

# A review on security issues and solutions for precision health in Internet-of-Medical-Things systems

Nan Li<sup>1</sup>, Minxian Xu<sup>1</sup>, Qimeng Li<sup>1,3</sup>, Jikui Liu<sup>1</sup>, Shudi Bao<sup>2</sup>, Ye Li<sup>1,\*</sup>, Jianzhong Li<sup>1</sup>, and Hairong Zheng<sup>1</sup>

<sup>1</sup>Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, 518055 Shenzhen, China

<sup>2</sup>Ningbo University of Technology, 315211 Ningbo, China

<sup>3</sup>University of Calabria, 87036 Rende, Italy

**Abstract.** Precision medicine provides a holistic view of a person's health that combines genes, environment and lifestyle, aiming at realizing the individualized therapy. With the developing of Internet of Things (IoT) devices, widespread emergence of Electronic Medical Records (EMR), booming of cloud computing and artificial intelligence, it provides an opportunity to collect the healthcare big data throughout the lifespan and analyze the disease risk at all stages of life. Thus, the focus of precision medicine is shifting from treatment to prediction and prevention, namely precision health. To achieve this goal, different types of data, such as omics, imaging, EMR, continuous physiological monitoring, lifestyle, and environmental information need to be collected, tracked, managed and shared. For this purpose, Internet-of-Medical Things (IoMT) is playing a vital role in bringing together the health systems, applications, services and devices, that can improve the speed and accuracy of diagnosis and treatments, and monitor and modify patient behaviour and health status in real time. However, due to the proliferation of IoMT devices, security has become a growing concern. The increasing interconnectivity of IoMT-enabled devices with the health data reception, transmission, and processing significantly increases the number of potential vulnerabilities within a system. To address the security issues for precision health in IoMT systems, in this article, we review the state-of-the-art techniques and schemes from the perspective of a hierarchical system architecture. We present an IoMT system model consisting of three layers: the sensing layer, the network layer and the cloud infrastructure layer. In each layer, we discuss the security vulnerabilities and threats, and review the existing security techniques and schemes corresponding to the system components and their functionalities. Due to the unique nature of biometric features in medical and health services, we highlight the biometrics-based technologies applied in IoMT systems, which make a great difference from the security solutions in other existing IoT systems. Finally, we summarize the challenges and future research directions in IoMT systems for a better and more secure future of precision health.

