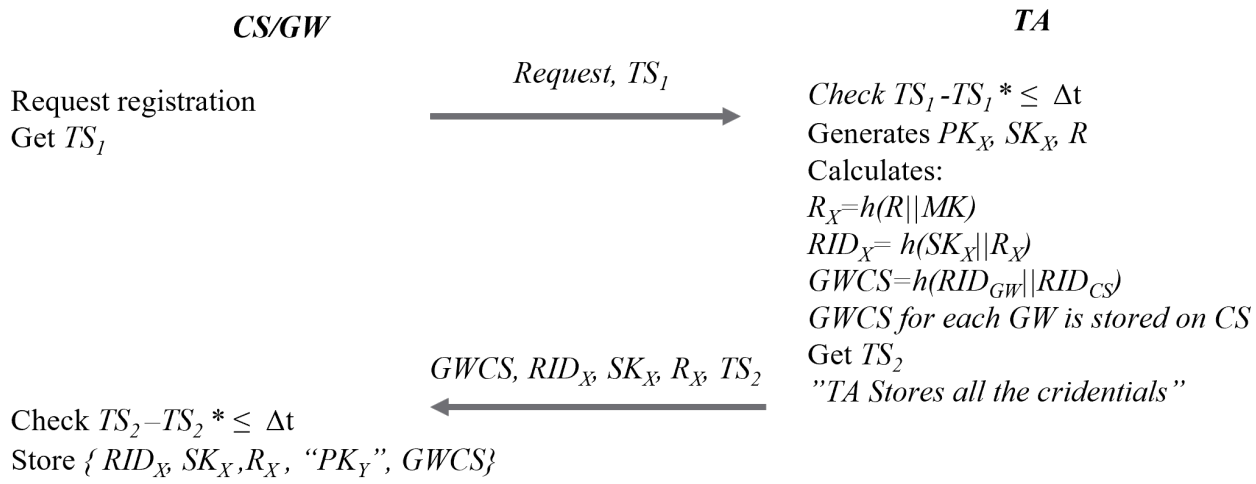


Figure 4.2: Cloud Server/Gateway registration

Both Cloud Server and Gateway follow the same registration steps. During this registration, CS/GW transmits a registration request to TA along with the current timestamp TS_1. The registration phase depicted in Figure 4.2 involves the following steps:

- Entity x transmits a registration request to TA accompanied by the current timestamp TS_1.
- Upon receiving the request, TA verifies the freshness of TS_1. If valid, TA generates a pair of keys (PK_x, SK_x) for entity x, along with a random number R. Subsequently, TA calculates $R_x = h(R||MK)$ and $RID_x = h(SK_x||R_x)$. Additionally, $GWCS = h(RID_{GW}||RID_{CS})$ is calculated and stored on the cloud server for each new GW registration. Finally, TA sends SK_x, RID_x, $GWCS$, R_x, and TS_2 to entity x.
- Upon receiving the message, CS verifies the freshness of TS_2. If valid, x stores RID_x, SK_x, R_x in its memory, along with $GWCS$ stored on both GW and CS.
- In the case of GW, an additional value PK_{CS} is sent from TA to be stored on GW.

User Registration

During the user registration phase, user U registers with TA. Figure 4.3 illustrates this phase, with the following steps:

- U selects U_{ID} and U_{PW}, then calculates $HU_{ID} = h(U_{ID})$ and $HU_{PW} = h(U_{PW}||HU_{ID})$. U sends U_{ID}, HU_{ID}, HU_{PW}, and TS_1 to TA.
- Upon receiving the request, TA verifies the freshness of TS_1. If valid, it checks the database for U_{ID}. If U_{ID} exists, the process stops; otherwise, TA calculates $HID_{CS} = h(HU_{ID}||RID_{CS})$, $HID_{GW} = h(HU_{ID}||RID_{GW})$, and stores HU_{PW}, HU_{ID} in CS's memory. TA then sends HID_{GW}, HID_{CS}, SK_U, PK_{GW}, PK_{CS}, and $TS2$ to GW.

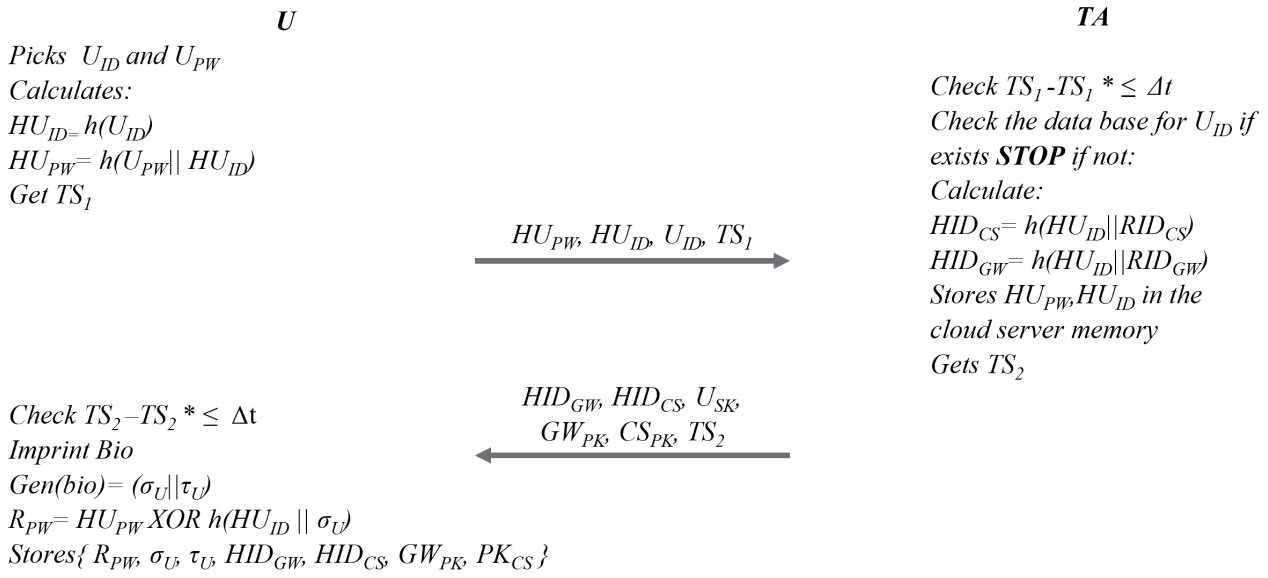


Figure 4.3: User registration

- Upon receiving the message, U verifies the freshness of TS_2. If valid, U provides biometric information, Bio $Gen(bio) = (\sigma_U||\tau_U)$, then calculates $R_{PW} = HU_{PW} \oplus h(HU_{ID}||\sigma_U)$. Finally, user U stores R_{PW}, σ_U, τ_U, HID_{GW}, HID_{CS}, PK_{GW}, PK_{CS} in its smart card SC.

Sensor Registration

The sensor registration phase is depicted in Figure 4.4, with the following steps:

- Sensor S selects S_{ID} and generates R. Then, it calculates $HS_{ID} = (S_{ID}||R_S)$. S sends S_{ID}, HS_{ID}, R_S, and $TS1$ to TA.
- Upon receiving the message from S, TA verifies the freshness of TS_1. If valid, TA checks the database for S_{ID}. If it exists, the process stops; otherwise, it generates PK_S, SK_S. Then, it calculates $RS_{ID} = h(HS_{ID}||MK)$, $HS_{CS} = h(RS_{ID}||RID_{CS})$, $HS_{GW} = h(RS_{ID}||RID_{GW})$, and stores S_{ID}, RS_{ID}, HS_{CS}, PK_S in the cloud server memory and PK_S, HS_{GW} in the gateway node memory. TA sends RS_{ID}, HID_{GW}, HID_{CS}, S_{SK}, and TS_2 back to the sensor.
- Upon receiving the message, S verifies the freshness of $TS2$. If valid, it stores S_{SK} , S_{ID}, RS_{ID}, HS_{GW}, HS_{CS} in its memory.

Upload Phase (UP)

During the upload phase, a distinct authentication process occurs between TA and CS. Whenever a patient (P) or a user (U) registers with TA, TA initiates authentication with CS to upload P's medical inspection report/sensor data or new user information to CS, as depicted in Figure 4.5. The process unfolds as follows:

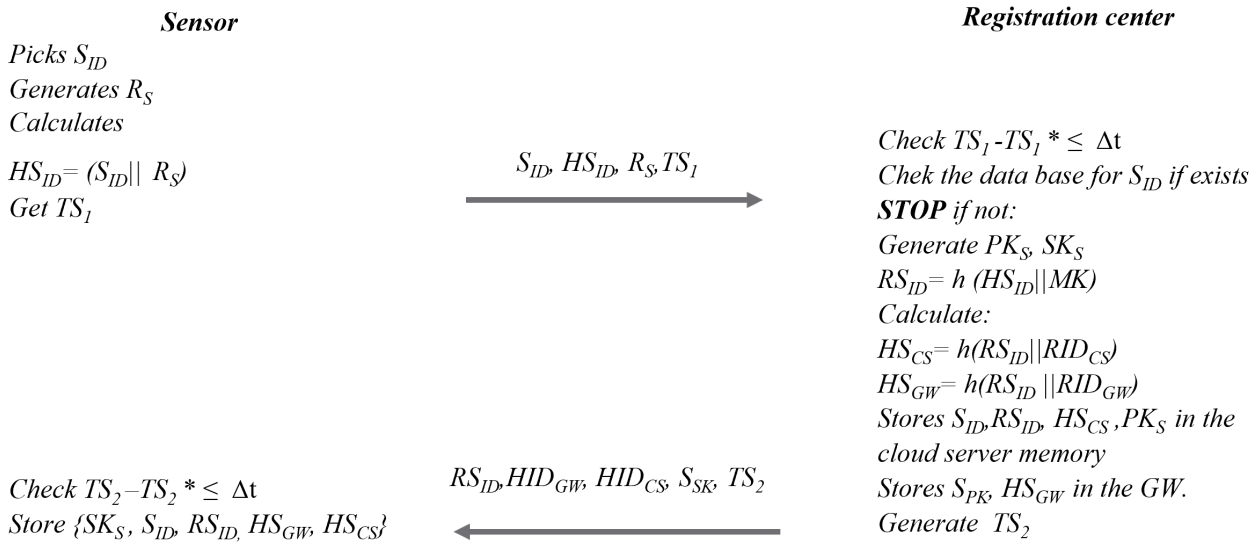


Figure 4.4: Sensor registration

- TA prepares the data for transmission. It generates R and obtains TS_1. These values are used to calculate $A = h(RID_{CS}||R||R_{CS}||TS_1)$ and $B = Kyber.enc_{PK_{CS}}(A \oplus R \oplus TS_1)$. Subsequently, TA sends A, B, and TS_1 to CS.

- Upon receiving the values, CS verifies the freshness of TS_1. If valid, it calculates: $C = Kyber.dec_{SK_{CS}}(B)$, $R' = C \oplus A \oplus TS_1$, and retrieves the stored value of RID_{CS} to calculate: $A' = h(RID_{CS}||R'||R_{CS}||TS_1)$. CS checks if $A = A'$; if yes, it generates M and obtains TS_2. It then calculates: $D = h(R_{CS}||M||TS_2||A')$ and $E = R' \oplus M \oplus TS_2$. CS sends the values D, E, and TS_2 to TA.

- Upon receiving the values from CS, TA verifies the freshness of TS_2. If valid, it calculates $M' = R \oplus E \oplus TS_2$ and $D' = (R_{CS}||M'||TS_2||A)$. It then checks if $D = D'$; if yes, TA generates L and calculates: the session key $SK = h(L||TS3||A||D')$ and $F = Kyber.enc_{PK_{CS}}(L \oplus TS_3)$. Finally, TA sends the values F and TS_3 to CS.

- Upon receiving the values, CS verifies the freshness of TS_3. If valid, it calculates: $L' = Kyber.dec_{SK_{CS}}(F) \oplus TS_3$. Then, it sets the session key $SK = h(L'||TS_3||A'||D)$.

Upon completion of the above steps, TA begins uploading the new information to CS.

