

Article

Medical Data in Wireless Body Area Networks: Device Authentication Techniques and Threat Mitigation Strategies Based on a Token-Based Communication Approach

Jan Herbst ^{1,*}, Matthias Rüb ^{1,*}, Sogo Pierre Sanon ¹, Christoph Lipps ¹ and Hans D. Schotten ^{1,2}

- ¹ Intelligent Networks Research Group, German Research Center for Artificial Intelligence, 67663 Kaiserslautern, Germany; sogo_pierre.sanon@dfki.de (S.P.S.); christoph.lipps@dfki.de (C.L.); schotten@rptu.de (H.D.S.)
- ² Institute for Wireless Communication and Navigation, RPTU Kaiserslautern-Landau, 67663 Kaiserslautern, Germany
- * Correspondence: jan.herbst@dfki.de (J.H.); matthias.rueb@dfki.de (M.R.)

Abstract: Wireless Body Area Networks (WBANs), low power, and short-range wireless communication in a near-body area provide advantages, particularly in the medical and healthcare sector: (i) they enable continuous monitoring of patients and (ii) the recording and correlation of physical and biological information. Along with the utilization and integration of these (sensitive) private and personal data, there are substantial requirements concerning security and privacy, as well as protection during processing and transmission. Contrary to the star topology frequently used in various standards, the overall concept of a novel low-data rate token-based WBAN framework is proposed. This work further comprises the evaluation of strategies for handling medical data with WBANs and emphasizes the importance and necessity of encryption and security strategies in the context of sensitive information. Furthermore, this work considers the recent advancements in Artificial Intelligence (AI), which are opening up opportunities for enhancing cyber resilience, but on the other hand, also new attack vectors. Moreover, the implications of targeted regulatory measures, such as the European AI Act, are considered. In contrast to, for instance, the proposed star network topologies of the IEEE 802.15.6 WBAN standard or the Technical Committee (TC) SmartBAN of the European Telecommunication Standards Institute (ETSI), the concept of a ring topology is proposed which concatenates information in the form of a ‘data train’ and thus results in faster and more efficient communication. Beyond that, the conductivity of human skin is included in the approach presented to incorporate a supplementary channel. This direct contact requirement not only fortifies the security of the system but also facilitates a reliable means of secure communication, pivotal in maintaining the integrity of sensitive health data. The work identifies different threat models associated with the WBAN system and evaluates potential data vulnerabilities and risks to maximize security. It highlights the crucial balance between security and efficiency in WBANs, using the token-based approach as a case study. Further, it sets a foundation for future healthcare technology advancements, aiming to ensure the secure and efficient integration of patient data.

Keywords: data exchange; medical data; Wireless Body Area Networks; Human–Body Communication; fully homomorphic encryption; secure data exchange; privacy; security; trust



Citation: Herbst, J.; Rüb, M.; Sanon, S.P.; Lipps, C.; Schotten, H.D. Medical Data in Wireless Body Area Networks: Device Authentication Techniques and Threat Mitigation Strategies Based on a Token-Based Communication Approach. *Network* **2024**, *4*, 133–149. <https://doi.org/10.3390/network4020007>

Academic Editor: Khaled Elleithy

Received: 1 February 2024

Revised: 8 March 2024

Accepted: 3 April 2024

Published: 9 April 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In the context of demographic change, increasing costs of healthcare, and the limited availability of medical professionals worldwide, digitalization in general as well as the developments in the field of networking and communication—in particular Beyond 5G (B5G) and Sixth Generation (6G) wireless systems—are opening up new opportunities. Applications such as Medical Digital Twin (MDT), Holographic Type Communication (HTC) [1],

and Artificial Intelligence (AI) methods offer possibilities for smart data collection, processing, and correlation to simplify and accelerate processes in clinics and medical centers. According to the World Health Organization (WHO) 'digital health, or the use of digital technologies for health has become a salient field of practice for employing routine and innovative forms of Information and Communication Technology (ICT) to address health needs' [2]. Furthermore, connectivity is said to have 'the potential to enhance welfare for individuals' [3]. By the International Telecommunication Union (ITU) account, 76% of the global urban population already have access to the internet (39% in rural environments) [3], emphasizing the potential (and market) for digital health applications. This process is accelerated by the progress and performance of current AI algorithms. In anticipation of this development, the WHO, together with the ITU, launched a focus group on Artificial Intelligence for Health (FG-AI4H) [4] in 2018, intending to define a framework for the use of AI-based methods for health, diagnosis, triage, and treatment decisions. Another relevant aspect in this context will be the European AI Act, which is intended to regulate the use of AI within the European Union (EU). In December 2023, the EU agreed on a provisional version with the EU member states, which, among other things, specifies that AI will be differentiated into four categories (from minimal to unacceptable) founded on a risk-based approach. However, stand-alone AI systems in the area of 'biometric identification and categorization of a natural person' [5] are to be classified as high-risk systems. Therefore, AI and the associated risks are discussed in particular in Section 3.

1.1. Wireless Body Area Networks

One approach to acquire the data necessary for the AI models is the use of so-called Wireless Body Area Networks (WBANs), a near-body, low-power, and short-range wireless communication device to aggregate health, sport, and well-being information. These have already been defined in 2012 in the IEEE Standard for Local and metropolitan area networks Part 15.6: Wireless Body Area Networks [6]. However, the standard is set to be deactivated at the end of March 2023, but the general approach is being further developed and enhanced through several standardization approaches, such as the SmartBAN Technical Committee established by the European Telecommunications Standards Institute (ETSI) in 2013 [7,8], which not only considers wireless communication on but also in the body, with the associated range of medical and health improvements, personal safety, and wellbeing in sport as leisure applications. Furthermore, initiatives such as the one2M2 standard approach, with the visions 'A world of interoperable and secure IoT services...', are addressing issues of health-related Internet of Things (IoT) structures and security [9]. The work described here is based on the WBAN approach, but in contrast to the common star network topology of the deprecated 802.15.6 standard, or that considered in SmartBAN [7] approaches, it proposes the concept of a ring topology that concatenates information and thus distributes computational load while increasing the data transmission rate. Furthermore, adding an additional Human Body Communication (HBC) channel to the system is proposed. This technology utilizes the conductivity of human skin as a complementary communication medium, thereby opening up additional options in terms of security and privacy of the system. The HBC approach plays a crucial role in introducing new sensors into the network and exchanging security information, such as public keys. The HBC also becomes relevant whereas adding additional sensors, as described in Section 2. Based on this described protocol, the security aspect of device authentication is especially evaluated, and therefore ordinary attack vectors such as spoofing or man-in-the-middle attacks can be excluded from the outlet because of the ground-based integrity checking of health-related systems. Authentication and AI-related attack vectors are shown, and countermeasures are presented. By focusing on encryption techniques and threat-mitigation strategies, an analysis of challenges and potential solutions in securing medical data in WBANs is provided. Similar to the AI Act and the high-risk classification of human information, specific requirements also apply to this type of data concerning privacy and security. To take this into account, in addition to standard encryption techniques such as symmetric and

asymmetric methods, homomorphic encryption algorithms are considered, particularly, the ability of distributed- and federated learning and operating on encrypted data. The healthcare sector is a critical infrastructure, so special attention must be paid to protecting the systems. As part of (cyber) resilience strategies, methods for detecting, mitigating, and preventing attacks are particularly relevant here, as are active protective measures to make it as difficult as possible for potential attackers [10].

1.2. Meeting Emerging Healthcare Technology Needs

Within the development of smart, interconnected healthcare-supporting devices, several different approaches are ongoing. Whereas the 802.15.6 WBAN standard is expired, approaches like the ETSI TC SmartBAN, one2M2, or the Alliance for IoT and Edge Computing Innovation (AIOTI) are working on fitting solutions to bring together such technologies.