**Keywords—** Precision health, Internet-of-Medical-Things, Security in hierarchical systems, Biometrics-based security

---

\*corresponding author, e-mail: ye.li@siat.ac.cn

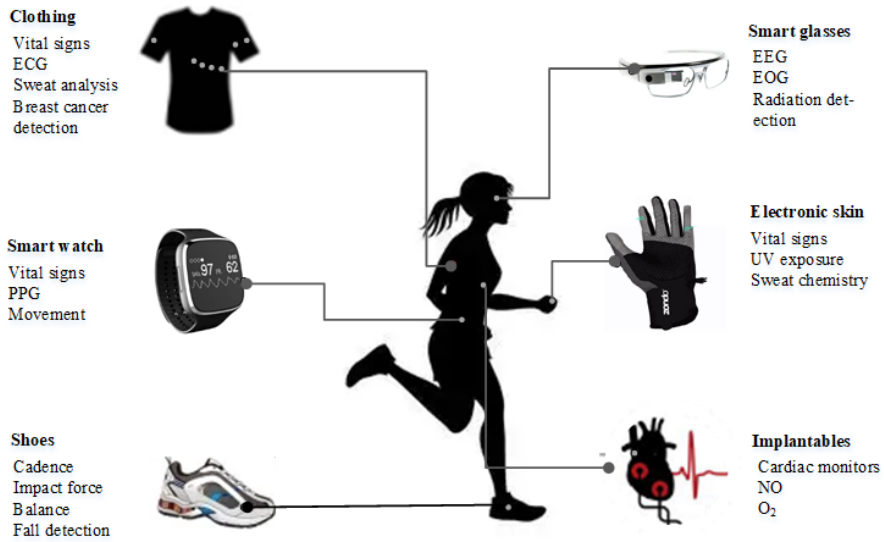
# 1 Introduction

In 2015, U.S. President Barack Obama proposed the "Precision Medicine Initiative" in his State of the Union address, which aims to revolutionize the way we improve health and treat disease [1]. Precision medicine mainly relies on the genetic, imaging, biochemical and other data obtained in the hospital to formulate individualized diagnosis and treatment plans for patients. However, the development of the disease and the occurrence of symptoms are a dynamic process, and only relying on the static data in the hospital is not enough to make an early diagnosis and comprehensive assessment of the disease. Therefore, disease prevention and early diagnosis require multi-dimensional dynamic monitoring data outside the hospital. In order to promote the development of precision medicine, developed countries such as the United States have successively launched precision health research programs since 2018. The precision health research primarily emphasizes the important role of prevention in health throughout the lifespan [2]. Similarly, the Chinese government has put forward the concept of prevention-oriented health management in Healthy China 2030. In this paradigm, a person's disease risk assessment is based on their genetic profile and family history, even including health monitoring information from before birth [3]. Precision health seeks to make healthcare contact more accessible by integrating monitoring and diagnostics into everyday life. This requires multiple types of sensors and devices to continuously monitor physiological signals (blood pressure (BP), electrocardiogram (ECG), photoplethysmography (PPG), etc.), biochemical indicators (blood sugar, biomarkers), behaviors and other health data outside hospital (Figure 1). Thanks to the development of Internet of Things (IoT) technology, it is possible to conduct long-term monitoring of human health-related data through human sensor networks and medical equipment [4–8]. IoT has assisted the healthcare providers in the new way of assistance and has been integral in monitoring and curing diseases. The adoption of IoT has revolutionized the healthcare industry by enabling providers to monitor patients' health remotely through connected medical and wearable devices via Internet of Medical Things (IoMT) [9].

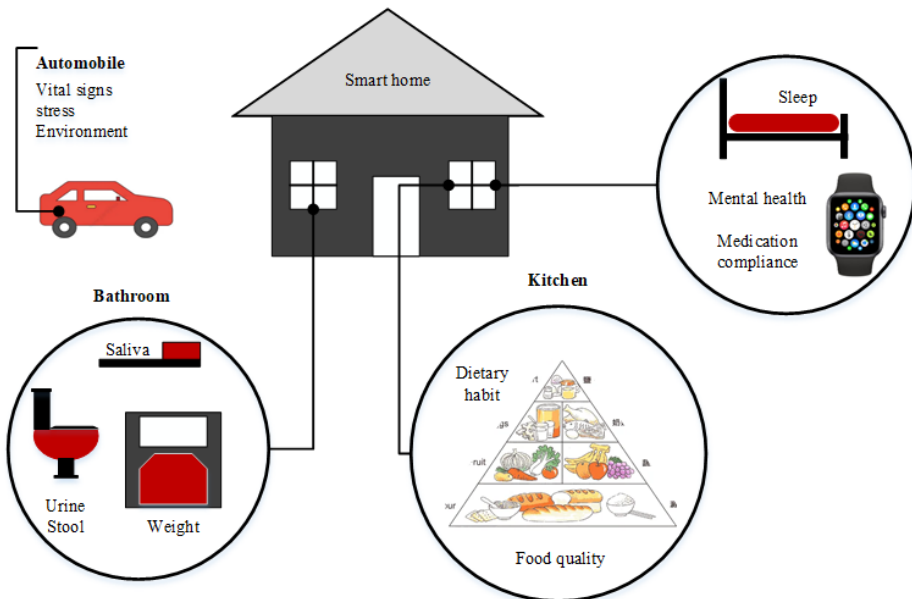
IoMT technology is changing the face of healthcare and has the potential to significantly improve patient access and system efficiencies. Especially in COVID-19 pandemic since 2020, the urgent and widespread need for care, coupled with the challenge of physical distancing, has accelerated the creation and adoption of new digital technologies, as well as new processes to support their adoption and implementation across healthcare [10–12]. The potential benefits of IoMT can be seen within a hospital setting, where monitoring COVID-19 patients is costly in terms of time and PPE (personal protective equipment) consumption [13]. IoMT technologies enable medical devices to send data to medical practitioners who can monitor a patient's condition without having to take readings at the bedside. The same technologies can also enable patients who do not require hospitalization to be safely monitored while remaining at home or in a community setting.