Authentication Phase

In this phase, we identify four types of authentication processes: Auth 1 - Offline data access (for accessing stored health records), Auth 2 - Periodic health records, Auth 3 - Real-time data access, and Auth 4 - Check-up phase. Each of these authentication types involves distinct steps where entities authenticate each other mutually. **Auth 1 - Accessing Stored Health Records (OfDA)**

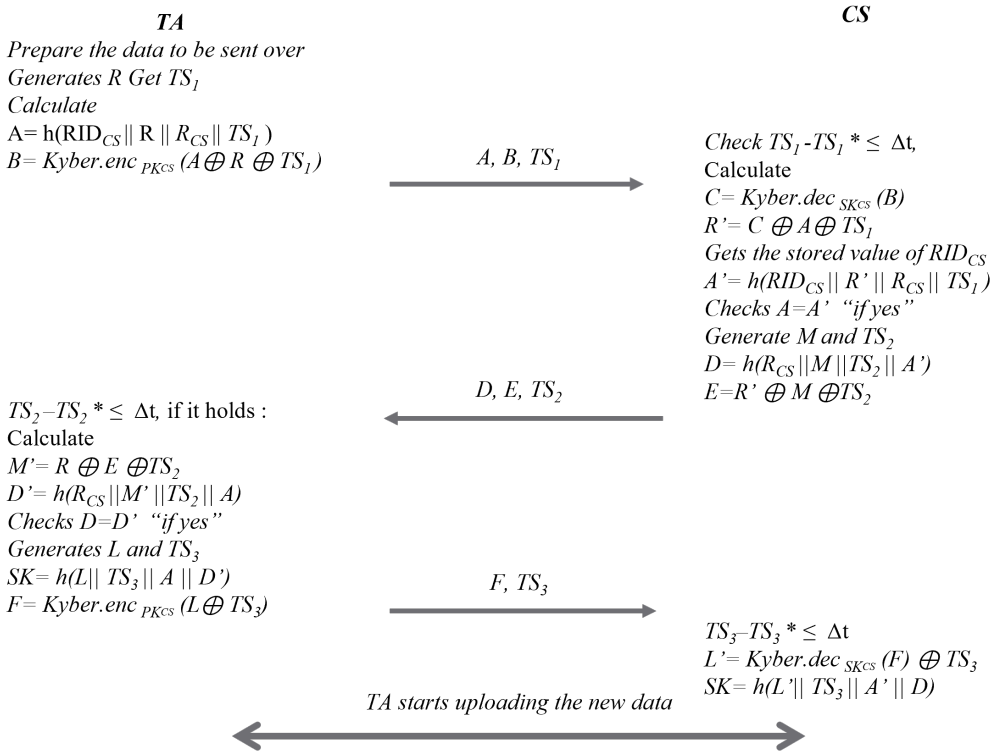


Figure 4.5: UP authentication process

During this authentication, user U must authenticate themselves to access a patient's stored health information on the cloud server CS. The process involves three entities: user (U), gateway (GW), and cloud server (CS), with each pair of entities mutually authenticating. The steps involved are as follows:

- U inserts their smart card SC and inputs U'_{ID} and U'_{PW} into a terminal to print their bio. The bio is generated using the formula $Gen(bio') = (\sigma'_U||\tau'_U)$. σ_U and τ_U are obtained from SC to compute $bio = (\sigma_U||\tau_U)$. If $bio' = bio$, the following steps are performed: $HU'_{ID} = h(U'_{ID})$, $HU'_{PW} = h(U'_{PW}||HU'_{ID})$, and $R'_{PW} = HU'_{PW} \oplus h(HU'_{ID}||\sigma'_U)$. If $R'_{PW} = R_{PW}$, TS_1 is generated. Then, the values $A = h(U'_{PW}||HU'_{ID}||HID_{GW}||TS_1)$, $B = h(HU'_{ID}||TS_1)$, $C1 = Kyber.enc_{PK_{GW}}(B \oplus (H'_{ID}||TS_1))$, and $C2 = Kyber.enc_{PK_{CS}}(HID_{CS} \oplus (HID_{GW}||TS_1))$ are calculated. Finally, U sends A, B, $C1$, and $C2$ to GW.

- Upon receiving the message, GW computes $Z = Kyber.dec_{SKGW}(C1) \oplus B$ to obtain HU''_{ID} and TS_1. If TS_1 is valid, $HID'_{GW} = h(HU''_{ID}||RID_{GW})$ and $B' = h(HU''_{ID} \oplus TS_1)$ are calculated. If $B = B'$, TS_2 is generated, and $C3 = Kyber.enc_{PK_{CS}}(HU''_{ID}||GWCS||TS_2)$ and $C4 = h(HU''_{ID}||GWCS||TS_2)$ are computed. GW then forwards $C2$, $C3$, $C4$, and A to CS.

- Upon receiving the values, CS computes $M = Kyber.dec_{SK_{CS}}$ to obtain HU''_{ID}, $GWCS$, and TS_2. If TS_2 is valid, $Y = Kyber.dec_{SK_{CS}}(C2) \oplus HID'_{CS}$ is computed. The corresponding HU'''_{ID} and HU''_{PW} are retrieved from the database using HU''_{ID} and $GWCS$. Then, $HID'_{CS} = h(HU'''_{ID}||RID_{CS})$, $A = h(U''_{PW}||HU'''_{ID}||Y)$, and $C4' = h(HU'''_{ID}||GWCS||TS_2)$

are calculated. If $C4 = C4'$, TS_3 is generated, and $C5 = Kyber.enc_{PK_{GW}}(HID'_{CS} \oplus TS_3)$ is computed. CS then calculates $C6 = h(HU'''_{ID}||GWCS||TS_3)$ and establishes its session key $SK = h(HU'''_{ID}||HID'_{GW}||HID'_{CS}||TS_3)$, sending $C5$, $C6$, and TS_3 to GW.

- Upon receiving the values, GW checks the freshness of TS_3 and computes $HID''_{CS} = Kyber.dec_{SK_{GW}}(C5) \oplus TS_3$ and $C6' = h(HU''_{ID}||GWCS||TS_3)$. Then, it checks if $C6' = C6$. If yes, TS_4 is generated, $C7 = h(C6'||HID'_{GW})$ is calculated, and $SK = h(HU''_{ID}||HID'_{GW}||HID''_{CS}||TS_3)$ is established. Finally, GW sends $C6$, $C7$, $TS3$, and $TS4$ to U.
- Upon receiving the values, U checks if TS_4 is valid. If yes, $C6'' = (HU'_{ID}||HID_{GW}||TS_3)$ is computed, and if $C6'' = C6$, $C7' = h(C6''||HID_{GW})$ is calculated. If $C7' = C7$, the session key $SK = h(HU'_{ID}||HID_{GW}||HID_{CS}||TS_3)$ is set.

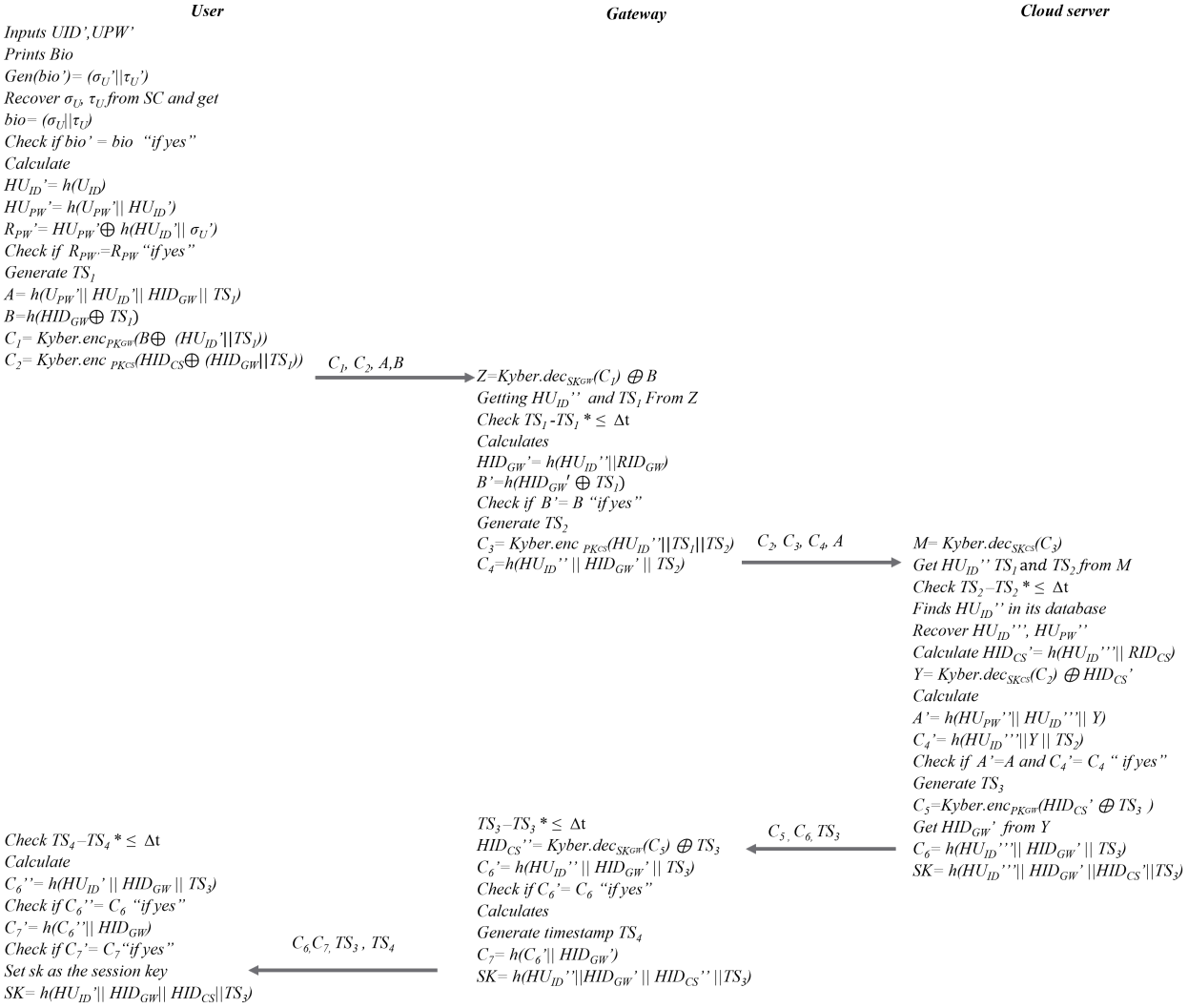


Figure 4.6: OfDA authentication

Auth 2- Periodic health records PHR During this authentication, S needs to authenticate itself and prove its legitimacy to send and store the patient's current health data on CS. This process involves three entities: CS, GW, and S. Each pair of entities mutually authenticate. Fig. 4.7 presents this phase, with the following steps:

- S generates the timestamp TS_1 then calculates: $C1 = h(HS_{GW}||TS_1), C2 = h(HS_{CS}||TS_1), C3 = h(HS_{GW}) \oplus TS_1$, and $C4 = h(TS_1) \oplus S_{ID}$. S then sends these values to GW: $C1$, $C2$, $C3$, and $C4$.

- Upon receipt of the values, GW calculates $TS_1 = h(HS_{GW} \oplus C3)$ then checks if TS_1 holds. If yes, it calculates $C1' = h(HS_{GW}||TS_1)$, checks if $C1' = C1$, and computes $S'_{ID} = h(TS_1) \oplus C4$. Then, it generates TS_2 and calculates $C5 = h(GWCS||TS_2)$ and $C6 = Kyber.enc_{PK_{CS}}((S'_{ID}||TS_2) \oplus C5)$. GW then sends $C2$, $C4$, $C5$, and $C6$ to CS.

- Upon receiving the values from GW, CS calculates $C6' = Kyber.dec_{SK_{CS}}(C6)$ and $X = C6' \oplus C5$. CS extracts S''_{ID} and TS_2 from X and checks if TS_2 holds. If yes, it retrieves S''_{ID} from its database and obtains the corresponding HS'_{CS}, RS'_{ID}, and $GWCS$. After retrieval, CS calculates $C5' = (GWCS||TS_2)$, $h(TS_1) = C4 \oplus S''_{ID}$, and $C2' = h(HS_{CS}||h(TS_1))$. It checks if $C2' = C2$ and $C5' = C5$. If yes, it generates TS_3 and calculates $C8 = h(RS'_{ID}||GWCS||TS_3)$, $C9 = Kyber.enc_{PKGW}(RS'_{ID}||TS_3)$, and $C10 = h(C8||TS_3)$. Finally, it establishes $SK = h(C5||C10||TS_3)$ and sends the values $C9$ and $C10$ to GW.

- Upon receiving the message, GW calculates $Y = Kyber.dec_{SK_{GW}}(C9)$ and obtains TS_3 from Y. It checks if TS_3 holds, then calculates $C8' = h(Y||GWCS||R_{GW})||TS_3)$, $C10' = h(C8'||TS_3)$, and $R = C1' \oplus TS_3$. If $C10' = C10$, it generates TS_4 and sets SK as $SK = h(C5'||C10'||TS_3)$. GW sends $C5$, $C10$, R, TS_4 back to S.

- Upon receiving the values, S checks if TS_4 holds. If yes, it calculates $TS_3 = C1 \oplus R$, $C8'' = h(RS_{ID}||C5||TS_3)$, and $C10'' = h(C8''||TS_3)$. Then, it checks if $C10'' = C10'$, if yes, the session key SK is generated as $SK = h(C5||C10''||TS_3)$.

Auth 3- Online data access (accessing current health status) OnDA During this authentication, U is required to authenticate themselves and establish their legitimacy to access the patient's current health data from the monitoring sensors (S). This process involves three entities: U, GW, and S. Each pair of entities is required to mutually authenticate. Fig. 4.8 illustrates this phase, with the following steps:

- U inserts their SC and utilizes a terminal to input their U'_{ID}, U'_{PW}, and prints their *bio*. Subsequently, the *bio* is regenerated using the formula $Gen(bio') = (\gamma'_U||\tau'_U)$. γ_U and τ_U are retrieved from SC to compute $bio = (\gamma_U||\tau_U)$. Verification is conducted to ascertain if $bio' = bio$. If affirmative, the following computations occur: $HU'_{ID} = h(U_{ID})$, $HU'_{PW} = h(U'_{PW}||HU'_{ID})$, $R'_{PW} = HU'_{PW} \oplus h(HU'_{ID}||\gamma'_U)$. Then, a validation is performed to check if $R_{PW} = R_{PW}$. If positive, the following are calculated: $A = h(HID_{GW}||TS_1)$, $C1 = Kyber.enc_{PK_{GW}}(A \oplus (TS_1||HU'_{ID}))$, $C2 = h(HU'_{ID}||TS_1||S'_{ID})$, and $C3 = Kyber.enc_{PK_S}(HU'_{ID}||TS_1)$. U transmits A, $C1$, $C2$, and $C3$ to GW.

- Upon reception, GW computes $X = Kyber.dec_{SK_{GW}}(C1) \oplus A$, subsequently retrieving HU''_{ID} and TS_1 from X. A validation is conducted to verify if TS_1 holds. If affirmative, $HID'_{GW} = h(HU''_{ID}||RID_{GW})$ is computed, followed by $A' = h(HID'_{GW}||TS_1)$.

Figure 4.7: PHR authentication

A check is performed to verify if $A' = A$. If positive, TS_2 is generated, and $C4 = h(HS_{GW}||HU''_{ID}||TS_1||TS_2)$ and $C5 = h(HU''_{ID}||TS_1) \oplus TS_2$ are calculated. GW then sends $C2, C3, C4, C5$ to CS.