However, as the frontiers of digital health are pushed, several key areas within a WBAN framework call for enhancement to meet evolving requirements and must be part of the mentioned synchronization processes:

Data Rate Capabilities: The burgeoning integration of Artificial Intelligence (AI) in healthcare necessitates data rates exceeding the current WBAN standard limit of 10 Mbps. AI-driven applications, particularly those demanding real-time processing and instantaneous decision-making, require bandwidths that can accommodate the increased data throughput.

Adaptive Security: The landscape of cyber threats is continuously evolving, rendering static security measures insufficient. WBANs must adopt adaptive security protocols that can dynamically respond to new threats, integrating AI to underpin advanced threat detection and adaptive response mechanisms.

Energy Efficiency: Although the WBAN standard prioritizes low power consumption, there is a pressing need to push beyond the current benchmarks. AI can be pivotal in optimizing power management and tailoring energy usage to user behavior and environmental conditions, thereby extending the wearables' battery life and operational reliability.

Encryption and Privacy: With the proliferation of wearables for health monitoring, safeguarding patient data privacy is of the utmost importance. The adoption of advanced encryption techniques and AI-enhanced privacy measures is essential to bolster defenses against unauthorized access and data breaches.

Interoperability and Personalization: The heterogeneity of devices and systems in the healthcare ecosystem necessitates robust interoperability standards. AI's potential to personalize device functionality to individual user patterns necessitates the WBAN standard to be flexible enough to accommodate diverse AI models and communication protocols.

2. Communication Framework Description

Although different standardization approaches have been established since 2012, recent advancements in AI tools, technological advancements, and the usage or integration into the healthcare sector have increasingly highlighted the significance of on-body sensors. These devices are becoming progressively pivotal for health monitoring and overall well-being, having a growing relevance in contemporary medical practices. It is therefore essential to develop new communication structures that utilize the technologies explored over the last decade while anticipating future advances. Future research therefore should focus on identifying technologies that can be synergistically combined or the ones still needed to fill the existing gaps. In contrast to other standardization approaches like SmartBAN [8], IEEE 802.15.6 [6], mainly focusing on star topologies, the focus in this work for evaluating digital health technologies is based on a multi-hop or token-based communication model, which works comparable to a 'Data train' by concatenating different messages of sensor nodes within the WBAN. To provide a comprehensive understanding of this model, a basic overview is provided. This introduction serves to explain the critical principles and functionalities of this communication protocol and highlight its implications and potential applications in healthcare technology.

2.1. Use Case—The Vision

Like in the aim of different standardization processes, the WBAN system can be used as a continuous health monitor. Therefore, in a concrete example, a patient with hypertension and a high risk for cardiovascular diseases could wear one of these systems to continuously track different vital signs, alerting them and their healthcare providers when anomalies are detected through the use of AI classifiers or specially trained networks. Sensors of different vendors can communicate with each other in a ring topology and exchange information securely. Because information traffic will be distributed through the different sensors through the ring topology, wearing many different sensors will hardly overload the master node, which could be a smartwatch or mobile phone. Through the workload distribution, less energy is needed by each sensor and master node. Through an HBC effortless new sensors can be connected securely if distributed at the patient skin. Grounded on the same protocol a doctor can have access to continuously monitored data of the sensors, whereas the present patient is just touching an HBC-enabled monitor device. Securely, data can be transmitted wirelessly to a hospital server, established through biometric authentication with the help of the WBAN sensors and/or combined with the HBC key exchange.

2.2. Overall Communication Mechanism

The proposed protocol for WBANs focuses on low-latency and efficient communication, implemented on an ESP32-centered Printed Circuit Board (PCB). The ESP-NOW-based protocol diverges from traditional star-like systems by adopting a token-based, multi-hop approach, which distributes the computational load and communication traffic across all devices in the network. This design notably enhances efficiency and reduces energy consumption. Furthermore, the aspect of transmitting information as a kind of ‘wired’ channel over the skin by using capacitive properties is included in the overall concept. Figure 1 illustrates the comprehensive architecture of the proposed low-latency and energy-efficient WBAN protocol. The heart of all sensor nodes is based on an ESP32-S3-Controller implemented on a PCB developed as a sensor carrier. The system employs an ESP-NOW-based protocol that departs from traditional star configurations, effectively distributing computational and communication loads, mimicking a ‘train’ going from sensor node to sensor node accumulating data, which refers to the used description of the ‘data train’. The figure highlights wireless communication paths (blue arrows) originating from the master unit, traversing through each sensor node, aggregating sensor information, and looping back to the master unit. Green arrows indicate the transmission of ‘full packages’ when the maximum packet length of 250 bytes is reached within a cycle. The red dotted lines represent the innovative HBC ‘wired’ channel that utilizes the body’s capacitive properties for a secure, tap-proof data exchange. Finally, the master unit is depicted as a gateway to cloud services and smart hospital systems, with orange arrows denoting external communication pathways.

2.3. Protocol Routine

At the core of the WBAN system is the utilization of the 2.4 GHz ESP-NOW protocol provided and defined by Espressif (<https://www.espressif.com/en/solutions/low-power-solutions/esp-now> (accessed on 1 February 2024)), a latency-optimized 2.4 GHz-based transmission protocol. It facilitates real-time communication between a master unit and a network of sensor nodes, each playing a crucial role in data acquisition and transmission. The master unit, acting as the central controller, orchestrates the network’s communication flow, ensuring synchronized and efficient data handling.

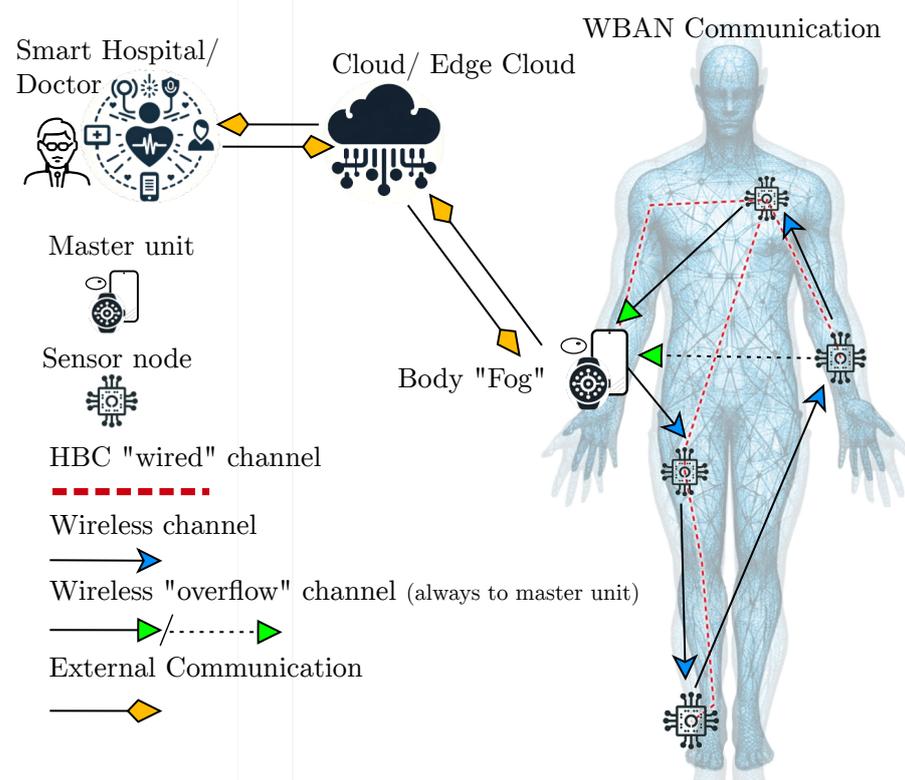


Figure 1. General overview of WBAN. The diagram delineates the wireless communication trajectories (illustrated with blue arrows) that commence at the master unit, extend to each sensor node, collating data, and then return to the master unit. The transmission of 'full packages' is depicted by green arrows, named wireless 'overflow' channel, activated when a cycle reaches the predefined maximum packet size. Furthermore, the red dotted lines define the HBC 'wired' channels, which exploit the body's own capacitive features to create a secure and interception-resistant communication medium. The master unit is portrayed not only as the central node of the WBAN but also as a conduit to broader networks, connecting to cloud infrastructure and healthcare facilities, as indicated by the orange arrows. The design shows a holistic approach of next-generation WBAN systems, ensuring secure, efficient, and scalable health data management.