The IoMT connects health systems, applications, services, and devices over the cloud via multiple transmission methods (e.g., Bluetooth, 5G, NB-IoT). It has revolutionized the way that how the patients are approached and healthcare data are managed [14–16]. Existing medical devices can be modified to IoMT devices to collect and store real-time data to a central or distributed location. Alarms and notifications can be set with different rules and defined thresholds. They can be applied to the collected data to detect and predict changes [17]. IoMT can also help discover trends in a patient's specific disease or health condition [18]. IoMT-enabled devices can also facilitate health guidance with monitoring systems for diet, physical activity, and quality of life [19–21]. Innovative devices such as wearable devices, implantable chips, and embedded systems in biomedical devices continuously gather data about patients' activities and related vital changes [8, 22]. Advanced sensors, converters, and firmware in smart devices also allow users to analyze and correlate various vital signs with health conditions at the device level [23]. In short, IoMT is able to increase the access from either the patients/caregivers or the healthcare practitioners, meanwhile, supporting manifold medical services and improving the quality of services. Considering that IoMT system-assisted precision health covers a variety of application scenarios, IoMT services fall into the following categories in general:

- 1) Real-time control service. In this case, the fast and accuracy response is vital, otherwise the outcome could be fatal. Therefore, the quality of services such as packet loss rate, latency, and jitter must be strictly guaranteed. Typical application scenarios include remote diagnosis, ambulance vehicular first-aid, remote surgery, remote biomedical monitoring in intensive care unit (ICU), etc.



(a)



(b)

**Figure 1.** Multiple physiological data monitoring outside the hospital. (a) Wearable device for multi-physiological monitoring; (b) Devices in the home or car can passively monitor various physiological data such as biological fluids, human behavior, and physiological signals.

2) Information exchange service. It involves forwarding a massive amount of medical-related data to remote data centers. Thus, the required network throughput is generally very high but the demand for packet loss rate and latency are not restricted. Typical application scenarios include 24-hour health data uploading, and remote health education video display, etc.

3) Periodical monitoring service. It is very common in E-health and occupies quite a large proportion of the overall network traffic. This kind of service shows strong regularity and has a low requirement in time delay. Typical application scenarios include remote ward rounds, in-home chronic disease management and community rehabilitation therapy, etc.

4) Event-driven service. It has the characteristics of being sudden, emergent, and unpredictable. Thus the most stringent real-time constraint is set, so that the medical staff or caregiver can quickly provide necessary assistance. Typical application scenarios include health monitoring alarms, elders falling alarms, etc.

In the IoMT system, modern technologies such as various wearable devices, bio-information sensors, and medical big data have undoubtedly improved the overall quality of medical care and strengthened the interaction between patients and medical practitioners [15]. However, a new report by Cynerio (2022) discovered [24] that “more than half of connected medical devices and other IoT devices contain critical vulnerabilities.” If exploited, these vulnerabilities could be detrimental to patient safety and privacy [25, 26]. Not only the medical devices connected to home networks, public Wi-Fi or cellular networks, but also the cloud with more health care applications and platforms moved to, an abundance of valuable data is stored and becomes more prone to hacking, making them prime targets [27–32]. With catastrophic consequences, any security concerns related to the healthcare system should be addressed proactively. In this case, security is considered as one of the most critical issues in the IoMT systems and even the healthcare industry.

Recent literature includes surveys that provide various taxonomies of potential threats and attacks, corresponding security and privacy issues, proposed techniques and solutions in different research areas. As summarized in Table 1, the most recent works review security of IoMT systems from different aspects. Yaqoob et al. [38] discussed the security risks and solutions faced by medical devices. Koutras et al. [34] summarized communication protocols applicable in IoMT systems and compared their application range. From the specific aspect of cryptography, Ghubaish et al. studied a large scale of cryptographic techniques in [33]. In the work of Newaz et al. [37], possible attacks in different types to IoMT systems were classified. There are also works differing from emphasis and analysis angle, such as the application scenario in Healthcare 4.0 [36] and circular economy [35]. Our work aims to make a difference from the existing surveys and to fully cover the whole process of health data in IoMT systems. An integrated system is discussed herein, including medical devices, network connections and cloud platform. Potential attacks through the stages of data processing and the corresponding security solutions are reviewed, from the collection, aggregation, communication and analysis of data. Our work focuses on a complete system architecture, covering the security risks and technologies in multiple functional layers. To this end, a thorough review from the aspects of network service and system architecture is given in this paper.