- Upon reception of the values, S computes $Y = Kyber.dec_{SK_S}(C3)$ to extract TS_2. A validation is performed to check if TS_2 holds. If affirmative, $Z = h(Y||S_{ID})$ is computed and validated against $C2$. Upon confirmation, HU'_{ID} is retrieved from Y, and $C4' = h(HS_{GW}||Y||TS_2)$ is calculated. A validation is performed to ensure $C4' = C4$. If positive, TS_3 is generated, and the following calculations occur: $C5 = h(h(HS_{GW})||TS_3||HU'_{ID})$, $C6 = C2 \oplus TS_3 \oplus HS_{GW}$, and $C7 = h(C4' \oplus C5)$. Subsequently, $SK = h(C_5||C_7||C_4||TS_3)$ is established, and $C6$ and $C7$ are transmitted to GW.

- Upon reception, GW calculates $TS_3 = C2 \oplus C6 \oplus HS_{GW}$. A validation is performed to ensure TS_3 holds. If affirmative, $C5' = h(h(HS_{GW})||TS_3||HU''_{ID})$ and $C7' = h(C4 \oplus C5')$ are computed. Subsequently, GW checks if $C7' = C7$. If positive, TS_4 is generated, and

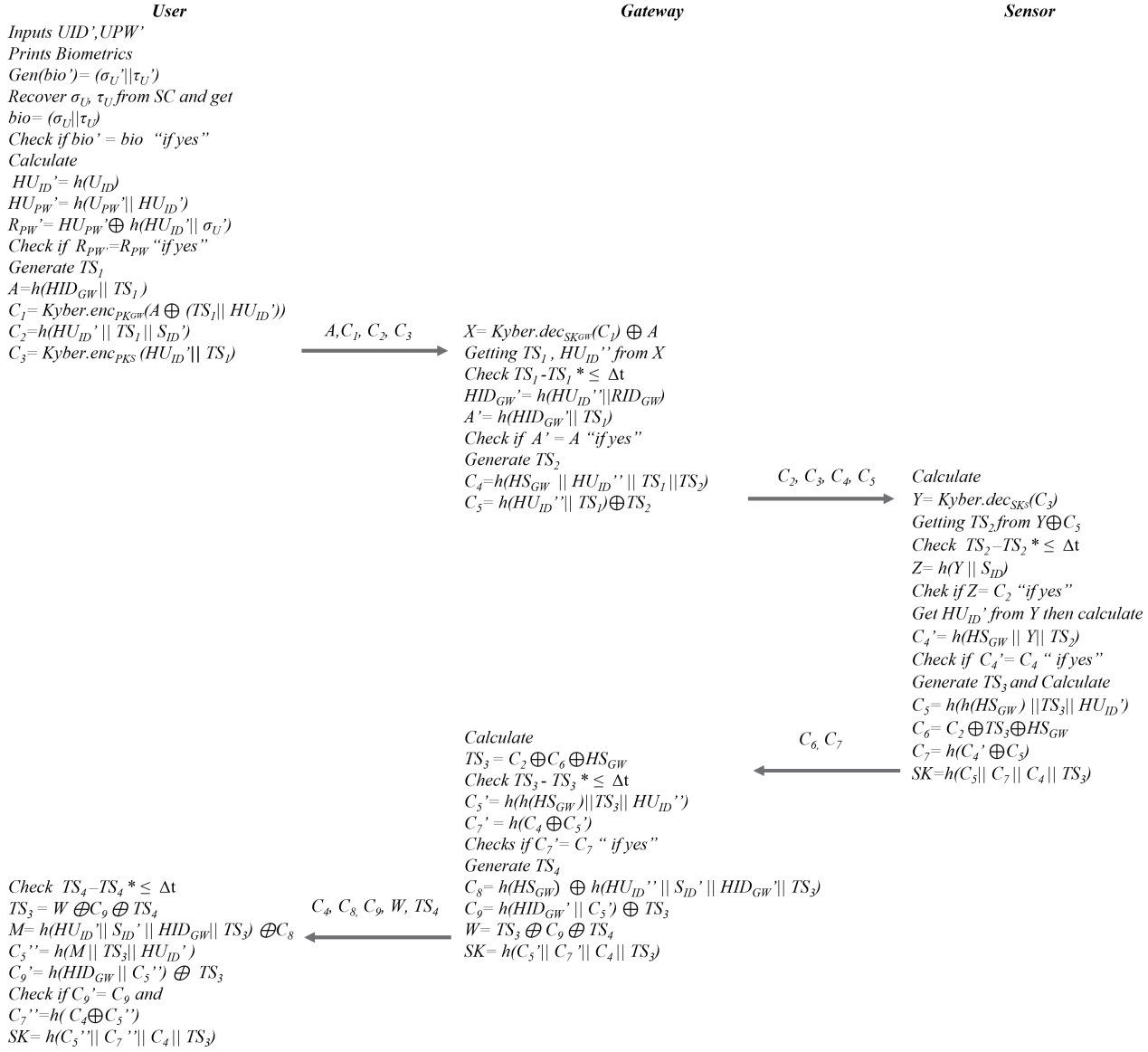


Figure 4.8: OnDA authentication

the following calculations occur: $C8 = H(HS'_{GW}||C5') \oplus TS_3$ and $W = TS_3 \oplus C9 \oplus TS_4$. At this stage, GW establishes $SK = h(C'_5||C'_7||C_4||TSC_3)$ and transmits $C4, C8, C9, W$ and TS_4 to S.

- Upon reception, S checks if TS_4 holds. If affirmative, $TS_3 = W \oplus C9 \oplus TS_4$, $C9' = W \oplus TS_3 \oplus TS_4$, $M = h(HU'_{ID}||S'_{ID}||HID_{GW}||TS_3)$, $C5'' = h(M||TS_3||HU'_{ID})$, and $C9' = h(HID_{GW}||C5'') \oplus TS_3$. Subsequently, S checks if $C9' = C9$. If affirmative, a session key SK is generated, where $SK = h(C5''||C7''||C4||TS_3)$.

Auth 4- Check up CP During this authentication, the patient utilizes their mobile device, denoted as GW, to access the CS for checking prescriptions and health observations uploaded by doctors and specialists. This process involves two entities: GW, and CS. Fig. 4.8 illustrates this phase, with the following steps:

- GW generates a random number R and obtains the timestamp TS_1. Then, it computes: $A = h(GWCS||R||TS_1)$ and $B = Kyber.enc_{PK_{CS}}((GWCS||R) \oplus TS_1)$. Subsequently, GW transmits A, B, TS_1 to CS.

- Upon receiving the values from GW, CS verifies the freshness of TS_1. If affirmative, it computes: $C = Kyber.dec_{SK_{CS}}(B)$ and $D = C \oplus TS_1$. Then, R and $GWCS$ are extracted from D, and $GWCS$ is checked in the database. Following this, $A' = h(GWCS||R||TS_1)$ is computed and validated against A. If affirmative, M and TS_2 are generated. Finally, $D = h(GWCS||M||TS_2||A')$ and $E = R \oplus M \oplus TS_2$ are calculated, and D, E, and TS_2 are sent to GW.

- Upon receipt, GW verifies the freshness of TS_2. If affirmative, it computes $M' = R \oplus E \oplus TS2$ and $D' = h(GWCS||M'||TS_2||A)$. Then, it checks $D' = D$. If affirmative, L and TS_3 are generated. At this stage, GW computes $F = Kyber.enc_{PK_{CS}}(L \oplus TS_3)$, $SK = h(L||TS_3||A||D')$, and transmits F and TS_3 to CS.

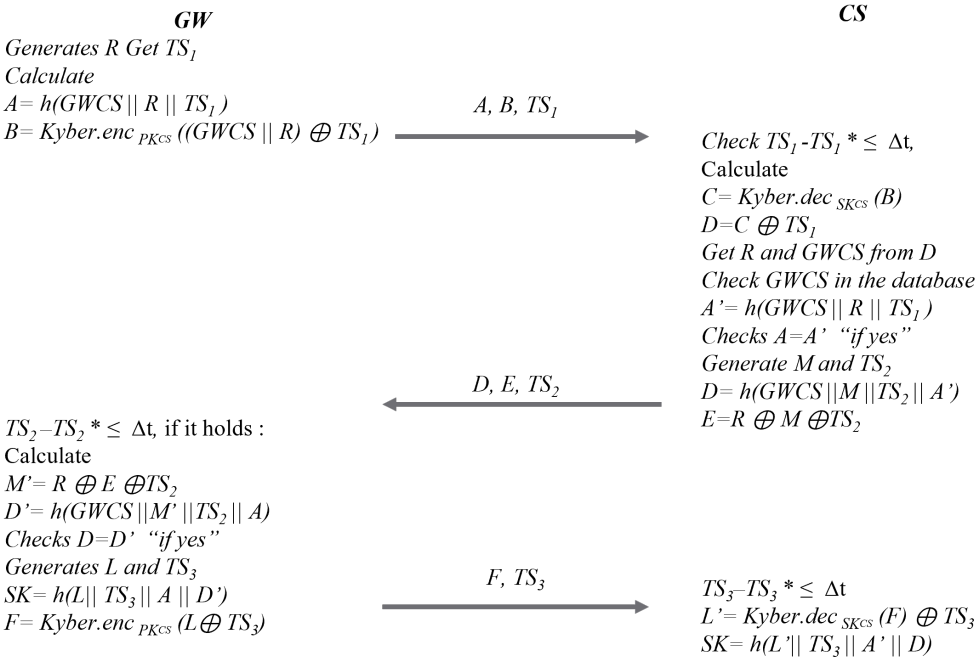


Figure 4.9: Check up authentication

- Finally, upon receiving the values, CS verifies the freshness of TS_3 and computes $L' = Kyber.dec_{SK_{CS}}(F) \oplus TS_3$. Finally, CS establishes a session key $SK = h(L'||TS_3||A'||D)$.

4.5 Conclusion

In this chapter, we introduced a thorough authentication framework "Securing Cloud-based Healthcare Applications With A Quantum-Resistant Authentication And Key Agreement

Framework: QR-AKAF" designed specifically for WBAN-based IoMT. Our framework QR-AKAF encompasses five distinct authentication scenarios, spanning from initial registration to real-time authentication during deployment. Leveraging the robustness of PQC algorithms, particularly the Kyber algorithms, our framework ensures secure authentication processes across various IoMT operations.

Each authentication scenario within our framework is meticulously crafted to seamlessly integrate with IoMT devices while upholding stringent security standards. From the secure on boarding of users and devices during registration to the dynamic authentication processes during data access and transmission, our framework provides robust safeguards against unauthorized access and malicious activities.

The deployment of our authentication framework represents a significant advancement in securing WBAN-based IoMT systems, instilling confidence in healthcare providers and patients regarding the integrity and confidentiality of their medical data. However, while the theoretical underpinnings of our framework are robust, its real-world efficacy and performance metrics remain to be rigorously evaluated.

In the subsequent chapter, we will delve into a comprehensive analysis of the security and performance aspects of our authentication framework. Through empirical testing and simulation, we aim to assess the resilience of the framework against various security threats and evaluate its computational efficiency in real-world deployment scenarios. By scrutinizing these critical aspects, we endeavor to provide valuable insights into the practical viability and effectiveness of our proposed authentication framework in safeguarding WBAN-based IoMT systems.

CHAPTER 5:

Evaluation and discussion

Chapter 5

Evaluation and discussion

Chapter Overview:: This chapter introduces all the results that prove the efficacity of our framework, through extensive testing on an ST B-L475E-IOT01A device, our proposed framework demonstrates commendable performance in terms of energy consumption, and computation time. Moreover, QR-AKAF ensures a high level of security.

5.1 Introduction

The advent of cloud-based healthcare applications has revolutionized the medical landscape, offering unprecedented opportunities for remote patient monitoring, diagnostics, and personalized treatment. However, with the vast amounts of sensitive medical data being transmitted and stored in the cloud, ensuring robust security while maintaining computational efficiency remains a paramount concern.

In response to this challenge, this chapter presents an in-depth exploration of QR-AKAF, an innovative framework meticulously crafted to address the unique security and efficiency requirements of cloud-based healthcare applications. At the core of QR-AKAF lies Kyber, a cutting-edge PQC algorithm renowned for its resource-efficient properties, effectively minimizing computational overhead without compromising on security.

Unlike conventional approaches that rely heavily on computationally expensive PBC and ECC functions, QR-AKAF harnesses the power of Kyber to optimize both computational and energy efficiency. Through meticulous formal verification using the AVISPA tool and comprehensive informal security analysis, we rigorously validate the security robustness of our framework, demonstrating its efficacy in mitigating a wide range of cyber threats prevalent in the IoMT domain.

Moreover, our study includes a comparative analysis with existing frameworks, showcasing the clear superiority of QR-AKAF in terms of reduced computation and energy expenditure. Furthermore, by significantly mitigating energy consumption at sensor nodes, our framework contributes to extending the network lifetime, thereby enhancing the overall sustainability of cloud-based healthcare systems.

In the subsequent sections, we delve into the intricate details of QR-AKAF, elucidating its architecture, security mechanisms, performance evaluation, and comparative analysis with existing solutions. Through this comprehensive examination, we aim to provide valuable insights into the development of secure and efficient frameworks tailored for the evolving landscape of cloud-based healthcare applications.

5.2 Security analysis

5.2.1 Formal verification using AVISPA

In this section, we'll provide an overview of the AVISPA verification tool, its selection rationale for evaluating our framework, and the verification results obtained with AVISPA.

Verification tool

We chose AVISPA as our formal security verification tool due to its widespread acceptance and capability to assess security protocols effectively. AVISPA's compatibility with the High-Level Protocol Specification Language (HLPSL) simplifies protocol specification and verification. Our decision to opt for AVISPA is based on several key factors:

- It can detect passive attacks, including Man-In-The-Middle (MITM) and replay attacks.
- HLPSL is widely adopted across various back-ends.
- AVISPA provides four distinct back-ends: CL-ATSE (Constraint-Logic-based Attack Searcher), SATMC (SAT-based Model Checker), OFMC (On-the-fly Model Checker), and TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols).
- AVISPA is recognized as a reliable tool for formally verifying cryptographic protocols in various domains, including RFID and WSN [172].

Additionally, we utilize SPAN (Security Protocol Animator) as a simulator to animate cryptographic security protocols specified in HLPSL and validated by AVISPA. SPAN extends its functionality to simulate communication scenarios and potential attacks.