The overall setup and communication of the protocol consist of three distinct phases, shown in Figure 2:

Initialization: the master unit broadcasts a signal to wake sensor devices from standby mode, transmitting their data (like MAC address, data type, size, and interrogation or query time) to the master.

Pathfinding: In this phase, the master calculates the round-trip time and confirms the successful enlistment of the sensor nodes, laying the groundwork for calculating bus schedules. A bus plan or schedule refers to the master's coordination of which sensor nodes are queried in the next round trip, based on the interrogation or query times previously transmitted by each sensor.

Communication Routine: This phase involves data transmission throughout the network. The communication routine within the WBAN system begins with a broadcast signal from the master unit. This signal contains a 'schedule' or 'plan' for the sensor nodes, informing them about their specific roles in the upcoming data transmission cycle. The plan, encoded in a 16-bit long string, dictates whether and when each sensor node will transmit data during the cycle. This strategic scheduling is crucial for maintaining the system's efficiency and reducing unnecessary data traffic.

After the broadcast, the master unit initiates a unicast communication with the first sensor node. The node then attaches its data, along with a sensor-specific header providing details

about the time and length of the data packet, to the transmitted structure. If the combined data packet does not exceed the 250-byte limit, it is passed on to the next sensor node. Should the limit be exceeded, the packet is sent back to the master unit for processing, and the communication cycle continues with the next sensor node.

The protocol's architecture is primarily designed for low data rates, allowing the combination of data from several sensors into a single message, but also capable of handling larger data packets. This system allows for dynamic flexibility in adding or removing sensor carriers, whereas an accompanying web application provides a bidirectional communication interface. Each sensor node in the WBAN is designed to capture specific medical data, such as vital signs or patient movement. These nodes, equipped with advanced sensors, continuously gather data and remain prepared to transmit this information as per the communication protocol.

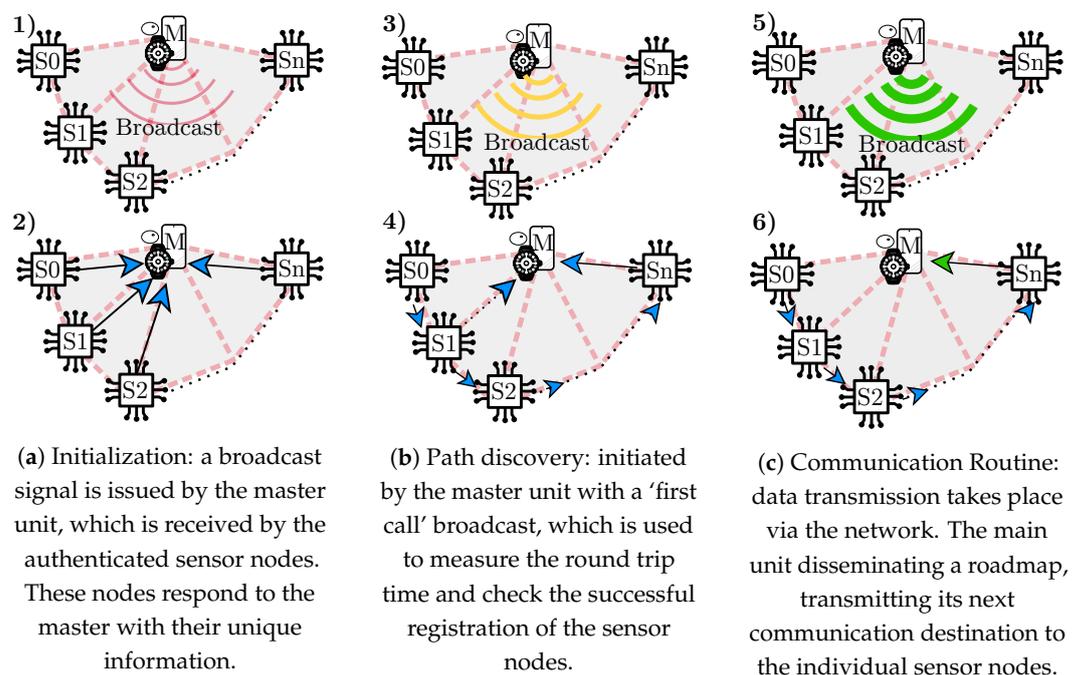


Figure 2. The diagram presented illustrates the token-based communication protocol, which is divided into three integral phases: initialization, path discovery, and communication routine. The red striped lines connecting all devices in the diagram represent the 'wired' HBC connection within the Body Area Network, showcasing a supplementary channel for transmitting broadcast signals between the devices or dedicated messages for each sensor node.

2.4. Human Body Communication

A unique aspect of the WBAN system is the incorporation of HBC. This technology uses the human body as a conduit for transmitting data, offering a secure and efficient method for data exchange. In contrast to conventional wireless transmission methods, this approach utilizes the skin surface as a quasi-wired connection between individual sensor nodes. As a result, there is minimal emission of radiation, effectively eliminating the presence of radio waves that could be intercepted. Consequently, this method intrinsically constitutes a more secure channel for data transmission. HBC is particularly useful in the secure integration of new sensors into the network and the exchange of critical security information, like public keys. This method significantly enhances the security of the data transmission, making it more resilient to external interference and eavesdropping.

2.5. Security and Data Integrity

Although the primary focus of the WBAN system is efficient data transmission, security and data integrity are paramount. The system offers a ground for the discussion of

sophisticated algorithms and encryption techniques to protect data during transmission as a general example in the On-Body health sector. This includes measures to verify data integrity and authenticity, ensuring that the medical information transmitted is both accurate and secure from unauthorized access.

The combination of ESP-NOW protocol efficiency, strategic data transmission scheduling, and the HBC method makes the WBAN system a robust and promising framework for medical data communication. It addresses key challenges in digital healthcare, such as real-time monitoring, data security, and efficient resource utilization, making it an indispensable technology in modern healthcare infrastructure.

3. Security Aspects Regarding Wireless Body Area Framework

WBANs are playing an important role in healthcare by enabling real-time monitoring and treatment delivery. However, the inherent resource constraints of WBAN devices pose significant challenges in securing communication against malicious attacks. Integrating security measures faces various challenges. In addition to the limited resource aspect, which makes it difficult to implement robust security protocols without draining device batteries, the dynamic nature of WBANs, with devices frequently joining or leaving, requires efficient key management and authentication mechanisms. Interference and changing channel conditions further complicate security, necessitating resilient protocols. WBANs often handle sensitive health data, highlighting the need for strong encryption, privacy safeguards, and regulatory compliance.

IEEE 802.15.6 [6], a standardized protocol for WBAN communication, has been shown to have inherent insecurities, including impersonation attacks and lack of forward secrecy, forward secrecy meaning that even if a key used to establish a secure connection is compromised, past or future sessions will not be vulnerable [11]. These vulnerabilities come from the authentication procedure employed by IEEE 802.15.6. We focused on addressing these vulnerabilities, as a strong device authentication mechanism will limit unauthorized access and prevent malicious actors from having access to the WBAN system, and attack scenarios like DoS and data tampering become obsolete.