**Table 1.** Comparison of Our Work with Previous Reviews

Reference	Research Area	Security Goals	Security Metrics	Attacks on IoMT Systems		Solutions for IoMT Systems	
				Attack Taxonomy	Existing Attacks	Solution Taxonomy	Existing Solutions
Ghubaish et al. [33]	Cryptographic Techniques	◦	•	•	•	◦	•
Koutras et al. [34]	Communication Protocols	•	◦	•	•	•	•
Hatzivasilis et al. [35]	Circular Economy-featured	◦	◦	•	•	•	•
Hathaliya et al. [36]	Security and Privacy in Healthcare 4.0	•	•	◦	◦	•	•
Newaz et al. [37]	Attack-aspect and Corresponding Defense	•	•	•	•	◦	•
Yaqoob et al. [38]	Security for Medical Devices	◦	◦	•	•	•	•
<b>Our work</b>	Security in Hierarchical IoMT Systems	•	•	•	•	•	•

• and ◦ represent yes and no, respectively.



In addition, the issue of functional safety cannot be ignored either in the IoMT system. Functional safety is part of overall safety and relies on a system or device to properly respond to its inputs. The safety objectives are achieved when each specific safety function is implemented and the required level of performance for each safety function is met [39]. The popularity of central processing units (CPUs) and software has inevitably introduced network security issues while improving traditional functional safety. At present, with the continuous deepening of human-machine-material integration, network security and functional safety have become an inseparable integrated security issue, and its connotation and extension will continue to expand in depth and breadth [40, 41].

With the recent advancements in security protection technologies to address attacks and potential risks targeting IoMT systems, this paper reviews the state-of-the-art techniques and schemes for IoMT systems from the perspective of a hierarchical system architecture. The main contributions can be summarized as follows:

- We build a hierarchical IoMT system architecture consisting of three layers: the sensing layer, the network layer and the cloud infrastructure layer. In each layer, the connected devices, the communication technologies and the provided resources have been introduced briefly. To emphasize the differences of IoMT systems from the general IoT systems, the specific security requirements are summed up from the aspect of service demands in IoMT for precision health.
- We discuss the security vulnerabilities and threats related to each layer, and review the existing security techniques and schemes corresponding to the system components and their functionalities. A comprehensive taxonomy of the state-of-the-art solutions is also provided in tables.
- We stress the biometrics-based technologies applied in IoMT systems due to the unique nature of biometric features in medical and health services. Although existing researches mainly focus on security issues on authentication and key management, it renders insights into employment of biometrics for security and shows a great potential on extensive uses.

In the following section, a brief overview of the security issues in IoMT system is described. We start with building up a three-layer IoMT system, in each layer we introduce the fundamental components and applied technologies, performing different functions.