To validate the security of our framework using AVISPA, we follow these essential steps:

- We specify the proposed framework schemes using HLPSL, including defining roles, describing transmitted messages, specifying the intruder's capabilities, laying out initial assumptions, and defining the protocol goals.
- We input the HLPSL specification of our schemes into the AVISPA tool, which translates the specification into an intermediate format (IF) to determine if the schemes are secure or if they fail to meet their security objectives.

Specification of QR:AKAF

Every HLPSL and AVISPA specification comprises basic and composed roles. Basic roles represent the actions of agents or communication entities, while composed roles instantiate the basic roles into models and sessions.

To avoid redundancy in the specifications, we outline the HLPSL pseudo-code structure for the basic roles in the Periodic Health Records scheme. This scheme includes the Sensor (S), Gateway (GW), and Cloud Server (CS) as primary roles.

The composed roles HLPSL pseudo-code within our framework, consisting of "session," "environment," and "goal," is depicted:

- The "session" role delineates the initial state of the protocol.
- The "environment" role showcases protocol sessions between various agents.
- In the "goal" role, we detail the security properties requiring verification.

The results obtained using AVISPA for our proposed framework schemes will be presented in the following subsection.

```
role cloud_server (CS,S,GW: agent, H: hash_func,
                   PKCS,PKGW: public_key, Snd,Rcv:
                   channel(dy))
played_by CS
def=
      local
      State: nat,
      SK,TS1,ID,TS3,TS2,RSID,GWCS,HSCS: text
init
State:= 0
transition
1. State=0
/\Rcv(H(HSCS.H(TS1)).xor(H(TS1),ID).
H(GWCS.TS2).{xor((ID.TS2),H(RIDGW.TS2.RGW))}_PKCS)=|>
State':=1 /\TS3':=new()/\request(CS,GW,gw_cs_auth,TS2)
/\request(CS,S, s_cs_auth_hts1,H(TS1))
/\witness(CS,GW,cs_gw_auth,TS3')
/\ witness (CS,S, cs_s_auth, TS3')
/\ secret({TS3}, sec_TS3,{S,GW,CS})
/\ Snd({RSID.TS3'}_PKGW.H(H(RSID. GWCS.TS3)))
/\ SK':=xor(H(GWCS.TS2), xor(H(H(RSID. H(RIDGW.
TS2.RGW) .TS3')),TS3'))

end role
```

```
role sensor (S,GW,CS: agent, H: hash_func,
             HSGW:text, HSCS: text,  PKCS,  PKGW:
             public_key, Snd,Rcv: channel(dy))

played_by S
def=
      local
      State: nat,
      SK,TS1,ID,TS3,TS2,RSID,GWCS: text,
      TS4: message
init
State:= 0
transition
1. State=0 /\ Rcv(start)=|> State':=1 /\ TS1':=
/\ secret({ID},sec_sid,{S,GW,CS})
/\secret(H(TS1),sec_HTS1,{S,GW,CS})
/\ witness(S,CS, s_cs_auth_hts1,H(TS1'))
/\ witness(S,GW, s_gw_auth,TS1') /\
Snd(H(HSGW.TS1).H(HSCS.H(TS1)).xor( H(HSGW),
TS1).xor(H(TS1),ID))
2. State= 1/\ Rcv(H(GWCS.TS2).H(H(RSID.
H(RIDGW.TS2.RGW).TS3)).TS4)=|> State':=2 /\request(S,CS,
cs_s_auth, TS3) /\ SK':=xor(H(GWCS.TS2), xor(H(H (RSID.
H(RIDGW.TS2.RGW).TS3)),TS3))

end role
```

```
role gateway (GW,S,CS: agent, H: hash_func, HSGW: text,
              PKCS,PKGW: public_key, Snd,Rcv: channel(dy))
played_by GW
def=
      local
      State: nat,
      SK,TS1,ID,TS3,TS2,RSID,GWCS,HSCS: text,
      TS4: message
init
State:= 0
transition
1. State=0
/\ Rcv(H(HSGW.TS1).H(HSCS.H(TS1)).xor(H(HSGW),TS1).x
(H(TS1),ID))=|> State':=1  /\ TS2':= new()
/\ request(GW,S,s_gw_auth,TS1)
/\ witness(GW,CS,gw_cs_auth,TS2)
/\ secret ({RIDGW}, sec_RIDGW, {GW,CS})
/\secret({TS2},sec_TS2,{GW,CS})
/\ Snd(H(HSCS.H(TS1)).xor(H(TS1),ID). H(GWCS.TS2).
{xor((ID.TS2), H(RIDGW.TS2.RGW))}_PKCS)
2. State=1
/\ Rcv({RSID.TS3}_PKGW. H(H(RSID. GWCS.TS3)))=|>
State':=2
/\request(GW,CS, cs_gw_auth,TS3)
/\Snd(H(GWCS.TS2).H(H(RSID.
H(RIDGW.TS2.RGW).TS3)).TS4)
/\SK':=xor(H(GWCS.TS2),
xor(H(H(RSID.H(RIDGW.TS2.RGW).TS3)) ,TS3))

end role
```

Figure 5.1: HLPSL specification pseudo-code for the basic roles in the PHR scheme

```
role session ( S, GW, CS: agent, H: hash_func,
               HSGW:text, HSCS: text,  PKCS:
               public_key, PKGW: public_key)
def=
      local
      Se,Re,Sg,Rg,Sf,Rf : channel(dy)
composition
sensor(S,GW,CS,H,HSGW,HSCS,PKCS,PKGW,Se,Re)
/\ gateway(S,GW,CS,H,HSGW,PKCS,PKGW, Sg,Rg)
/\ cloud_server(S,GW,CS,H,PKGW,PKCS,Rf,Sf)

end role
```

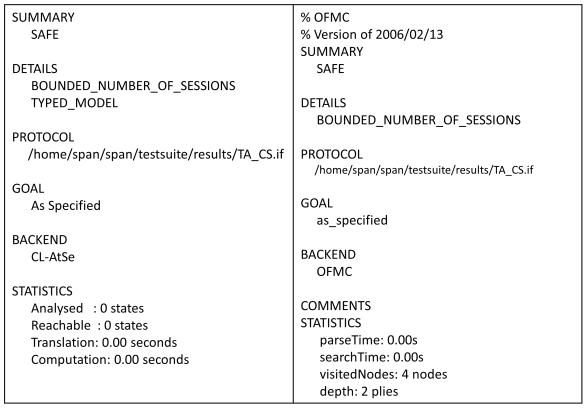
```
role environment()
def=
const
      a,b,c : agent,
      h : hash_func,
      hsgw,hscs:text,
      pkcs,pkgw: public_key,
      sec_sid, sec_TS1, sec_HTS1, sec_TS2,sec_TS3,
      sec_RIDGW, s_gw_auth_sid,s_gw_auth,
      s_cs_auth_hts1, s_cs_auth_sid,gw_cs_auth,
      cs_s_auth,cs_gw_auth: protocol_id

intruder_knowledge = {a,b,c,h,pkcs,pkgw}
composition
      session(a,b,c,h,hsgw,hscs,pkcs,pkgw)
      /\ session(a,b,c,h,hsgw,hscs,pkcs,pkgw)
      /\ session(i,b,c,h,hsgw,hscs,pkcs,pkgw)
      /\ session(a,i,c,h,hsgw,hscs,pkcs,pkgw)
      /\ session(a,b,i,h,hsgw,hscs,pkcs,pkgw)

end role
```

```
goal
      secrecy_of sec_sid % secrecy of sensor id
      secrecy_of sec_TS1 % secrecy of TS1
      secrecy_of sec_HTS1% secrecy of H(TS1)
      secrecy_of sec_TS2 % secrecy of TS2
      secrecy_of sec_RIDGW % secrecy of RIDGW
      secrecy_of sec_TS3 % secrecy of TS3
      authentication_on s_gw_auth
      authentication_on s_cs_auth_hts1
      authentication_on gw_cs_auth
      authentication_on cs_gw_auth
      authentication_on cs_s_auth


end goal

environment()
```

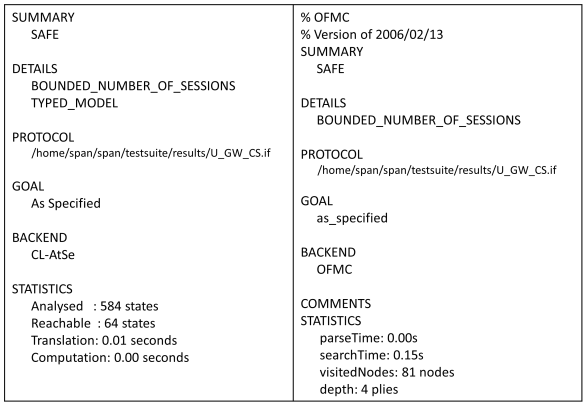
Figure 5.2: HLPSL specification pseudo-code for the composed roles in PHR scheme

Verification results

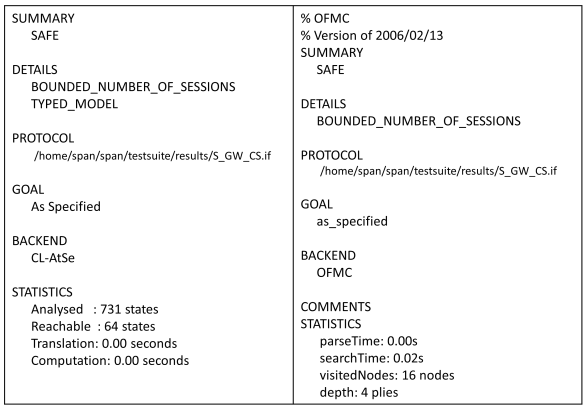
The AVISPA simulation provided validation results for each of our proposed schemes, employing the OFMC and CL-AtSe backends. The results are summarized in Figure 5.3, showcasing the verification outcomes for each scheme.



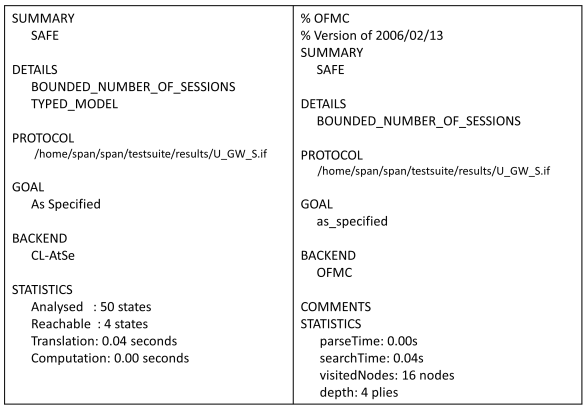
(a) Upload scheme



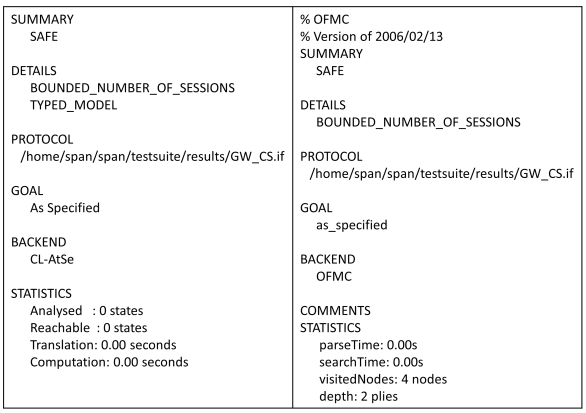
(b) Offline scheme



(c) Periodic health records scheme



(d) Online data access scheme



(e) Check-up CP scheme

Figure 5.3: CL-AtSe and OFMC results for the PHR scheme

The validation results from both backends indicate that all schemes are SAFE, thus meeting the security objectives outlined for ensuring confidentiality, mutual authentication, and protection against MITM and replay attacks. This affirmation underscores the effectiveness of our

proposed framework in achieving robust security measures.

5.2.2 Informal security analysis

The formal verification process has confirmed the safety of our framework schemes. However, it's important to note that formal analysis alone may not be entirely conclusive in demonstrating safety [173]. To ensure a comprehensive assessment, we conducted an informal security analysis for each of the proposed schemes. Detailed results of the informal security analysis for each scheme are provided below:

- **Anonymity**: Our framework ensures anonymity for both the user (U) and patient (S). In schemes like $OfDA$ and $OnDA$, the U_{ID} is never transmitted as a clear message. Instead, HU_{ID}, representing the hash of U_{ID}, is concatenated with a timestamp and other values, then hashed or encrypted before transmission, thus protecting the anonymity of U.

- **MITM attack**: The proposed framework effectively prevents MITM attacks by never sending shared secret values such as RID_{CS}, HS_{GW}, HS_{CS}, S_{ID}, HU_{ID}, HID_{GW}, and HID_{CS} as clear messages. Instead, GW and CS retrieve these values using their private keys PK_{GW} and PK_{CS}, making it difficult for an attacker ($\mathcal{A}$) to intercept this information from exchanged messages.

- **Replay attack**: Our framework mitigates replay attacks by ensuring that every message changes in every session due to random values such as R, L, M, and timestamps. Even if $\mathcal{A}$ manages to steal information and retransmit it, the framework's timestamp validation detects message reuse, effectively safeguarding against replay attacks.

- **Untraceability**: The proposed framework provides untraceability by generating exchanged messages with fresh random values and timestamps in every session. This prevents $\mathcal{A}$ from tracing messages back to the same user, thus protecting against traceability attacks.

- **Data confidentiality**: Our framework ensures data confidentiality by utilizing the post-quantum Kyber algorithm for encryption/decryption and a one-way hash function in various schemes. This prevents $\mathcal{A}$ from accessing data information during transmission unless they have the specific private key and hash value of inputs, ensuring confidentiality.

- **Authentication**: The proposed protocol offers message authentication within the UP context and other components like CP, $OnDA$, $OfDA$, and PHR. Message authentication is verified by conducting authenticity checks and validation processes for exchanged messages, ensuring security at each phase of operation.