3.1. Security of IEEE 802.15.6 Protocols

The IEEE 802.15.6 standard provides three security levels: Unsecured Communication Level, Authentication Level, and Authentication and Encryption.

- **Unsecured Communication Level:** This is the least-secure level, where data are transmitted through unsecured frames. This lacks mechanisms for data authentication, integrity, confidentiality, and privacy protection.
- **Authentication Level:** An intermediate security level where data are transmitted through secured authentication without encryption. This level does not support confidentiality or privacy.
- **Authentication and Encryption Level:** The highest security level involves authenticated and encrypted frame transmission. It addresses security concerns not covered by the previous lower security levels.

During the association process of the master unit and sensor node, one of the security levels is chosen. Unicast secured communication activates a Master Key (MK), which can be pre-shared or established through unauthenticated association. A Pairwise Temporal Key (PTK) is then created for a single session. For multicast secured communication, a Group Temporal Key (GTK) is shared with the corresponding group via the unicast method.

It is important to note that, given the sensitivity of the data gathered by WBANs, using unsecured communication and authentication levels is impractical. The focus should solely be on the authentication and encryption levels. However, vulnerabilities have been identified in this approach, primarily from the pre-sharing or establishment of the MK through unauthenticated association [11]. The use of unauthenticated pre-shared or established MKs comes from the limitations of certificate-based authentication, which, although effective in traditional networks, proves unsuitable for WBANs. These limitations

arise from the resource constraints nature of WBAN devices, particularly their limited computational power and memory capacity. In this work, different authentication methods are explored.

3.2. Authentication and Key Agreement

As mentioned above, certificate-based authentication, whereas effective in traditional networks, is not well-suited for WBANs due to the limited computational capabilities and memory resources of WBAN devices. The overhead associated with certificates, including their creation, distribution, and storage, can significantly impact the performance and efficiency of WBANs [12]. Authentication is essential in ensuring that only authorized devices are being connected to the WBAN. To address these limitations, alternative authentication mechanisms that are more lightweight and resource-efficient are explored.

3.2.1. Physical Unclonable Functions

One promising approach involves the use of Physical Unclonable Functions (PUFs) [13,14]. PUFs are unique physical characteristics of electronic devices that can be used to generate cryptographic keys. They exploit the inherent and unavoidable variations that occur during the manufacturing of semiconductor circuits. The randomness and uniqueness of PUF-derived keys make them suitable for authentication in WBANs without the need for certificates [15]. In the system in Figure 1, the authentication between the master unit and a sensor node operates on a challenge–response mechanism. The device being authenticated, the sensor node, is challenged with a set of known input values (challenges), and the corresponding responses are recorded in the master unit. This database of challenges and responses is called a Challenge-Response Pair (CRP). During the authentication, the sensor node is challenged by the master node which then generates a response and compares it to the stored CRPs. If the response is close enough to a stored one, the device is deemed to be authentic. PUF authentication is secure because it is based on the physical characteristics of the device itself. These characteristics are unique to each device and cannot be replicated. Therefore, it is very difficult for an attacker to forge a PUF response. Physical Layer Security, in general, is a promising approach to enhancing the security of resource-constrained devices [16].

3.2.2. Use of Implicit Certificates

Conventional public key certificates consist of three elements: identification data, a public key, and a digital signature that binds the public key to the ID data and confirms that this binding has been verified by a trusted authority, typically a Certificate Authority (CA). Implicit certificates (ICs) deviate from this structure by eliminating the explicit public key and digital signature [17]. An IC comprises only identification data and cryptographic data, which serve as the foundation for deriving the IC's public key. The private key linked to this public key is exclusively held by the entity identified in the IC. The process of deriving the public key also encompasses validating the IC, since a public key derived from an invalid IC would imply the existence of an undiscovered private key. This leads to a crucial conclusion: an IC cannot be forged unless the CA's private key is exposed. The absence of a digital signature contributes to the IC's smaller size. Elliptic Curve Qu-Vanstone (ECQV) cryptography is an implicit certificate scheme that is based on elliptic curve cryptography. It optimizes cryptographic operations and could suit the resource-constrained nature of WBAN devices [18]. Leveraging the inherent efficiencies of elliptic curve cryptography, ECQV can be embedded in resource-constrained WBAN devices to provide more efficient authentication schemes.

3.2.3. Symmetric Cryptographic-Based Authentication

In addition to PUFs and ECQV, symmetric cryptographic-based authentication mechanisms are also suitable for WBANs [19]. Symmetric key-based authentication proposed in [19] is lightweight and efficient and is also suitable for post-quantum deployment scenarios.

The emergence of quantum computers poses a significant threat to traditional asymmetric cryptographic algorithms, including those employed for WBAN communication like ECQV [20]. As quantum computers gain computational power, they will be able to break the encryption used in these algorithms, rendering WBANs vulnerable to eavesdropping and tampering. To safeguard WBAN security in the face of quantum computing, alternative authentication mechanisms that are resilient to quantum attacks are being developed [21–23].

The development of these alternative authentication mechanisms has significantly enhanced the security of WBAN communication. By addressing the inherent vulnerabilities of IEEE 802.15.6 and leveraging novel authentication techniques, WBANs can provide a secure and reliable platform for healthcare applications.

3.2.4. Biometrics

For WBAN, biometric authentication introduces a novel dimension of security by ensuring the alignment of the right user with the correct device [24]. This method employs unique biological, physiological, or behavioral characteristics like fingerprints, voice patterns, retinal scans, or more advanced technologies like the use of gait, ECG, or EEG [25]. It transcends the limitations of traditional device authentication, which focuses solely on the device's trustworthiness to a more holistic view. The integration of biometric authentication is particularly vital in healthcare applications, where the security and accuracy of medical data are paramount. Biometrics offer a robust layer of security, as these personal traits are inherently difficult to replicate or forge, compared to conventional passwords or PINs [26]. However, this enhanced security comes with its own set of challenges and privacy concerns. The collection and management of biometric data necessitate stringent protection measures and compliance with privacy regulations to prevent misuse or unauthorized access. Implementing biometric systems in WBANs also involves balancing the complexity and computational demands of these systems against the energy efficiency of wearable devices. Innovations such as lightweight biometric algorithms and energy-efficient data transmission methods are essential to addressing these concerns. As technology evolves, it is expected that biometrics will become increasingly integral to enhancing the security and functionality of WBAN systems, especially in the sensitive domain of healthcare [27].

3.3. Data Transmission

Once authentication between the different entities of the WBAN has been established, communication and data transmission can proceed securely. This involves employing robust encryption, integrity, and message authentication mechanisms.

Traditional encryption algorithms like Advanced Encryption Standard (AES), AES-GCM (Galois/Counter Mode), AES-CCM (Counter with CBC-MAC), Hash-Based Message Authentication Code (HMAC), and Cipher-based Message Authentication Code (CMAC) have been widely used for WBAN communication. These algorithms provide strong encryption and message authentication to protect against unauthorized access and data tampering [6,11].

3.3.1. ASCON

ASCON is a lightweight cryptographic standard with authenticated encryption with associated data (AEAD) designed for efficient implementation in various constrained environments, including IoT devices, embedded systems, and low-power devices like those commonly found in WBANs [28]. In 2023, NIST declared ASCON the US standard for lightweight cryptography. It is notable for its simplicity, security, and speed, making it suitable for resource-constrained environments [29]. It provides both authenticated encryption (ensuring confidentiality and integrity) and the ability to handle associated data, which are additional pieces of information not directly encrypted but are authenticated alongside the encrypted message.