## 2 Overview of Security in IoMT System

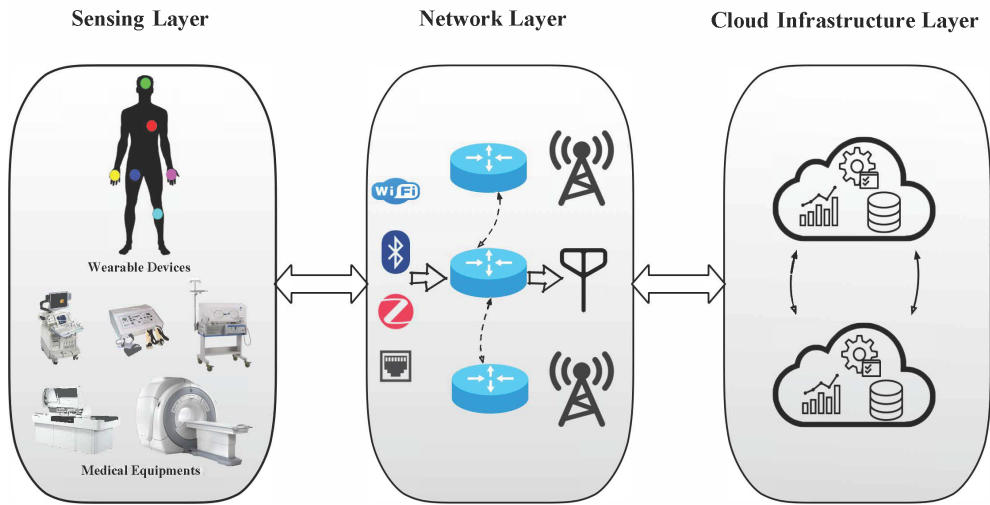
### 2.1 System Architecture

To comprehend the structure of communication that patients and devices follow to interact with physicians, hospital management system and data analytics system, Figure 2 shows the Internet of Medical Things (IoMT) system architecture, consisting of three layers: sensing layer, network layer and cloud infrastructure layer. These layers include all data stages starting from the individual's biometrics collection stage and ending in data storage and subsequent process and analysis.

#### 2.1.1 Sensing Layer

Sensing layer presents wireless medical devices that integrate a set of intelligent, small-sized, and resource-constrained wireless on-body sensors and in-body sensors to store, process, and monitor different psychological parameters required for diagnosis. Medical equipment in the hospital are presented as well, including radiology and ICU equipment, ventilator, dialysis machines, etc., to provide accurate health treatments. The devices including various type of sensors which fall into the following groups:

- *Wearables devices* - are integrated into wearable objects or directly with the body in order to help monitor health and/or provide clinically relevant data for care. They will be divided into consumer wearable, clinical wearables, implantable and ambient devices based on requirement and usage.
  - *Consumer wearable* - is usually used to monitor physiological signals (BP, ECG, PPG, etc.) and behavioral data (gait, acceleration, etc.) in real-time on the body surface.



**Figure 2.** The hierarchical architecture of IoMT systems.

- *Implantable Device* - is a kind of medical devices which will place inside patients' body during a medical procedure, such as surgery. a state of the art implantable device including pacemaker, smart pills (also known as smart drugs or digital pills). Existing ingestible pills, e.g., capsule endoscopy, can collect a patient's gastrointestinal information over a longer period outside the hospital, and various sensors can be incorporated to gather more information.
- *Ambient Devices* - which are usually a series of sensors, such as motion detectors, contact switches, break-beam sensors, and pressure mats used to detect environmental information/ambient changes in a specific environment (e.g., home and workplace).
- *Medical equipments* - mainly includes medical imaging, biochemistry analyzer, and bedside monitor for disease screening in hospitals.
  - *Medical imaging equipment* - refers to detection instruments that obtain human body structure information through medical imaging technology, such as magnetic resonance (MR), computed tomography (CT), and ultrasound. Medical image data has the characteristics of large data size and low real-time requirement.
  - *Biochemistry analyzer* - is mainly used to detect various biochemical markers in the human body, and the detected data has the characteristics of small data volume and low real-time requirements.
  - *Bedside monitor* - is used to monitor all kinds of physiological parameters of patients in the ward in real time, and to timely alarm the occurrence of dangerous events, has high requirements on real-time data transmission.

### 2.1.2 Network Layer

Network layer depicts the transmission of sensed data from sensing devices or medical equipment to a local gateway and a remote platform via wired or wireless communication protocols. Health providers can also access sensed patient information through the gateway. Several gateways are distributed geographically developing edge/fog computing to perform health-related tasks. Gateway can bridge Internet/local switches and wireless sensor networks (WSNs) as it supports different protocols. Networked medical devices require both wireless short-range standards and wired technologies to perform their respective tasks efficiently. Personal Area Network (PAN) comprising short distance technologies like ZigBee, Bluetooth and Ultra Wideband (UWB) or Local Area Network (LAN), Ethernet and Wi-Fi

connection. It is used to transfer sensed information to the gateway. Wide Area Network (WAN) such as global system for mobile communication (GSM) that do not require connectivity, but employ back-end servers/applications and WSN, having capability to accommodate a large number of sensor nodes, helpful in some sensors requiring low power connectivity can be used. The communication of data happens through different technologies described below and the comparison is listed in Table 2.