- **Impersonation attack**: Our framework defends against impersonation attacks by making it practically impossible for $\mathcal{A}$ to impersonate a valid participant (TA or CS). This is achieved by encrypting essential values and utilizing mechanisms that require guessing multiple values simultaneously, effectively thwarting impersonation attempts.

- **Session key agreement**: The proposed framework ensures the security of session keys, as demonstrated in the UP phase. The execution of session keys relies on complex calculations involving random numbers and timestamps, making it extremely difficult for $\mathcal{A}$ to guess or calculate valid session keys.
- **Node capture attack**: Our framework protects against node capture attacks by preventing $\mathcal{A}$ from calculating valid session keys even if they obtain secret values stored in nodes (S). Additionally, our framework defends against parallel session attacks by requiring extensive knowledge of message components, effectively safeguarding against this type of attack.

5.2.3 Comparison with related frameworks

Here, we juxtapose the security attributes of our framework with those of similar frameworks: specifically, the works by Chen et al. [106], Chen et al. [107], Chiou et al. [108], Mohit et al. [109], Chandrakar et al. [129], and Kumari et al. [130]. Our analysis reveals that our framework demonstrates superior robustness compared to these counterparts. In the ensuing table (5.1), a checkmark (✓) denotes that the framework successfully thwarts the specified attack, ensuring the preservation of the corresponding security attribute. Conversely, a cross (×) indicates that the framework does not provide guaranteed protection against the mentioned security threat, rendering it vulnerable to exploitation or compromise.

Table 5.1: Security and privacy comparison

Framework	A1	A2	A3	A4	A5	A6	A7	A8	A9
Chen et al[106].	×	✓	✓	×	✓	×	✓	×	×
Chen et al.[107]	×	×	✓	×	✓	✓	✓	×	×
Chiou et al.[108]	×	✓	✓	×	✓	×	×	×	×
Mohit et al.[109]	×	✓	✓	×	✓	×	×	×	×
Chandrakar et al.[129]	✓	✓	✓	×	✓	×	✓	✓	×
Kumari et al.[130]	×	✓	✓	✓	✓	✓	✓	✓	×
Ours	✓	✓	✓	✓	✓	✓	✓	✓	✓

A1: Anonymity, A2: Message Authentication, A3: Replay, A4: Untraceability
A5: Man in the middle , A6: Impersonation, A7: Session key security
A8: Offline guessing, A9: Online monitoring

5.3 Performance analysis

Theoretical appraisal

This section entails a comprehensive performance evaluation of the scrutinized frameworks, focusing on two fundamental metrics: computational cost and energy consumption. Table 5.2 offers a theoretical appraisal and comparative analysis of performance across the various framework schemes under examination. Subsequently, we leverage the data from this table to facilitate cost calculations spanning different facets of the frameworks.

Table 5.2: Comparative Analysis of Performance in the studied Frameworks

Framework	Schemes					Total calculation cost
	UP	OnDA	OfDA	PHR	CP	
Chen et al.[106]	$7T_S + T_{Sig} + 3T_H + 2T_M + 2T_P$	NA	$2T_P + T_M + 10T_S + 2T_H + T_{Sig}$	$7T_S + 3T_H + 2T_P + T_M$	NA	$5890,836mS \approx 5.9S$
Chen et al.[107]	$T_{Sig} + 3T_S + 8T_H + 4T_P + 4T_M$	NA	$8T_H + 4T_M + 4T_P + 4T_S + T_{Sig}$	$8T_H + 4T_M + 4T_P + 4T_S$	NA	$10235.028mS \approx 10.2S$
Chiou et al.[108]	$T_{Sig} + 6T_H + 3T_P + 3T_S$	NA	$10T_h + 3T_P + 2T_S + 2T_{Sig}$	$9T_h + 2T_P + 2T_S + T_{Sig}$	$T_{Sig} + 9T_H + 2T_P + 2T_S$	$10726.298mS \approx 10.7S$
Mohit et al.[109]	$12T_H + 3T_S + T_{Sig}$	NA	$9T_H + 2T_{Sig} + 2T_S$	$10T_H + 2T_{Sig} + 2T_S$	$9T_H + 2T_S + 2T_{SIG}$	$6930.562mS \approx 6.9S$
Chandrakar et al.[129]	$12T_H + 2T_S + T_{Sig}$	NA	$12T_H + 2T_{Sig} + T_s$	$5T_S + 7T_H + 3T_{Sig}$	$5T_H + 2T_S + T_{Sig}$	$6930.234mS \approx 6.9S$
Kumari et al.[130]	$13T_H + 5T_S + T_{Sig}$	NA	$15T_H + 8T_S + 2T_{Sig}$	$18T_H + 8T_S + 2T_{Sig}$	$7T_H + 8T_S$	$4960.664mS \approx 5S$
Ours	$8T_H + 2T_{Kenc} + 2T_{Kdec}$	$17T_H + 2T_{Kenc} + 2T_{Kdec}$	$17T_H + 4T_{Kenc} + 4T_{Kdec}$	$17T_H + 2T_{Kenc} + 2T_{Kdec}$	$9T_H + 2T_{Kenc} + 2T_{Kdec}$	$98.864mS \approx 0.1S$

Table 5.3: Experimental results of the Cryptographic Primitives

Crypto-operation	Notation	Calculation time (mS)	Energy consumed (mJ)
Sign and Verification	T_{Sig}	988.830	6.541
Hash operation (SHA 256)	T_H	0.154	0.00102
Symmetric decryption/encryption (AES-128)	T_S	0.288	0.019
Scalar point multiplication (Curve BN-P254)	T_M	261.066	1.127
Bilinear pairing operation (Curve BN-P254)	T_P	577.432	3.82
Kyber encryption	T_{Kenc}	6.694	0.443
Kyber decryption	T_{Kdec}	0.672	0.0445

5.3.1 Experimental results

We utilized the RELIC Toolkit [174] for implementing both symmetric and asymmetric cryptographic primitives. This toolkit is renowned for its lightweight implementation of asymmetric cryptographic algorithms. Additionally, for integrating Kyber post-quantum cryptography, we leveraged the pqm4 library, specifically tailored for ARM Cortex-M4 microcontrollers, encompassing implementations of post-quantum key encapsulation mechanism (KEM) and signature schemes [175]. The experimental setup was conducted on the FIT IoT-LAB: Open Experimental IoT Testbed [176], which offers a diverse array of low-power wireless nodes and mobile robots for large-scale experimentation with wireless IoT technologies. Our implementation was executed on an ST B-L475E-IOT01A board, featuring a 64-Mbit Quad-SPI (Macronix) Flash memory, an Arm Cortex-M4 core with 1 Mbyte of Flash memory, and 128 Kbytes of SRAM.

Table 5.3 presents a detailed breakdown of the cryptographic primitives employed in the analyzed frameworks, accompanied by their respective computational times and energy consumption observed during our implementation.

Computational cost

Figure 5.4 visually presents the computational costs (in mS) associated with the frameworks examined. Upon initial examination of Figure 5.4, it is evident that our framework demonstrates a significantly lower computational cost, approximately 98.9 mS. In comparison, the computational time for the Chiou et al. [108] framework is substantially higher at 10726.3

Table 5.4: Comparison the communication cost in bytes

Framework	Schemes					Total communication cost in Bytes
	UP	OnDA	OfDA	PHR	CP	
Chen et al.[106]	102	NA	118	102	NA	322
Chen et al.[107]	242	NA	274	258	NA	944
Chiou et al.[108]	88	NA	264	200	265	817
Mohit et al.[109]	74	NA	224	218	148	664
Chandrakar et al.[129]	100	NA	662	140	278	1180
Kumari et al.[130]	66	NA	86	66	66	372
Ours	1684	1808	1808	1828	1684	8812

mS. Similarly, Chen et al. [107], Mohit et al. [109], Chandrakar et al. [129], Chen et al. [106], and [130] frameworks exhibit computational times of 10235 mS, 6930.6 mS, 6930.2 mS, 5890.8 mS, and 4960.7 mS, respectively. It should be noted that this significant disparity in computational results is primarily attributed to the utilization of Kyber encryption, which outperforms traditional PBC and ECC by a computation difference of 86 times and 39 times, respectively. Consequently, Kyber proves to be a more suitable choice for IoT-based frameworks.

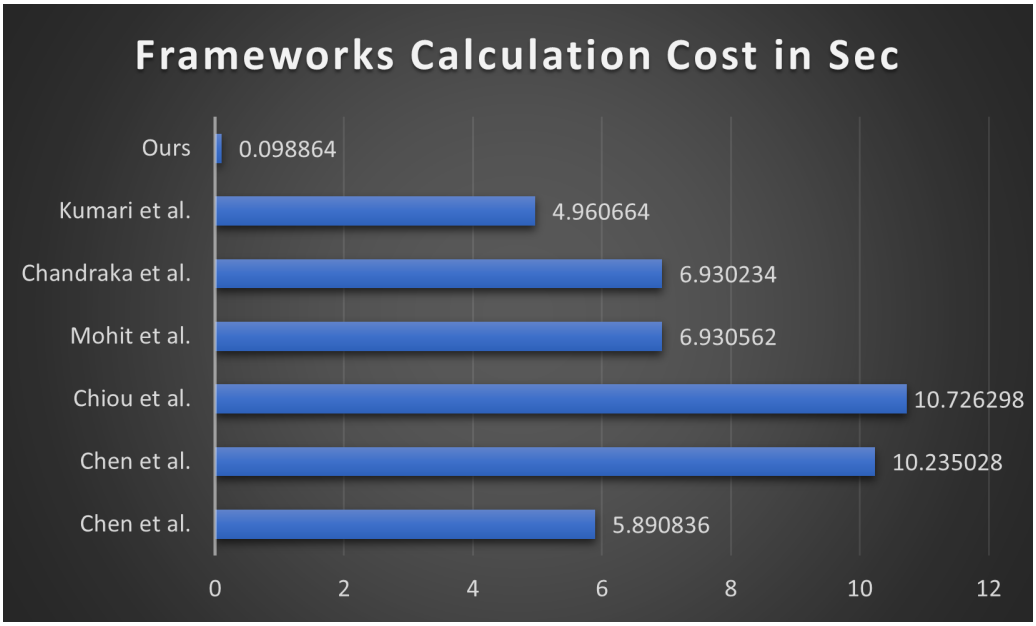


Figure 5.4: Calculation cost evaluation

Communication cost

To compute the communication cost of the studied frameworks, we initially use the same assumptions in [108, 109] and define the following assumptions:

- The output of kyber encryption is 800 bytes.
- Length of timestamp is 8 bytes.

Table 5.4 presents the detailed communication cost of the studied frameworks and Figure 5.5 present a comparative analysis of the total communication costs in bytes across the different studied frameworks, with a focus on our proposed framework ("Ours").

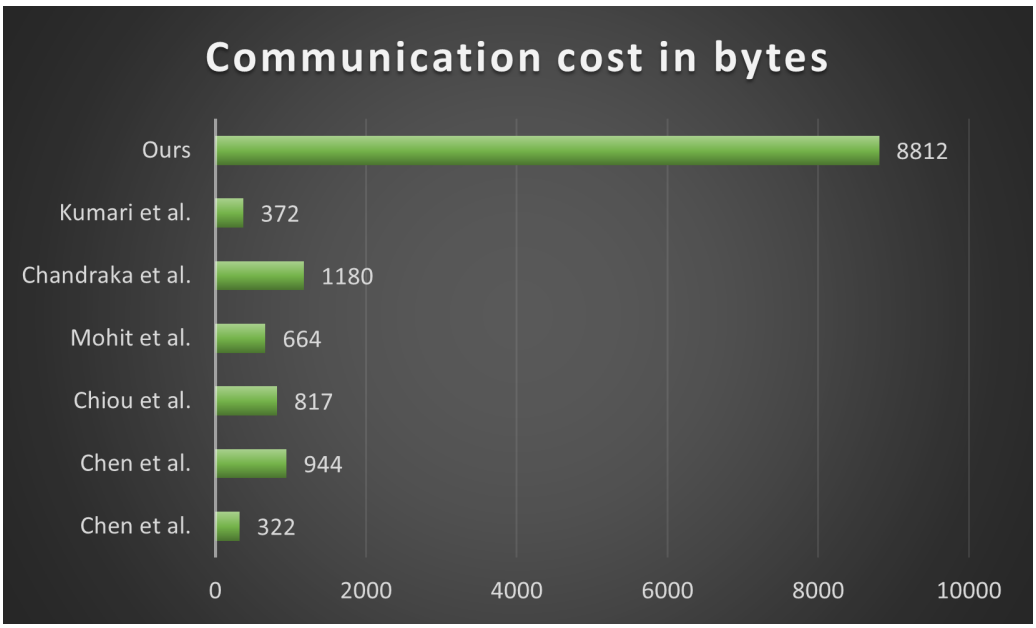


Figure 5.5: Communication cost evaluation

The communication costs for various schemes are as follows: Chiou et al. [107] with 322 bytes, Chen et al. [106] with 944 bytes, Chiou et al. [108] with 817 bytes, Mohit et al. [109] with 664 bytes, Chandrakar et al. [129] with 1180 bytes, and Kumari et al. [130] with 372 bytes. In contrast, our proposed scheme exhibits a considerably higher communication cost of 8812 bytes.

At first glance, Kumari et al. [130] appears to have the most efficient communication overhead. However, this advantage is offset by its shortcomings in security measures.

The relatively high communication cost in our scheme, as reflected in the total communication cost, can be primarily attributed to the output size of the Kyber encryption, which amounts to 800 bytes. Despite this, our scheme boasts lower computational demands and provides superior security features compared to existing frameworks. While other schemes may exhibit lower communication costs, our emphasis on robust security and efficient computation justifies this trade-off.

Energy cost

Figure 5.6 illustrates the energy consumption across the analyzed frameworks. To estimate the energy consumption throughout the computation process, we employed the formula $W = V \times I \times t$. In this equation, W signifies the power consumption measured in millijoules (mJ), V represents the voltage in volts (V), I denotes the current draw during active mode in milliamps (mA), and t corresponds to the time measured in seconds (s), as detailed in [160].