3.3.2. Fully Homomorphic Encryption

Fully Homomorphic Encryption (FHE) represents a novel cryptographic technique that enables computations to be performed directly on encrypted data without requiring decryption [30]. FHE is still in its early stages of development, but its potential is immense. For instance, it could enable WBAN devices to perform advanced data analysis and processing without compromising patient privacy. Additionally, FHE could facilitate secure collaboration among healthcare providers, allowing them to share and analyze patient data without compromising confidentiality. However, FHE's computational complexity has been a significant hurdle. The processing demands for performing computations on encrypted data are substantially higher. This is expected to not be a hurdle as FHE is projected to be fast enough by 2025 for most use cases [31].

3.4. Special Consideration

This section discusses specialized considerations vital to optimizing the security and functionality of WBANs. It highlights strategies to address unique challenges in data collection, physical layer attacks, and system integrity within the network.

3.4.1. Data Collection

The communication within the WBAN relies on efficient communication protocols to ensure seamless data transmission while minimizing unnecessary traffic. This is achieved by employing cyclical data transmission methods. In case this is conducted by merely concatenating previously collected encrypted information, the final ciphertext may carry patterns from the same plaintext (from different nodes), and the same repetitive part-blocks of ciphertext can emerge, making the encryption not semantically secure and vulnerable to Chosen Plaintext Attack (CPA).

To prevent these attacks, the data that are concatenated with the previous data must be encrypted using a different initialization vector each time. Another approach to preventing such vulnerability is the encryption of the entire message each time data are collected from a node.

3.4.2. Human–Body Communication as Security Enhancer

HBC, by using the human body as a medium for data transmission, presents an innovative way to augment WBAN security. It is particularly effective for the secure transmission of encryption keys within the WBAN, utilizing the physical proximity required for communication as a natural security measure. However, HBC's utility is inherently limited by its short-range capability, confining its application to scenarios where devices maintain close physical contact.

3.4.3. Physical Layer Attacks

Utilizing HBC for secure, short-range communication enhances security at the physical layer but is limited in range and dependent on the physical proximity of devices. In securing a WBAN system, particularly for healthcare applications, a multi-layered, sophisticated approach is required. This approach must carefully balance the need for strong encryption to protect sensitive health data with practical considerations of system performance, energy consumption, and user experience. The integration of HBC adds an innovative layer of security, particularly useful for key exchange and device authentication within the network. Selecting specific encryption methods and security strategies must align with the WBAN's operational requirements, considering the nature of the data, the computational capabilities of the network devices, and the overall system architecture. This balance is crucial in ensuring that the WBAN not only remains secure but also functional and user-friendly. A basic overview of added security, benefits, and considerations across the WBAN protocol is given in Table 1.

Table 1. Authentication mechanisms across WBAN communication channels.

Communication Channel	Physical Unclonable Functions	Implicit Certificates	Symmetric Crypto-Based Auth.	Biometrics
HBC Channel	Ideal for device auth.; high security	Limited by proximity	Suitable for key exchange	Effective for user auth.
Wireless Cyclic Channel	Enhances device fingerprinting; adds complexity	Suitable for trust chains	Optimal for data in transit	Feasible for user auth.
Edge Device Channel	Useful for device fingerprinting	Critical for secure network interactions	Standard for data protection	User verification before data exit

The integration of authentication mechanisms and other security measures discussed earlier can effectively address security threats in WBANs, as outlined in [32]. These include service interruption, data interception, and tampering, as well as user, hardware, and software attacks. To further enhance security, intrusion detection systems can be deployed. These systems swiftly detect and respond to anomalies, preventing service disruptions, unauthorized access, and data breaches such as DoS attacks or tampering. By continuously monitoring network activity, intrusion detection systems help preemptively address vulnerabilities, ensuring the integrity and confidentiality of WBAN data.

4. Securing Artificial Intelligence Accompanying the WBAN

In future clinical environments, it is expected that an increasing number of multimodal patient data will be automatically consolidated and analyzed. Such holistic systems, which are expected to support the work of clinical personnel, are particularly enabled by advances in the field of artificial intelligence. Apart from the support in terms of decision-making and diagnosis within the WBAN, which provides multiple attack surfaces for outside attackers, AI can also be used as a defense mechanism. The latter is discussed briefly, concerning the limited computation power of WBAN sensors.

Intrusion detection for networks is a particularly complex task that is often tackled via deep learning techniques [33,34], whereas there are some efforts regarding IoT environments, the limited computational power of the sensors and sensor carriers prevent the efficient implementation of large deep learning models with multiple hidden layers or sophisticated architectures. Recurrent neural networks are an especially successful technology for intrusion detection but require massive computational overhead not feasible for IoT systems [33].

More suitable for intrusion detection regarding the computational complexity within the WBAN are machine learning methods as proposed in several recent works, e.g., Support Vector Machines [35–37]. Alsubaie et al. present an intruder detection system specifically designed for WBANs based on Decision Trees which, if the employed sensors produce data with only little noise, can outperform Neural Networks [38].

In the following, the AI applications within the WBAN are discussed. These can be used for diagnosis and therapy recommendations, but offer attack vectors for intruders. Thus, there is a conflict of interest between the potential diagnosis and therapy recommendation improvements, which directly benefit the individual patient and data security and privacy concerns. Those are both addressed, for instance, by the EU in the General Data Protection Regulation (GDPR) [39] and the European AI Act [5]. The GDPR does not specifically discuss WBANs but still contains implications. With the scope of holistic, global AI frameworks, there could be issues that are not yet fully addressed by regulatory frameworks, One principle is the purpose limitation, which might limit the use of collected patient data to benefit an individual patient. This contradicts the idea of AI models that benefit from many different datasets from several locations. Whether the potential diagnosis and treatment benefits outweigh privacy concerns will be an ongoing discussion as AI increases in performance in the future.

Depending on which layer within the WBAN clinic infrastructure artificial intelligence is deployed, different security requirements arise. An overview of the application layers of AI and most anticipated attack vectors are shown in Figure 3. In the following, the role of AI on each layer, as well as the most prominent attack vectors, are discussed. Especially in the advent of the AI Act of the European Union, it is necessary to understand, assess, and mitigate underlying risks, as the data in the healthcare sector are always considered confidential.

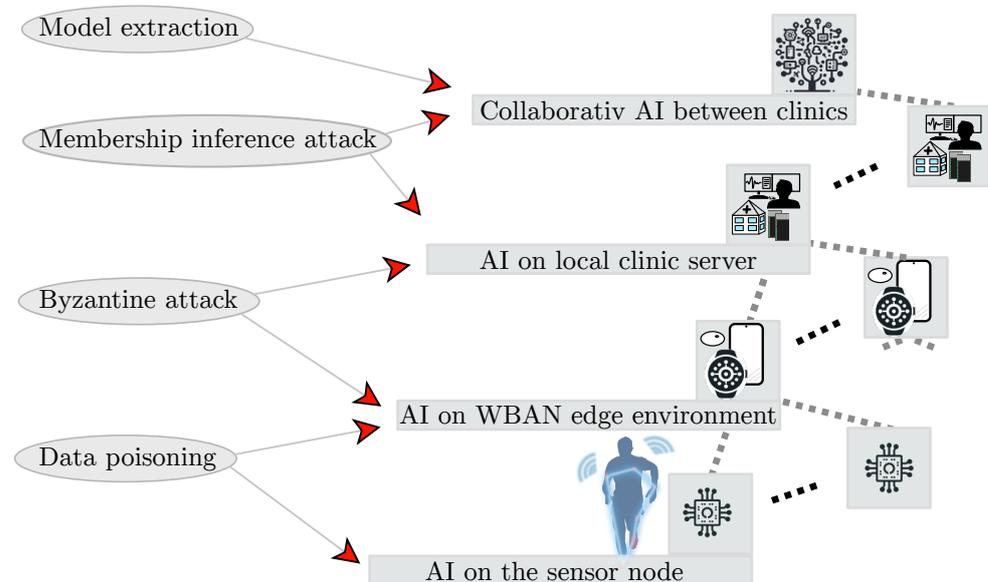


Figure 3. AI abstraction levels concerning WBAN systems in the healthcare structure, from bottom to top: AI models and threats on sensor nodes, WBAN edge devices, each with their own set of sensor nodes, local clinic servers, and AI models spanning different clinics.