- *Radio-Frequency Identification (RFID)* - is a short-range communication tag which does not require any external power source, but highly insecure.
- *Near Field Communications (NFC)* - operates in two modes: in active mode, there is simultaneous production of radio-frequency and data transmission without pairing, while in passive mode radio-frequency is generated by only one device.
- *Bluetooth and Bluetooth Low Energy (BLE)* - Bluetooth can establish an authenticated, encrypted and low interference connection for protected data transmission [42]. However, it is still vulnerable to viruses, Man-in-the-Middle (MITM), tracking, and sniffing [43]. Bluetooth Low Energy (BLE) is appropriate for sensor-based medical devices due to low power consumption.
- *ZigBee* - is used by the majority of the sensor based devices for interconnected, uninterrupted connection among medical devices. Its low power consumption makes it an ideal choice for healthcare applications with the help of sleep mode feature. Advanced Encryption Standard (AES) algorithm along with a 128-bit key is used in this standard to provide security. However, such standard is vulnerable for energy depletion attack, replay attack, and sniffing [44]. Moreover, AES is not suitable for resource-constrained sensory devices.
- *Wi-Fi* - all devices, laptops, tablets, and smartphones are Wi-Fi integrated while high-energy consumption emerges as an important drawback.
- *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)* - is inexpensive, consumes less power and is easily adaptable, which make it suitable for sensor based IoMT systems.
- *Ethernet* - as one of the most widely used standards put forth by the IEEE for wired connectivity, provides the provision of connectionless user data integrity, origin authenticity, and data confidentiality, data confidentiality.
- *Cellular Networks* - The security solutions have been well regulated and applied. Evolving 5G cellular networks provide more technical supports such as software-defined networks (SDN) and network slicing to ensure an even more reliable communication system.

### 2.1.3 Cloud Infrastructure Layer

Cloud infrastructure layer represents the infrastructure that provides physical/virtual resources to support the running of applications at the sensing layer [45]. The data collected at the sensing layer can be transmitted from the network layer, and then be stored in the cloud infrastructure layer. The typical resources that can be provisioned are included as below:

**Table 2.** Communication Technologies in IoMT Systems

Network Type	Communication Technology	Coverage	Peak Data Rate	Frequency Band	Power Consumption	Protocols
Personal Area Network (PAN)	RFID	10cm-200m	varies with frequency	30K-2.45GHz	-	-
	NFC	20cm	424Kbps	13.56MHz	Low	-
	Bluetooth/BLE	10-100m	2.1Mbps	2.4-2.5GHz	Low/Very low	IEEE 802.15.1
	Zigbee	10-200m	250Kbps	2.4GHz	Low	IEEE 802.15.4
	Wi-Fi	100-300m	54Mbps	2.4/5GHz	High	IEEE 802.11
	6LoWPAN	10-100m	50Kbps	2.4GHz	Low	IPv6 and IEEE 802.15.4
	Ethernet	Wired	400Gbps	-	Very high	IEEE 802.3
Wide Area Network (WAN)	Cellular Network	10-30km	20Gbps	600M-6GHz 24-60GHz	Very high	-

- *Processing capability* - when deploying applications in the cloud, the cloud infrastructure can provision computation resources along with memory to process the data. For instance, the collected medical data requires to be analyzed by a complicated model based on data computation. Especially, for the computation-intensive tasks, sufficient computation resources should be provided to ensure the quality of supported services.
- *Storage capability* - medical data can be stored in cloud to relieve the local storage bottleneck. Cloud storage can provide efficient data storage and access methods to support the execution of applications. The hardware of cloud storage is provided by manufacturers and can be managed by cloud manager to ensure data security. The cloud storage should be utilized as reliable, consistent, and fault-tolerant.
- *Virtualized resources* - by taking advantage of virtualization technology, the physical resources can be transformed into virtualized resources and shared by multiple users in a more efficient manner, i.e. single physical machine can be virtualized into 8 virtual machines in Amazon. The virtualized resources can be instantiated by virtual machines (VMs) or microservice-based containers. Apart from accessing physical resources directly, the users can also rent the VMs to run their applications.