When comparing the results depicted in Figure 5.6, it becomes evident that our framework demonstrates significantly lower energy consumption in contrast to the other frameworks. The energy expended during the computation process is notably impacted by the duration of computational operations, where extended computational times invariably lead to elevated

energy consumption. Furthermore, selecting cryptographic primitives also plays a pivotal role in shaping energy consumption levels.

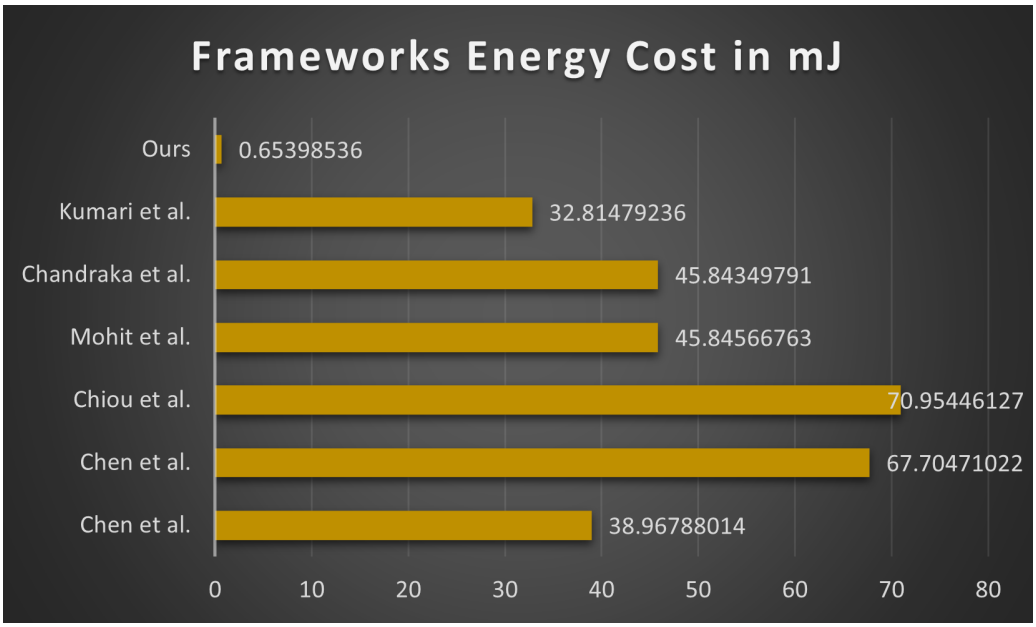


Figure 5.6: Calculation cost evaluation

5.4 Conclusion

This chapter delves into the performance evaluation of QR-AKAF, our innovative framework tailored for cloud-based healthcare applications. Our primary objective was to strike a delicate balance between security and efficiency within our design. In QR-AKAF, we employ Kyber, a resource-efficient PQC algorithm that minimizes the computational overhead.

Unlike traditional approaches utilizing expensive PBC and ECC functions, QR-AKAF leverages Kyber to enhance both computational and energy efficiency. To validate the security robustness of our scheme, we conducted formal verification using the AVISPA tool. Additionally, a comprehensive informal security analysis demonstrates that our framework achieves all essential security properties and effectively mitigates various cyber threats in the IoMT domain.

Comparative analysis with existing frameworks underscores the superiority of QR-AKAF in terms of reduced computation and energy expenditure. Moreover, our framework contributes to prolonging network lifetime by mitigating energy consumption at sensor nodes.

Conclusion and perspectives

Conclusion and perspectives

Ensuring security in WBAN-based IoMT presents a formidable challenge due to the dynamic and open nature of these networks. Vulnerable to various cyber threats, WBANs operate in environments where conventional security measures struggle to cope. Moreover, the inherent resource constraints of sensor devices hinder the implementation of traditional security protocols, leading to excessive computation overhead, communication complexities, and heightened energy consumption. Cryptography emerges as a pivotal security measure in safeguarding communications within WBANs, offering fundamental security assurances necessary for IoMT applications.

SKC-based schemes demonstrate remarkable efficiency in terms of computational overhead and energy consumption. However, the challenge lies in the distribution of keys, presenting a significant hurdle. Moreover, these schemes often lack a satisfactory balance between resilience and cryptographic key storage. Early attempts to implement PKC in sensor networks using RSA proved impractical due to its large key size and computationally intensive cryptographic primitives. Subsequent research has shown ECC to be a more viable option for PKC in resource-constrained devices, owing to its smaller key sizes and faster execution time. Nonetheless, integrating PKC schemes into IoMT necessitates the authentication of public keys, a requirement that poses challenges. Traditional PKI solutions are infeasible in sensor networks due to the overhead and complexity associated with public-key certificates, including their distribution, storage, and verification.

Kyber, a post-quantum cryptographic (PQC) scheme, offers a promising alternative to traditional public-key cryptography (PKC) methods like RSA and ECC. Unlike these conventional schemes, Kyber is designed to withstand quantum attacks, making it suitable for use in environments where quantum computing poses a threat to security. With Kyber, cryptographic keys are generated and managed differently, leveraging lattice-based techniques to ensure resilience against quantum adversaries. Additionally, Kyber exhibits favorable performance characteristics, boasting low computational and communication overheads compared to traditional PKC methods. This makes Kyber an attractive choice for securing sensitive data in the face of emerging quantum threats.

In this thesis, our focus was on addressing security concerns in WBAN-based IoMT applications while maintaining optimal performance. We commenced by examining the security landscape of IoMT, delving into various constraints, requirements, and potential cyber threats faced by WBANs. Following this, we conducted a comprehensive review of existing PKC-based schemes in WBAN-based IoMT applications, covering pairings, ECC-based, hash-based, and SKC schemes. Through this review, we identified shortcomings across these schemes, paving the way for our proposed solution. Our proposal involves leveraging Kyber PQC to bolster

IoMT security. With Kyber, our objective is to strike a balance between efficiency and security, ensuring robust protection with lightweight operations.

In our endeavor to fortify the security of WBAN-based healthcare systems, we have introduced a novel authentication framework in our recent work, documented in [164]. By harnessing the capabilities of Kyber, a PQC solution, we aim to address the inherent vulnerabilities and security challenges prevalent in WBAN-enabled healthcare environments. This authentication framework represents a significant advancement in IoMT security, offering robust protection against a myriad of cyber threats while ensuring the integrity and confidentiality of sensitive medical data. Through meticulous design and implementation, our framework seeks to establish a seamless balance between stringent security requirements and the operational efficiency demanded by real-world WBAN deployments. By leveraging the advanced cryptographic features of Kyber, we envision a future where WBAN-based healthcare systems can operate with enhanced resilience and trustworthiness, safeguarding patient privacy and facilitating reliable medical services in an increasingly connected healthcare landscape.

Moving forward, our ongoing research endeavors will encompass an extension of our proposed solutions. Our future perspectives are summarized as follows:

- Extend our proposals to support blockchain-based IoT in healthcare applications. This extension will secure communication between IoT devices and blockchain nodes, ensuring the privacy of sensitive data such as Electronic Health Records (EHRs).
- Validate our proposals using the Random Oracle Model (ROM).

Bibliography

[1] Anwar Noureddine Bahache, Noureddine Chikouche, and Fares Mezrag, "Authentication schemes for healthcare applications using wireless medical sensor networks: A survey", in: *SN Computer Science* 3.*5* (2022), p. 382.

[2] Jorge E Ibarra-Esquer et al., "Tracking the evolution of the internet of things concept across different application domains", in: *Sensors* 17.*6* (2017), p. 1379.

[3] Alem Čolaković and Mesud Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues", in: *Computer networks* 144 (2018), pp. 17–39.

[4] MFM Firdhous, BH Sudantha, and PM Karunaratne, "IoT enabled proactive indoor air quality monitoring system for sustainable health management", in: *2017 2nd International Conference on Computing and Communications Technologies (ICCCT)*, IEEE, 2017, pp. 216–221.

[5] Bhagya Nathali Silva, Murad Khan, and Kijun Han, "Internet of things: A comprehensive review of enabling technologies, architecture, and challenges", in: *IETE Technical review* 35.*2* (2018), pp. 205–220.

[6] GGKWMSIR Karunarathne, KADT Kulawansa, and MFM Firdhous, "Wireless communication technologies in internet of things: A critical evaluation", in: *2018 International conference on intelligent and innovative computing applications (ICONIC)*, IEEE, 2018, pp. 1–5.

[7] Feng Wang et al., "A survey from the perspective of evolutionary process in the internet of things", in: *International Journal of Distributed Sensor Networks* 11.*3* (2015), p. 462752.

[8] Charith Perera et al., "Context aware computing for the internet of things: A survey", in: *IEEE communications surveys & tutorials* 16.*1* (2013), pp. 414–454.

[9] Arbia Riahi Sfar et al., "A roadmap for security challenges in the Internet of Things", in: *Digital Communications and Networks* 4.*2* (2018), pp. 118–137.

[10] Veena Pureswaran and Paul Brody, "Device democracy: Saving the future of the Internet of Things", in: *IBM Corporation* 23 (2015).

[11] Asma Haroon et al., "Constraints in the IoT: the world in 2020 and beyond", in: *International Journal of Advanced Computer Science and Applications* 7.*11* (2016).

[12] Pallavi Sethi and Smruti R Sarangi, "Internet of things: Architectures, protocols, and applications.", in: *Journal of Electrical & Computer Engineering* (2017).

[13] Miao Wu et al., "Research on the architecture of Internet of Things", in: *2010 3rd international conference on advanced computer theory and engineering (ICACTE)*, vol. 5, IEEE, 2010, pp. V5–484.

[14] Rafiullah Khan et al., "Future internet: the internet of things architecture, possible applications and key challenges", in: *2012 10th international conference on frontiers of information technology*, IEEE, 2012, pp. 257–260.

[15] Laura Garcıa-Garcıa et al., "Wireless technologies for IoT in smart cities", in: *Network Protocols and Algorithms* 10.*1* (2018), pp. 23–64.

[16] NIDAL M Turab, "IoT wireless home automation technologies and their relation to specific absorption rate", in: *Journal of Theoretical and Applied Information Technology* 96.*14* (2018), pp. 4597–4609.

[17] Delphine Christin, Parag S Mogre, and Matthias Hollick, "Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives", in: *Future Internet* 2.*2* (2010), pp. 96–125.

[18] Olakunle Elijah et al., "An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges", in: *IEEE Internet of things Journal* 5.*5* (2018), pp. 3758–3773.

[19] Ibrar Yaqoob et al., "Enabling communication technologies for smart cities", in: *IEEE Communications Magazine* 55.*1* (2017), pp. 112–120.

[20] Sankar Mukherjee and GP Biswas, "Networking for IoT and applications using existing communication technology", in: *Egyptian Informatics Journal* 19.*2* (2018), pp. 107–127.

[21] Mani Pareek and Sushil Buriya, "A study of link layer protocols in IoT", in: *International Journal on Future Revolution in Computer Science & Communication Engineering* 4.*2* (2018), pp. 355–359.

[22] Tara Salman and Raj Jain, "A survey of protocols and standards for internet of things", in: *arXiv preprint arXiv:1903.11549* (2019).

[23] Wu Mengdi, "Wireless communication technologies in Internet of Things (IoT)", in: *MSc Thesis, Faculty of Technology, Communication and Systems Engineering* (2017).

[24] Lionel Metongnon and Ramin Sadre, "Fast and efficient probing of heterogeneous IoT networks", in: *International Journal of Network Management* 28.*1* (2018), e1997.

[25] Huang-Chen Lee and Kai-Hsiang Ke, "Monitoring of large-area IoT sensors using a LoRa wireless mesh network system: Design and evaluation", in: *IEEE Transactions on Instrumentation and Measurement* 67.*9* (2018), pp. 2177–2187.

[26] Mahmoud Elkhodr, Seyed Shahrestani, and Hon Cheung, "Emerging wireless technologies in the internet of things: a comparative study", in: *arXiv preprint arXiv:1611.00861* (2016).

[27] Antar Shaddad Abdul-Qawy et al., "The internet of things (iot): An overview", in: *International Journal of Engineering Research and Applications* 5.*12* (2015), pp. 71–82.

[28] Zhuguo Li et al., "The evolution of IoT wireless networks for low-rate and real-time applications", in: 18.*1* (2017), pp. 175–188.

[29] H Kaur and S Sharma, "A comparative study of wireless technologies: zigbee, bluetooth le, enocean, wavenis, insteon and uwb", in: *Proceedings of the International Conference on Recent Trends in Computing and Communication Engineering (RTCCE'13)*, 2013.

[30] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi", in: *IECON 2007-33rd Annual Conference of the IEEE Industrial Electronics Society*, Ieee, 2007, pp. 46–51.

[31] Sharmin Akter, Rashidah Funke Olanrewaju, Thouhedul Islam, et al., "LiFi based automated shopping assistance application in IoT", in: *Journal of Physics: Conference Series*, vol. 1018, 1, IOP Publishing, 2018, p. 012001.

[32] Manirafasha Cedrick, M Anandraj, and Bugingo Jean de Dieu, "How LI-FI will improve the reliability of internet of things: A review", in: *International Research Journal of Engineering and Technology* 4.*4* (2017), pp. 2686–2689.

[33] Manas Ranjan Mallick, "A comparative study of wireless protocols with Li-Fi technology: A survey", in: *Proceedings of 43rd IRF International Conference*, 2016, pp. 8–12.

[34] Ian F Akyildiz et al., "A survey on sensor networks", in: *IEEE Communications magazine* 40.*8* (2002), pp. 102–114.

[35] Chiara Buratti et al., "An overview on wireless sensor networks technology and evolution", in: *Sensors* 9.*9* (2009), pp. 6869–6896.

[36] Lanfang Sun et al., "Edge-cloud computing and artificial intelligence in internet of medical things: architecture, technology and application", in: *IEEE access* 8 (2020), pp. 101079–101092.

[37] Naeem Ali Askar et al., "Architecture, Protocols, and Applications of the Internet of Medical Things (IoMT).", in: *J. Commun.* 17.*11* (2022), pp. 900–918.