4.1. AI on the Sensors within the WBAN

Possible tasks for artificial intelligence directly at the sensor include the preprocessing, pruning, and general orchestrating of the data acquisition. In general, it should be considered that the on-sensor computing power is extremely low.

For an assessment of security requirements in this context, a distinction needs to be made between two cases:

Case A: The AI is specialized only for a single sensor and its vital parameters. Accordingly, the AI system operates locally on a computing unit at the sensor directly with the raw data captured by the sensor. In this case, no further security measures are necessary since the AI performs onboard preprocessing. For the transmission of the processed data by AI, encryption can again be employed, although it is not relevant for the on-sensor AI.

Case B: The AI system on the sensor collaborates with similar systems on other sensors either by sharing network parameters directly in the context of distributed learning of artificial neural networks or by adjusting itself based on contextual information deduced by other networks within the WBAN [40].

In general, due to the low computational power of the sensor carriers within the WBAN, it is expected to be more feasible to employ crucial AI functionalities on the first reachable edge computing instance within the clinic but outside the WBAN. The most relevant adversarial attack vector for AI on the sensor in machine learning will most likely be data poisoning [41]. An attacker tries to maliciously infuse data to invoke a specific output of the AI, e.g., suppressing features that might indicate diseases resulting in a wrong diagnosis for the specific patient. In the described multi-hop setup, the prevention of man-in-the-middle attacks is of particular importance, as each sensor receives from another sensor and sends data to another [42].

4.2. AI on Edge Environment of WBANs

In addition to the computationally weak master unit, there would be another edge device within the clinic, e.g., B. a smartphone, the first that could use the multimodal data to make deductions that can include critical information like stroke and fall detection of patients. Another application of AI in this position would be controlling the workflow within the WBAN, e.g., through fault prediction [43]. In this case, it is crucial that intact information can be received from the local networks within the WBAN as well as the encrypted raw data. Here, it needs to be considered whether there is an advantage in periodically transmitting additional network parameters or gradients from neural networks directly to the sensors to make further deductions within a framework of collaborative learning, or if this would compromise real-time functionality. In the latter case, local networks may only engage in preprocessing but cannot be integrated into a collaborative system. This step can still be taken over by an edge device that already has access to the complete multimodal dataset of individual sensors. Hereby, the authentication of the participating sensors is crucial, as a 'byzantine' sensor might infuse malicious data, changing the output of the AI, e.g., to alter the diagnosis of the patient. In this context, the authentication of individual WBAN sensors is crucial, yet it should involve as little effort as possible from the clinical staff. In particular, additional sensors must be easily integrated into the multi-hop network described in Figure 1 using plug and play. A possible solution could be HBC, which is described in Section 3.4.2.

4.3. AI on a Local Clinic Server

Central AI models within a clinic, for instance, receive vital data from multiple WBANs belonging to different patients, thereby aiding in diagnosis and therapy selection. Additionally, the integration of other modalities, such as data from additional examinations like MRI and EEG for an individual patient, is expected to enhance the performance of such systems. Such a model could operate locally within the clinic, ensuring that patient raw data do not leave the premises and can only be intercepted on the path from data acquisition to the clinic server. Currently, the usage of multimodal data, especially when different data are available for some patients, is under ongoing investigation [44]. On such a local basis, the AI would still be prone to byzantine attacks, as malicious data (e.g., wrongly labeled) could impede the training process. Another attack on the clinic server could be a membership inference attack. The goal of such an attack is to find information about which patient's data were part of the training set of AI on the clinic server, which already reveals sensitive information [45].

4.4. Collaborative AI between Clinics

Newer holistic visions, and especially advances in artificial intelligence, suggest that automated diagnosis and therapy selection can be significantly improved when clinics collaborate. Particularly with rare medical conditions, there is a likelihood that a local neural network from a single clinic may not be able to assist in the diagnosis. The situation changes when working with patient data from other clinics. An approach for this scenario is the machine learning method of Federated Learning (FL), which allows the training of a global AI model without the exchange of raw data between local models [40].

Note that this does not fully solve the privacy issue, as even model weights contain sensitive information, therefore allowing privacy attacks [46].

For secure aggregation of the results of the distributed global models into the global model, multiple approaches have been proposed [47,48]. In its simplest form, such an algorithm computes the average of the model parameters and gradients of the local models [40].

To prevent information about the raw data contained in the training datasets from flowing to other partners in this collaborative network, random noise is added to the model updates in the context of Differential Privacy Average Aggregation before merging [49]. It is important to find the right compromise between the precision of the model and the

privacy of individual models, since in the use case of collaboration between networks responsible for diagnosis and treatment selection, both aspects are crucial.

FL introduces unique challenges compared to traditional centralized machine learning approaches. The decentralized nature of FL raises concerns about privacy, robustness, and communication efficiency.

Regarding the intention of an attacker on the WBANs data, there are multiple possible targets: (A) Extracting information about the types of vital data acquired at a specific patient or even accessing information about the health state itself. (B) Altering information (network parameters or data) to change the diagnosis output. That way a neural network could be tricked into classifying a terminally ill person as healthy, preventing them from receiving necessary treatment. This could be conducted by entering a contaminated dataset into the network which will hamper the performance of the network. This process is known as data poisoning [41]. Alternatively, in the context of FL, local models could feed malicious gradients or parameters to the main network [50]. State-of-the-art systems employ robust gradient aggregation techniques to mitigate the influence of such ‘byzantine’ contributions to the main network. Unfortunately, in the specific use case of rare disease treatment, a real dataset might be classified as malicious, as seemingly similar datasets have been classified as healthy so far. The goal of the global model is precisely to accept such rare cases and, considering multiple instances over an extended period, identify new patterns enabling the diagnosis of rare diseases. To address these challenges, there are various approaches that imply specific drawbacks in the discussed context.

(A) Differential Privacy: Adding random noise to the shared model parameters increases protection against information leakage and reconstruction attacks. This has to be conducted very carefully as additional noise might impede the accuracy of the final model. Therefore, a suitable tradeoff between security and accuracy needs to be found [51].

(B) Secure Multi-Party Computation (SMPC): Utilizing cryptographic protocols to enable secure aggregation of local model updates without revealing sensitive information. This is achievable in the future, for instance, by using homomorphic encryption, as mentioned in Section 3.

(C) Federated Averaging with Robustness: Incorporating techniques such as Byzantine fault tolerance to ensure the integrity of model updates and prevent manipulation by malicious participants. This implies the aforementioned issue of false positives of malicious attacks for rare disease data.

Since vital data of an individual are already aggregated within the WBANs, there is the possibility of biometric authentication [25,52]. Artificial neural networks are used to recognize patterns in vital data, which, although often not providing secure authentication on their own, could at least support an automated intrusion-detection system. Note that even though intrusion detection is present, it can still be prone to model extraction attacks, which seek to gain information about the used AI model or its parameters [53]. If an attacker tries to infuse malicious data, the context of the multimodal data stream could enable the detection of malicious datasets as outliers, thereby preventing data poisoning.

5. Conclusions

This research has provided an in-depth exploration of the security and efficiency challenges in modern Wireless Body Area Networks (WBANs), particularly focusing on a token-based communication approach for enhancing device authentication and mitigating threats. This study has looked into the integration of Human–Body Communication (HBC) as an innovative security enhancer, leveraging the physical properties of the human body for secure data transmission. By implementing unequivocal device authentication, a range of common attack vectors can be pre-emptively mitigated. Utilizing the introduced framework in conjunction with HBC and the described security protocols, overall security can be significantly enhanced. Furthermore, the role of Artificial Intelligence (AI) in WBANs is discussed, highlighting the potential of AI in optimizing system performance and addressing security concerns. The exploration of AI across various layers of the WBAN,

from sensors to clinic servers, underlines the importance of robust security measures in safeguarding sensitive medical data against emerging cyber threats. Additionally, the implications of the European AI Act on WBAN systems have been considered, emphasizing the need for compliance with evolving regulatory frameworks.

Especially in the context of the rapidly advancing healthcare technologies and further developments regarding ‘beyond 5G’ and 6G, adaptive, efficient, and secure WBAN systems are of great importance. The proposed token-based approach, complemented by AI integration and advanced security measures such as HBC, paves the way for future innovations in healthcare technology, ensuring patient data are both secure and seamlessly integrated into medical care. In future work, the incorporated communication framework in combination with an HBC channel will be used to integrate the proposed encryption methods alongside the ring topology. The aim is to evaluate the system, regarding overall security, energy consumption, and applicability.

Author Contributions: Conceptualization, J.H. and M.R.; methodology, J.H., M.R. and S.P.S.; investigation, S.P.S., J.H. and M.R.; resources, S.P.S., J.H. and M.R.; writing—original draft preparation, J.H., M.R., S.P.S. and C.L.; writing review and editing, J.H., S.P.S. and M.R.; visualization, J.H.; supervision, H.D.S.; project administration, M.R., J.H., C.L. and H.D.S.; funding acquisition, C.L., M.R., J.H. and H.D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been supported by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennezeichen 16KISK003K, Open6GHub and 16KISK214, 6G-Health). The authors alone are responsible for the content of this article.

Data Availability Statement: Data sharing not applicable—no new data generated.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Akyildiz, I.; Guo, H. Holographic-Type Communication: A New Challenge for the Next Decade. *ITU J. Future Evol. Technol.* **2022**, *3*, 421–442. [CrossRef]
2. WHO. *WHO Guideline Recommendations on Digital Interventions for Health System Strengthening*; National Library of Medicine, National Center for Biotechnology Information: Bethesda, MD, USA, 2019. Available online: <https://www.ncbi.nlm.nih.gov/books/NBK541905/> (accessed on 16 January 2024).
3. International Telecommunication Union—Development Sector. *Global Connectivity Report 2022*. ISBN: 978-92-61-33551-9. Available online: https://www.itu.int/dms_pub/itu-d/opb/ind/d-ind-global.01-2022-pdf-e.pdf (accessed on 16 January 2024).
4. Salathè, M.; Wiegand, T.; Wenzel, M. Focus Group on Artificial Intelligence for Health. 2018. Available online: <https://arxiv.org/pdf/1809.04797.pdf> (accessed on 16 January 2024)
5. European Commission. *Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*; European Commission: Luxembourg, 2021.
6. *IEEE802.15.6*; IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks. IEEE Computer Society: Washington, DC, USA, 2012; ISBN 9780738172064. [CrossRef]
7. Hamalainen, M.; Paso, T.; Mucchi, L.; Girod-Genet, M.; Farserotu, J.; Tanaka, H.; Chin, W.H.; Ismail, L.N. ETSI TC SmartBAN: Overview of the wireless body area network standard. In *Proceedings of the 2015 9th International Symposium on Medical Information and Communication Technology (ISMICT)*, Kamakura, Japan, 24–26 March 2015; pp. 1–5. [CrossRef]
8. Hamalainen, M.; Mucchi, L.; Girod-Genet, M.; Paso, T.; Farserotu, J.; Tanaka, H.; Anzai, D.; Pierucci, L.; Khan, R.; Alam, M.M.; et al. ETSI SmartBAN Architecture: The Global Vision for Smart Body Area Networks. *IEEE Access* **2020**, *8*, 150611–150625. [CrossRef]
9. Ennesser, F.; Shah, Y. Security Solutions and Services for the IoT, oneM2M IoTing Series. Available online: https://www.onem2m.org/images/images/files/oneM2M_Security_Briefing_A4.pdf (accessed on 16 January 2024).
10. Lipps, C.; Tjabben, A.; Rüb, M.; Herbst, J.; Sanon, S.P.; Reddy, R.; Munoz, Y.; Schotten, H.D. Designing Security for the Sixth Generation: About Necessity, Concepts and Opportunities. In *Proceedings of the 22nd European Conference on Cyber Warfare and Security (ECCWS2022)*, Athens, Greece, 22–23 June 2023. [CrossRef]
11. Toorani, M. On vulnerabilities of the security association in the IEEE 802.15. 6 standard. In *Proceedings of the Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable*, San Juan, Puerto Rico, 30 January 2015; Revised Selected Papers; Springer: Berlin/Heidelberg, Germany, 2015; pp. 245–260.
12. Li, X.; Ibrahim, M.H.; Kumari, S.; Sangaiah, A.K.; Gupta, V.; Choo, K.K.R. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. *Comput. Netw.* **2017**, *129*, 429–443. [CrossRef]