[38] Ognjen Riđić et al., "The smart city, smart contract, smart health care, internet of things (IoT), opportunities, and challenges", in: *Blockchain Technologies for Sustainability* (2022), pp. 135–149.

[39] R Madhumathi, T Arumuganathan, and R Shruthi, "Internet of things in precision agriculture: A survey on sensing mechanisms, potential applications, and challenges", in: *Intelligent Sustainable Systems: Proceedings of ICISS 2021* (2022), pp. 539–553.

[40] Satarupa Mohanty et al., "Smart healthcare analytics using internet of things: An overview", in: *Smart Healthcare Analytics: State of the Art* (2022), pp. 1–11.

[41] Samiya Khan and Mansaf Alam, "Wearable internet of things for personalized healthcare: Study of trends and latent research", in: *Health informatics: A computational perspective in healthcare* (2021), pp. 43–60.

[42] Alaa Hamid Mohammed, Raad M Khaleefah, Ihsan Amjad Abdulateef, et al., "A review software defined networking for internet of things", in: *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, IEEE, 2020, pp. 1–8.

[43] Ghulam Muhammad, Mohammed F Alhamid, and Xiaomi Long, "Computing and processing on the edge: Smart pathology detection for connected healthcare", in: *IEEE Network* 33.*6* (2019), pp. 44–49.

[44] Omaji Samuel et al., "IoMT: A COVID-19 healthcare system driven by federated learning and blockchain", in: *IEEE Journal of Biomedical and Health Informatics* 27.*2* (2022), pp. 823–834.

[45] Eman M Abounassar, Passent El-Kafrawy, and Ahmed A Abd El-Latif, "Security and interoperability issues with internet of things (IoT) in healthcare industry: A survey", in: *Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions* (2022), pp. 159–189.

[46] Hadeel Elayan, Raed M Shubair, and Asimina Kiourti, "Wireless sensors for medical applications: Current status and future challenges", in: *2017 11th European Conference on Antennas and Propagation (EUCAP)*, IEEE, 2017, pp. 2478–2482.

[47] Eric J Topol, Steven R Steinhubl, and Ali Torkamani, "Digital medical tools and sensors", in: *Jama* 313.*4* (2015), pp. 353–354.

[48] Amal Bouazizi et al., "Wireless body area network for e-health applications: Overview", in: *2017 International Conference on Smart, Monitored and Controlled Cities (SM2C)*, IEEE, 2017, pp. 64–68.

[49] GK Ragesh and K Baskaran, "An overview of applications, standards and challenges in futuristic wireless body area networks", in: *International Journal of Computer Science Issues (IJCSI)* 9.*1* (2012), p. 180.

[50] GS Karthick and PB Pankajavalli, "A review on human healthcare Internet of things: a technical perspective", in: *SN Computer Science* 1.*4* (2020), pp. 1–19.

[51] Josip Car et al., "The impact of eHealth on the quality and safety of healthcare", in: *A Systemic Overview & Synthesis of the Literature Report for the NHS Connecting for Health Evaluation Programme* (2008).

[52] Richard Hillestad et al., "Can electronic medical record systems transform health care? Potential health benefits, savings, and costs", in: *Health affairs* 24.*5* (2005), pp. 1103–1117.

[53] Kumar Laxman, Sharanie Banu Krishnan, and Jaspaljeet Singh Dhillon, "Barriers to adoption of consumer health informatics applications for health self management", in: *Health Science Journal* 9.*5* (2015), p. 1.

[54] Md Taslim Arefin, Mohammad Hanif Ali, and AKM Fazlul Haque, "Wireless body area network: An overview and various applications", in: *Journal of Computer and Communications* 5.*7* (2017), pp. 53–64.

[55] Gulraiz J Joyia et al., "Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain.", in: *J. Commun.* 12.*4* (2017), pp. 240–247.

[56] Chao-Hsi Huang and Kung-Wei Cheng, "RFID technology combined with IoT application in medical nursing system", in: *Bulletin of Networking, Computing, Systems, and Software* 3.*1* (2014), pp. 20–24.

[57] Chetanya Puri et al., "iCarMa: inexpensive cardiac arrhythmia management–an IoT healthcare analytics solution", in: *Proceedings of the first workshop on IoT-enabled healthcare and wellness technologies and systems*, 2016, pp. 3–8.

[58] Duddela Dileep Kumar and Pratti Venkateswarlu, "Secured smart healthcare monitoring system based on iot", in: *Imperial Journal of Interdisciplinary Research* 2.*10* (2016).

[59] Rashmi Singh, "A proposal for mobile e-care health service system using IoT for Indian scenario", in: *Journal of Network Communications and Emerging Technologies (JNCET)* 6.*1* (2016).

[60] Vivek Chandel et al., "Exploiting IMU sensors for IOT enabled health monitoring", in: *Proceedings of the First Workshop on IoT-enabled healthcare and wellness technologies and systems*, 2016, pp. 21–22.

[61] Shu-yuan Ge et al., "Design and implementation of interoperable IoT healthcare system based on international standards", in: *2016 13th IEEE annual consumer communications & networking conference (CCNC)*, IEEE, 2016, pp. 119–124.

[62] Jamil Y Khan and Mehmet R Yuce, *Wireless body area network (WBAN) for medical applications*, InTechOpen, 2010.

[63] Pallavi Chavan et al., "ECG-Remote patient monitoring using cloud computing", in: *Imperial Journal of Interdisciplinary Research* 2.*2* (2016), pp. 368–372.

[64] Luis ML Oliveira and Joel JPC Rodrigues, "Wireless Sensor Networks: A Survey on Environmental Monitoring.", in: *J. Commun.* 6.*2* (2011), pp. 143–151.

[65] Foteini Andriopoulou, Tasos Dagiuklas, and Theofanis Orphanoudakis, "Integrating IoT and fog computing for healthcare service delivery", in: *Components and services for IoT platforms: Paving the way for IoT standards* (2017), pp. 213–232.

[66] Robert SH Istepanian et al., "Internet of m-health Things "m-IoT"", in: *IET Seminar on Assisted Living 2011*, IET, 2011, pp. 1–3.

[67] Vasileios Tsoutsouras et al., "Software design and optimization of ECG signal analysis and diagnosis for embedded IoT devices", in: *Components and Services for IoT Platforms: Paving the Way for IoT Standards* (2017), pp. 299–322.

[68] Subrato Bharati et al., "Applications and challenges of cloud integrated IoMT", in: *Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications* (2021), pp. 67–85.

[69] Md Robiul Alam Robel et al., "Fault tolerance in cloud computing-an algorithmic approach", in: *Innovations in Bio-Inspired Computing and Applications: Proceedings of the 10th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2019) held in Gunupur, Odisha, India during December 16-18, 2019 10*, Springer, 2021, pp. 307–316.

[70] Hong-Linh Truong and Schahram Dustdar, "Principles for engineering IoT cloud systems", in: *IEEE Cloud Computing* 2.*2* (2015), pp. 68–76.

[71] AHM Shahariar Parvez et al., "Effect of fault tolerance in the field of cloud computing", in: *Inventive Computation Technologies 4*, Springer, 2020, pp. 297–305.

[72] R Katz, P Goldstein, and R Yanosky, *Cloud computing in higher. EDUCAUSE (2010)*.

[73] Victor Chang, "An overview, examples, and impacts offered by emerging services and analytics in cloud computing virtual reality", in: *Neural Computing and Applications* 29.*5* (2018), pp. 1243–1256.

[74] Alessandra Flammini and Emiliano Sisinni, "Wireless sensor networking in the internet of things and cloud computing era", in: *Procedia Engineering* 87 (2014), pp. 672–679.

[75] Djallel Eddine Boubiche et al., "Cybersecurity issues in wireless sensor networks: current challenges and solutions", in: *Wireless Personal Communications* 117 (2021), pp. 177–213.

[76] John Paul Walters et al., "Wireless sensor network security: A survey", in: *Security in distributed, grid, mobile, and pervasive computing* 1.*367* (2007), p. 6.

[77] Jason Hill et al., "System architecture directions for networked sensors", in: *ACM Sigplan notices* 35.*11* (2000), pp. 93–104.

[78] Ali Ghubaish et al., "Recent advances in the internet-of-medical-things (IoMT) systems security", in: *IEEE Internet of Things Journal* 8.*11* (2020), pp. 8707–8718.

[79] Philemon Kasyoka, Michael Kimwele, and Shem Mbandu Angolo, "Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system", in: *Journal of medical engineering & technology* 44.*1* (2020), pp. 12–19.

[80] Taha Belkhouja, Sameh Sorour, and Mohamed S Hefeida, "Role-based hierarchical medical data encryption for implantable medical devices", in: *2019 IEEE Global Communications Conference (GLOBECOM)*, IEEE, 2019, pp. 1–6.

[81] Mohammad Sadegh Yousefpoor and Hamid Barati, "Dynamic key management algorithms in wireless sensor networks: A survey", in: *Computer Communications* 134 (2019), pp. 52–69.

[82] Ayoub Benayache et al., "MsM: A microservice middleware for smart WSN-based IoT application", in: *Journal of Network and Computer Applications* 144 (2019), pp. 138–154.

[83] Usha Jain and Muzzammil Hussain, "Securing wireless sensors in military applications through resilient authentication mechanism", in: *Procedia Computer Science* 171 (2020), pp. 719–728.

[84] Jinfang Jiang et al., "A survey on location privacy protection in wireless sensor networks", in: *Journal of Network and Computer Applications* 125 (2019), pp. 93–114.

[85] Roberto Di Pietro et al., "Security in wireless ad-hoc networks–a survey", in: *Computer Communications* 51 (2014), pp. 1–20.

[86] Bharat Bhushan and Gadadhar Sahoo, "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks", in: *Wireless Personal Communications* 98 (2018), pp. 2037–2077.

[87] Sarika Choudhary and Nishtha Kesswani, "Detection and prevention of routing attacks in internet of things", in: *2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)*, IEEE, 2018, pp. 1537–1540.

[88] Kyung-Ah Shim, "A survey of public-key cryptographic primitives in wireless sensor networks", in: *IEEE Communications Surveys & Tutorials* 18.*1* (2015), pp. 577–601.

[89] Shushan Zhao et al., "A survey of applications of identity-based cryptography in mobile ad-hoc networks", in: *IEEE Communications surveys & tutorials* 14.*2* (2011), pp. 380–400.

[90] Simon Heron, "Advanced encryption standard (AES)", in: *Network Security* 2009.*12* (2009), pp. 8–12.

[91] Ronald L Rivest, Adi Shamir, and Leonard Adleman, "A method for obtaining digital signatures and public-key cryptosystems", in: *Communications of the ACM* 21.*2* (1978), pp. 120–126.

[92] Neal Koblitz, "Elliptic curve cryptosystems", in: *Mathematics of computation* 48.*177* (1987), pp. 203–209.

[93] Victor S Miller, "Use of elliptic curves in cryptography", in: *Conference on the theory and application of cryptographic techniques*, Springer, 1985, pp. 417–426.

[94] Alfred Menezes, "An introduction to pairing-based cryptography", in: *Recent trends in cryptography* 477 (2009), pp. 47–65.

[95] Ritik Bavdekar et al., "Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research", in: *arXiv preprint arXiv:2202.02826* (2022).

[96] Lily Chen et al., *Report on post-quantum cryptography*, vol. 12, US Department of Commerce, National Institute of Standards and Technology . . ., 2016.

[97] Gregg Jaeger, "Classical and quantum computing", in: Springer, 2007, pp. 203–217.

[98] Matthew Edward Briggs, "An Introduction to the General Number Field Sieve", PhD thesis, Virginia Polytechnic Institute and State University, 1998.

[99] Peter W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", in: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (1994), pp. 124–134, DOI: 10.1109/SFCS.1994.365700.

[100] Lov K Grover, "A fast quantum mechanical algorithm for database search", in: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (1996), pp. 212–219.

[101] Abderahman Rejeb et al., "The Internet of Things (IoT) in healthcare: Taking stock and moving forward", in: *Internet of Things* (2023), p. 100721.

[102] Anwar Noureddine Bahache and Noureddine Chikouche, "A comparative analysis of RFID authentication protocols for healthcare applications", in: *2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP)*, IEEE, 2021, pp. 1–6.

[103] Pardeep Kumar, Sang-Gon Lee, and Hoon-Jae Lee, "E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks", in: *Sensors* 12.*2* (2012), pp. 1625–1647.

[104] Debiao He et al., "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks", in: *Multimedia Systems* 21.*1* (2015), pp. 49–60.

[105] Fan Wu et al., "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks", in: *Multimedia Systems* 2.*23* (2017), pp. 195–205.

[106] Chin-Ling Chen, Tsai-Tung Yang, and Tzay-Farn Shih, "A secure medical data exchange protocol based on cloud environment", in: *Journal of medical systems* 38 (2014), pp. 1–12.

[107] Chin-Ling Chen et al., "A privacy authentication scheme based on cloud for medical environment", in: *Journal of medical systems* 38 (2014), pp. 1–16.

[108] Shin-Yan Chiou, Zhaoqin Ying, and Junqiang Liu, "Improvement of a privacy authentication scheme based on cloud for medical environment", in: *Journal of medical systems* 40.*4* (2016), p. 101.

[109] Prerna Mohit et al., "A standard mutual authentication protocol for cloud computing based health care system", in: *Journal of medical systems* 41 (2017), pp. 1–13.

[110] Jangirala Srinivas, Dheerendra Mishra, and Sourav Mukhopadhyay, "A mutual authentication framework for wireless medical sensor networks", in: *Journal of medical systems* 41.*5* (2017), p. 80.

[111] Mohammad Wazid et al., "A novel authentication and key agreement scheme for implantable medical devices deployment", in: *IEEE journal of biomedical and health informatics* 22.*4* (2017), pp. 1299–1309.

[112] Xiong Li et al., "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity", in: *Security and Communication Networks* 9.*15* (2016), pp. 2643–2655.

[113] Ashok Kumar Das et al., "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks", in: *Wireless Personal Communications* 94.*3* (2017), pp. 1899–1933.

[114] Deming Mao et al., "Trusted authority assisted three-factor authentication and key agreement protocol for the implantable medical system", in: *Wireless Communications and Mobile Computing* 2018 (2018).

[115] Chia-Hui Liu and Yu-Fang Chung, "Secure user authentication scheme for wireless healthcare sensor networks", in: *Computers & Electrical Engineering* 59 (2017), pp. 250–261.

[116] Sravani Challa et al., "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks", in: *Computers & Electrical Engineering* 69 (2018), pp. 534–554.

[117] Preeti Soni, Arup Kumar Pal, and SK Hafizul Islam, "An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system", in: *Computer methods and programs in biomedicine* 182 (2019), p. 105054.

[118] Zeeshan Ali et al., "A robust authentication and access control protocol for securing wireless healthcare sensor networks", in: *Journal of Information Security and Applications* 52 (2020), p. 102502.

[119] Guoai Xu et al., "Efficient and Provably Secure Anonymous User Authentication Scheme for Patient Monitoring Using Wireless Medical Sensor Networks", in: *IEEE Access* 8 (2020), pp. 47282–47294.

[120] Ruhul Amin et al., "A robust and anonymous patient monitoring system using wireless medical sensor networks", in: *Future Generation Computer Systems* 80 (2018), pp. 483–495.

[121] Qi Jiang et al., "Efficient end-to-end authentication protocol for wearable health monitoring systems", in: *Computers & Electrical Engineering* 63 (2017), pp. 182–195.

[122] Rifaqat Ali et al., "An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring", in: *Journal of Ambient Intelligence and Humanized Computing* (2018), pp. 1–22.

[123] Yoney Kirsal Ever, "Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks", in: *IEEE systems journal* 13.*1* (2018), pp. 456–467.

[124] Mohammad Wazid, Ashok Kumar Das, and Athanasios V Vasilakos, "Authenticated key management protocol for cloud-assisted body area sensor networks", in: *Journal of Network and Computer Applications* 123 (2018), pp. 112–126.

[125] Geeta Sharma and Sheetal Kalra, "A lightweight user authentication scheme for cloud-IoT based healthcare services", in: *Iranian Journal of Science and Technology, Transactions of Electrical Engineering* 43.*1* (2019), pp. 619–636.

[126] Bander A Alzahrani et al., "A secure and efficient remote patient-monitoring authentication protocol for cloud-IoT", in: *International Journal of Communication Systems* (2020), e4423.

[127] Xin Liu, Ruisheng Zhang, and Mingqi Zhao, "A robust authentication scheme with dynamic password for wireless body area networks", in: *Computer Networks* 161 (2019), pp. 220–234.

[128] Seyed Farhad Aghili et al., "LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT", in: *Future Generation Computer Systems* 96 (2019), pp. 410–424.

[129] Preeti Chandrakar, Sonam Sinha, and Rifaqat Ali, "Cloud-based authenticated protocol for healthcare monitoring system", in: *Journal of Ambient Intelligence and Humanized Computing* 11 (2020), pp. 3431–3447.

[130] Adesh Kumari et al., "Csef: cloud-based secure and efficient framework for smart medical system using ecc", in: *IEEE Access* 8 (2020), pp. 107838–107852.

[131] Mengxia Shuai et al., "Lightweight and secure three-factor authentication scheme for remote patient monitoring using on-body wireless networks", in: *Security and Communication Networks* 2019 (2019).

[132] Mahdi Fotouhi et al., "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT", in: *Computer Networks* 177 (2020), p. 107333.

[133] Chien-Ming Chen et al., "Attacks and solutions for a two-factor authentication protocol for wireless body area networks", in: *Security and Communication Networks* 2021 (2021), pp. 1–12.

[134] Mehedi Masud et al., "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare", in: *IEEE Internet of Things Journal* (2021).

[135] Haqi Khalid et al., "Cross-SN: A Lightweight Authentication Scheme for a Multi-Server Platform Using IoT-Based Wireless Medical Sensor Network", in: *Electronics* 10.7 (2021), p. 790.

[136] Kevin Andrae Delgado-Vargas, Gina Gallegos-Garcia, and Ponciano Jorge Escamilla-Ambrosio, "Cryptographic Protocol with Keyless Sensors Authentication for WBAN in Healthcare Applications", in: *Applied Sciences* 13.3 (2023), p. 1675.

[137] JoonYoung Lee, Jihyeon Oh, and Youngho Park, "A Secure and Anonymous Authentication Protocol Based on Three-Factor Wireless Medical Sensor Networks", in: *Electronics* 12.6 (2023), p. 1368.

[138] Keunok Kim et al., "An Improved Lightweight User Authentication Scheme for the Internet of Medical Things", in: *Sensors* 23.3 (2023), p. 1122.

[139] Maged Hamada Ibrahim et al., "Secure anonymous mutual authentication for star two-tier wireless body area networks", in: *Computer methods and programs in biomedicine* 135 (2016), pp. 37–50.

[140] Xiong Li et al., "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks", in: *Computer Networks* 129 (2017), pp. 429–443.

[141] Abdullah M Almuhaideb and Kawther S Alqudaihi, "A Lightweight and Secure Anonymity Preserving Protocol for WBAN", in: *IEEE Access* 8 (2020), pp. 178183–178194.

[142] Ankur Gupta, Meenakshi Tripathi, and Aakar Sharma, "A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN", in: *Computer Communications* (2020).

[143] Marko Kompara, SK Hafizul Islam, and Marko Hölbl, "A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs", in: *Computer Networks* 148 (2019), pp. 196–213.

[144] Zia Ur Rehman, Saud Altaf, and Saleem Iqbal, "An Efficient Lightweight Key Agreement and Authentication Scheme for WBAN", in: *IEEE Access* 8 (2020), pp. 175385–175397.

[145] Zisang Xu et al., "A lightweight mutual authentication and key agreement scheme for medical Internet of Things", in: *IEEE Access* 7 (2019), pp. 53922–53931.

[146] Mahender Kumar and Satish Chand, "A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network", in: *IEEE Systems Journal* (2020).

[147] Tao Wan et al., "A lightweight continuous authentication scheme for medical wireless body area networks", in: *Peer-to-Peer Networking and Applications* (2021), pp. 1–15.

[148] Aneesh M Koya and PP Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network", in: *Computer Networks* 140 (2018), pp. 138–151.

[149] Shadi Nashwan, "An End-to-End Authentication Scheme for Healthcare IoT Systems Using WMSN", in: *CMC-COMPUTERS MATERIALS & CONTINUA* 68.*1* (2021), pp. 607–642.

[150] Liping Zhang et al., "Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement", in: *IEEE Transactions on Industrial Electronics* 65.*3* (2017), pp. 2795–2805.

[151] Zia ur Rehman et al., "An Efficient, Hybrid Authentication using ECG and Lightweight Cryptographic Scheme for WBAN", in: *IEEE Access* (2021).

[152] Kisung Park et al., "LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme without Verification Table in Medical Internet of Things", in: *IEEE Access* (2020).

[153] Mohammad Amin Rakeei and Farokhlagha Moazami, "Cryptanalysis of an Anonymous Authentication and Key Agreement Protocol for Secure Wireless Body Area Network.", in: *IACR Cryptol. ePrint Arch.* 2020 (2020), p. 1465.

[154] Deepti Singh et al., "Evaluating Authentication Schemes for Real-Time Data in Wireless Sensor Network", in: *Wireless Personal Communications* 114.*1* (2020), pp. 629–655.

[155] Jiaqing Mo, Wei Shen, and Weisheng Pan, "An Improved Anonymous Authentication Protocol for Wearable Health Monitoring Systems", in: *Wireless Communications and Mobile Computing* 2020 (2020).

[156] MF Mridha et al., "An Improved User Anonymous Secure Authentication Protocol for Healthcare System Using Wireless Medical Sensor Network", in: *International Journal of Computing and Digital Systems* 10 (2020), pp. 2–12.

[157] Jiaqing Mo, Zhongwang Hu, and Yuhua Lin, "Cryptanalysis and security improvement of two authentication schemes for healthcare systems using wireless medical sensor networks", in: *Security and Communication Networks* 2020 (2020).

[158] Feifei Wang, Guoai Xu, and Guosheng Xu, "A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map", in: *IEEE Access* 7 (2019), pp. 101596–101608.

[159] DeokKyu Kwon, YoHan Park, and YoungHo Park, "Provably Secure Three-Factor-Based Mutual Authentication Scheme with PUF for Wireless Medical Sensor Networks", in: *Sensors* 21.*18* (2021), p. 6039.

[160] Kyung-Ah Shim, "S2DRP: Secure implementations of distributed reprogramming protocol for wireless sensor networks", in: *Ad Hoc Networks* 19 (2014), pp. 1–8.

[161] David Joseph et al., "Transitioning organizations to post-quantum cryptography", in: *Nature* 605.*7909* (2022), pp. 237–243.

[162] Adarsh Kumar et al., "Securing the future internet of things with post-quantum cryptography", in: *Security and Privacy* 5.*2* (2022), e200.

[163] National Institute of Standards and Technology, *Post-Quantum Cryptography (PQC) Candidates to be Standardized and Round 4*, https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4, [Accessed: April 17, 2023], 2022.

[164] Anwar Noureddine Bahache, Noureddine Chikouche, and Sedat Akleylek, "Securing cloud-based healthcare applications with a quantum-resistant authentication and key agreement framework", in: *Internet of Things* (2024), p. 101200.

[165] Oded Regev, "En celosıas, aprendizaje con errores, códigos lineales aleatorios y criptografıa", in: *Actas del Trigésimo Séptimo Simposio Anual de ACM sobre Teorıa de la Computación, STOC*, vol. 5, 2009, pp. 84–93.

[166] Denisa Greconici, "Kyber on RISC-V", PhD thesis, Master's Thesis, 2020.

[167] Daniel J Bernstein et al., "SPHINCS+ Submission to the NIST post-quantum project", in: *Submission to NIST* (2017).

[168] Joppe Bos et al., "CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM", in: *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2018, pp. 353–367.

[169] Mojtaba Bisheh-Niasar, Reza Azarderakhsh, and Mehran Mozaffari-Kermani, "High-speed NTT-based polynomial multiplication accelerator for CRYSTALS-Kyber post-quantum cryptography", in: *Cryptology ePrint Archive* (2021).

[170] Kevin Bürstinghaus-Steinbach et al., "Post-quantum tls on embedded systems: Integrating and evaluating kyber and sphincs+ with mbed tls", in: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 2020, pp. 841–852.

[171] Ayesha Khalid et al., "Lattice-based cryptography for IoT in a quantum world: Are we ready?", in: *2019 IEEE 8th international workshop on advances in sensors and interfaces (IWASI)*, IEEE, 2019, pp. 194–199.

[172] Noureddine Chikouche, Pierre-Louis Cayrel, Brice Odilon Boidje, et al., "A privacy-preserving code-based authentication protocol for Internet of Things", in: *The Journal of Supercomputing* 75.*12* (2019), pp. 8231–8261.

[173] Jihyeon Ryu et al., "Secure and efficient three-factor protocol for wireless sensor networks", in: *Sensors* 18.*12* (2018), p. 4481.

[174] Diego F Aranha and Conrado PL Gouvêa, *RELIC is an Efficient LIbrary for Cryptography*, 2020, URL: https://github.com/relic-toolkit/relic.

[175] Matthias J. Kannwischer et al., *PQM4: Post-quantum crypto library for the ARM Cortex-M4*, https://github.com/mupq/pqm4.

[176] Cedric Adjih et al., "FIT IoT-LAB: A large scale open experimental IoT testbed", in: *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, IEEE, 2015, pp. 459–464.

[177] Hyun Jung La, Han Ter Jung, and Soo Dong Kim, "Extensible disease diagnosis cloud platform with medical sensors and IoT devices", in: *2015 3rd International Conference on Future Internet of Things and Cloud*, IEEE, 2015, pp. 371–378.

[178] SangCheol Lee et al., "Provably Secure PUF-Based Lightweight Mutual Authentication Scheme for Wireless Body Area Networks", in: *Electronics* 11.*23* (2022), p. 3868.

[179] Abdullah M Almuhaideb and Huda A Alghamdi, "Secure and efficient WBAN authentication protocols for intra-BAN tier", in: *Journal of Sensor and Actuator Networks* 11.*3* (2022), p. 44.

[180] R Meenakshi et al., "Kerberos based Authentication for healthcare application (KAHA) in IoT WBAN", in: *Cardiometry 25* (2022), pp. 186–191.

[181] Qingfeng Cheng et al., "A certificateless authentication and key agreement scheme for secure cloud-assisted wireless body area network", in: *Mobile Networks and Applications* (2022), pp. 1–11.

[182] Javad Alizadeh, Masoumeh Safkhani, and Amir Allahdadi, "ISAKA: Improved Secure Authentication and Key Agreement protocol for WBAN", in: *Wireless Personal Communications* 126.*4* (2022), pp. 2911–2935.

[183] Bhawna Narwal and Amar Kumar Mohapatra, "SAMAKA: Secure and anonymous mutual authentication and key agreement scheme for wireless body area networks", in: *Arabian Journal for Science and Engineering* 46.*9* (2021), pp. 9197–9219.

[184] Abdullah M Almuhaideb and Huda A Alghamdi, "Design of Inter-BAN Authentication Protocols for WBAN in a Cloud-Assisted Environment", in: *Big Data and Cognitive Computing* 6.*4* (2022), p. 124.

[185] J Cohn et al., "Device democracy: Saving the future of the Internet of Things", in: *IBM Institute for Business Value* (2014).

[186] Pradip Kumar Sharma, Young-Sik Jeong, and Jong Hyuk Park, "EH-HL: Effective communication model by integrated EH-WSN and hybrid LiFi/WiFi for IoT", in: *IEEE Internet of Things Journal* 5.*3* (2018), pp. 1719–1726.

[187] Oratile Khutsoane, Bassey Isong, and Adnan M Abu-Mahfouz, "IoT devices and applications based on LoRa/LoRaWAN", in: *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society*, IEEE, 2017, pp. 6107–6112.