13. Wallrabenstein, J.R. Practical and secure IoT device authentication using physical unclonable functions. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 99–106.
14. Lipps, C.; Weinand, A.; Krummacker, D.; Fischer, C.; Schotten, H.D. Proof of Concept for IoT Device Authentication Based on SRAM PUFs Using ATMEGA 2560-MCU. In Proceedings of the 2018 1st International Conference on Data Intelligence and Security (ICDIS), South Padre Island, TX, USA, 8–10 April 2018; pp. 36–42. [CrossRef]
15. Nyangaresi, V.O.; Rodrigues, A.J.; Al Rababah, A.A. Secure Protocol for Resource-Constrained IoT Device Authentication. *Int. J. Interdiscip. Telecommun. Netw. (IJITN)* **2022**, *14*, 1–15. [CrossRef]
16. Mucchi, L.; Jayousi, S.; Caputo, S.; Panayirci, E.; Shahabuddin, S.; Bechtold, J.; Morales, I.; Stoica, R.A.; Abreu, G.; Haas, H. Physical-Layer Security in 6G Networks. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1901–1914. [CrossRef]
17. Sciancalepore, S.; Capossele, A.; Piro, G.; Boggia, G.; Bianchi, G. Key management protocol with implicit certificates for IoT systems. In Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, Florence Italy, 18 May 2015; pp. 37–42.
18. Ha, D.A.; Nguyen, K.T.; Zao, J.K. Efficient authentication of resource-constrained IoT devices based on ECQV implicit certificates and datagram transport layer security protocol. In Proceedings of the 7th Symposium on Information and Communication Technology, Ho Chi Minh, Vietnam, 8–9 December 2016; pp. 173–179.
19. Khan, H.; Dowling, B.; Martin, K.M. Highly efficient privacy-preserving key agreement for wireless body area networks. In Proceedings of the 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), New York, NY, USA, 1–3 August 2018; pp. 1064–1069.
20. Sanon, S.P.; Alzalam, I.; Schotten, H.D. Quantum and Post-Quantum Security in Future Networks. In Proceedings of the IEEE Future Networks World Forum 2023, Baltimore, MD, USA, 3–15 November 2023. Available online: https://www.researchgate.net/publication/375665731_Quantum_and_Post-Quantum_Security_in_Future_Networks (accessed on 19 January 2024).
21. Chen, A.C. PQCMC: Post-Quantum Cryptography McEliece-Chen Implicit Certificate Scheme. *arXiv* **2023**, arXiv:2401.13691.
22. Seyhan, K.; Nguyen, T.N.; Akleylek, S.; Cengiz, K. Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: A survey. *Clust. Comput.* **2022**, *25*, 1729–1748. [CrossRef]
23. Charjan, S.; Kulkarni, D. Quantum Key Distribution by Exploitation Public Key Cryptography (ECC) in Resource Constrained Devices. *Int. J. Emerg. Eng. Res. Technol.* **2015**, *3*, 5–12.
24. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. *Cryptography* **2018**, *2*, 1. [CrossRef]
25. Herbst, J.; Petershans, J.; Rüb, M.; Lipps, C.; Beck, A.K.; Carmo, J.C.; Lachmann, T.; Schotten, H.D. Inception Based Deep Learning: Biometric Identification Using Electroencephalography (EEG). In Proceedings of the 2023 International Symposium on Networks, Computers and Communications (ISNCC), Doha, Qatar, 23–26 October 2023; pp. 1–7. [CrossRef]
26. Herbst, J.; Bergkemper, L.; Petershans, J.; Shobairian, S.; Rüb, M.; Lipps, C. Body Area Networks in the Era of 6G: An Evaluation of Modern Biometrics regarding Multi-Factor-Authentication. In Proceedings of the Workshop on Next Generation Networks and Applications (NGNA 2022), Kaiserslautern, Germany, 8 December 2022.
27. Cornet, B.; Fang, H.; Ngo, H.; Boyer, E.W.; Wang, H. An Overview of Wireless Body Area Networks for Mobile Health Applications. *IEEE Netw.* **2022**, *36*, 76–82. [CrossRef]
28. Dobraunig, C.; Eichlseder, M.; Mendel, F.; Schläffer, M. Ascon v1.2: Lightweight authenticated encryption and hashing. *J. Cryptol.* **2021**, *34*, 33. [CrossRef]
29. Turan, M.S.; McKay, K.; Chang, D.; Bassham, L.E.; Kang, J.; Waller, N.D.; Kelsey, J.M.; Hong, D. *Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process*; NIST Internal Report NIST IR 8454; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023. [CrossRef]
30. Gentry, C. Fully homomorphic encryption using ideal lattices. In Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, 31 May–2 June 2009; pp. 169–178.
31. Private Smart Contracts Using Homomorphic Encryption. Available online: <https://www.zama.ai/post/private-smart-contract-using-homomorphic-encryption-ethcc-2022> (accessed on 18 January 2024).
32. Mucchi, L.; Jayousi, S.; Martinelli, A.; Caputo, S.; Marcocci, P. An Overview of Security Threats, Solutions and Challenges in WBANs for Healthcare. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019; pp. 1–6. [CrossRef]
33. Yin, C.; Zhu, Y.; Fei, J.; He, X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access* **2017**, *5*, 21954–21961. [CrossRef]
34. Haghghat, M.H.; Li, J. Intrusion detection system using voting-based neural network. *Tsinghua Sci. Technol.* **2021**, *26*, 484–495. [CrossRef]
35. Priya, D.D.; Kiran, A.; Purushotham, P. Lightweight Intrusion Detection System(L-IDS) for the Internet of Things. In Proceedings of the 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC), Bhubaneswar, India, 19–20 November 2022; pp. 1–4. [CrossRef]
36. Roy, S.; Li, J.; Choi, B.J.; Bai, Y. A lightweight supervised intrusion detection mechanism for IoT networks. *Future Gener. Comput. Syst.* **2022**, *127*, 276–285. [CrossRef]

37. Azimjonov, J.; Kim, T. Designing accurate lightweight intrusion detection systems for IoT networks using fine-tuned linear SVM and feature selectors. *Comput. Secur.* **2024**, *137*, 103598. [[CrossRef](#)]
38. Alsubaie, F.; Al-Akhras, M.; Alzahrani, H.A. Using Machine Learning for Intrusion Detection System in Wireless Body Area Network. In Proceedings of the 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 3–5 November 2020; pp. 100–104. [[CrossRef](#)]
39. European Commission. *EU General Data Protection Regulation (GDPR) No. 679/2016*; European Commission: Luxembourg, 2016.
40. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A.y. Communication-Efficient Learning of Deep Networks from Decentralized Data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), Ft. Lauderdale, FL, USA, 20–22 April 2017; Singh, A., Zhu, J., Eds.; PMLR: New York, NY, USA, 2017; Volume 54, pp. 1273–1282.
41. Albattah, A.; Rassam, M.A. Detection of Adversarial Attacks against the Hybrid Convolutional Long Short-Term Memory Deep Learning Technique for Healthcare Monitoring Applications. *Appl. Sci.* **2023**, *13*, 6807. [[CrossRef](#)]
42. Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man In The Middle Attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051. [[CrossRef](#)]
43. Awad, M.; Sallabi, F.; Shuaib, K.; Naeem, F. Artificial intelligence-based fault prediction framework for WBAN. *J. King Saud Univ.—Comput. Inf. Sci.* **2022**, *34*, 7126–7137. [[CrossRef](#)]
44. Che, L.; Wang, J.; Zhou, Y.; Ma, F. Multimodal Federated Learning: A Survey. *Sensors* **2023**, *23*, 6986. [[CrossRef](#)]
45. Hu, H.; Salcic, Z.; Sun, L.; Dobbie, G.; Yu, P.S.; Zhang, X. Membership Inference Attacks on Machine Learning: A Survey. *ACM Comput. Surv.* **2022**, *54*, 1–37. [[CrossRef](#)]
46. Truong, N.; Sun, K.; Wang, S.; Guitton, F.; Guo, Y. Privacy preservation in federated learning: An insightful survey from the GDPR perspective. *Comput. Secur.* **2021**, *110*, 102402. [[CrossRef](#)]
47. Moshawrab, M.; Adda, M.; Bouzouane, A.; Ibrahim, H.; Raad, A. Reviewing Federated Learning Aggregation Algorithms; Strategies, Contributions, Limitations and Future Perspectives. *Electronics* **2023**, *12*, 2287. [[CrossRef](#)]
48. Kim, J.; Park, G.; Kim, M.; Park, S. Cluster-Based Secure Aggregation for Federated Learning. *Electronics* **2023**, *12*, 870. [[CrossRef](#)]
49. Wei, K.; Li, J.; Ding, M.; Ma, C.; Yang, H.H.; Farokhi, F.; Jin, S.; Quek, T.Q.S.; Vincent Poor, H. Federated Learning with Differential Privacy: Algorithms and Performance Analysis. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3454–3469. [[CrossRef](#)]
50. Baruch, G.; Baruch, M.; Goldberg, Y. A Little Is Enough: Circumventing Defenses For Distributed Learning. In *Advances in Neural Information Processing Systems*; Wallach, H., Larochelle, H., Beygelzimer, A., d’Alché-Buc, F., Fox, E., Garnett, R., Eds.; Curran Associates, Inc.: Brooklyn, NY, USA, 2019; Volume 32.
51. Kim, M.; Günlü, O.; Schaefer, R.F. Federated Learning with Local Differential Privacy: Trade-Offs between Privacy, Utility, and Communication. In Proceedings of the ICASSP 2021—2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Toronto, ON, Canada, 6–12 June 2021; pp. 2650–2654. [[CrossRef](#)]
52. Rüb, M.; Herbst, J.; Lipps, C.; Schotten, H.D. No One Acts like You: AI based Behavioral Biometric Identification. In Proceedings of the 2022 3rd International Conference on Next Generation Computing Applications (NextComp), Flic-en-Flac, Mauritius, 6–8 October 2022; pp. 1–7. [[CrossRef](#)]
53. Qiu, H.; Dong, T.; Zhang, T.; Lu, J.; Memmi, G.; Qiu, M. Adversarial Attacks Against Network Intrusion Detection in IoT Systems. *IEEE Internet Things J.* **2021**, *8*, 10327–10335. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.