## 2.2 Security Metrics Based on the IoMT Service Demands

Compared with the general IoT systems, the IoMT system pays more attention to the demand of services. Following the categories of IoMT services in Section 1, the performance demands can be classified as:

1) *Timeliness*. Health care should happen promptly, for the sake of both patients and the health care providers, especially when IoMT enables remote monitoring and treatment. Yet, the requirement on decision and feedback time delay of IoMT applications varies according to different use cases. For example, a patient's condition is tracked regularly during chronic disease monitoring, while in clinical decision support systems, accurate and timely diagnosis should be performed by doctors.

2) *Diversity*. The IoMT system brings together medical devices and mobile applications, multi-source data, processes (monitoring and care delivering), and people (patients, providers, professionals). It is expected to generate and consolidate measurable information from different sources that improve treatment speed and accuracy according to an individual's service requirement.

3) *Accuracy*. Accuracy should be throughout every component of IoMT. From data collection, data transmission, data storage, to data analysis and decision making, accurate information delivery is life-critical.

4) *Reliability*. A reliable IoMT system must achieve its functional goals at all times, meaning it should not be prone to unexpected failure under normal operating conditions. The potential diagnostic nature of IoMT-based systems mandates reliability of every system component in order to guarantee the correctness of delivered information and services.

5) *Scalability*. To handle the explosive growth of different kinds of medical services, IoMT applications must have the ability to support an increasing number of connected devices (including types as in Subsection 2.1), users (with different service requirements), application features, and analytics capabilities, without any degradation in the quality of service. Scalable IoMT applications are also essential to monitoring, securing, and managing an increasing number of devices through a proportionate increase in the resources.

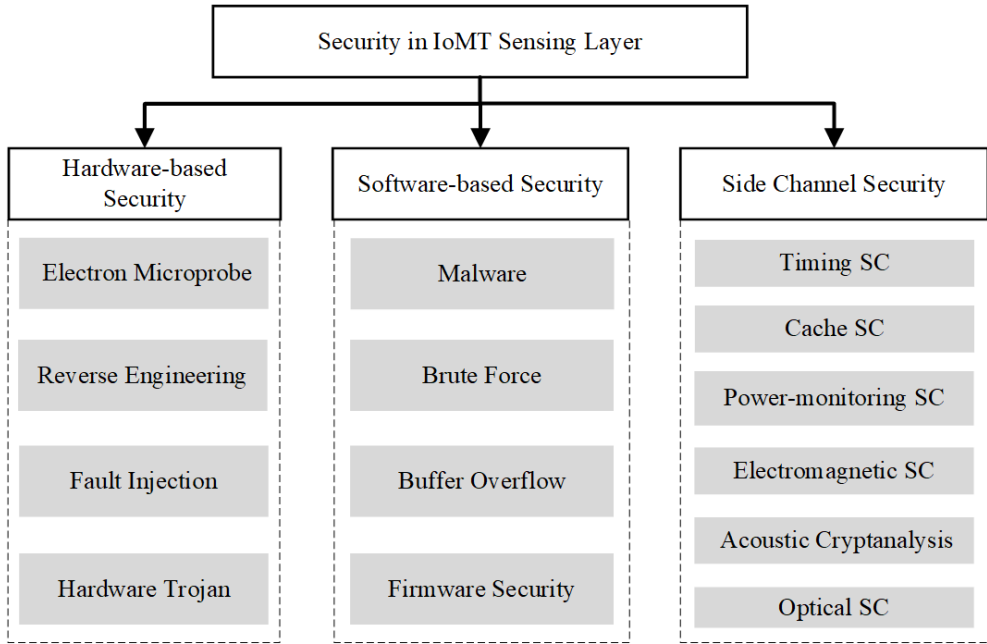
To satisfy all demands of services that being summarized, there is one of the main drawbacks of IoMT, that is the weak security. Any exploited vulnerability in IoMT enables cybercriminals to take a number of malicious actions, such as seizing control of the medical device; stealing sensitive patient health, personal and insurance data; stealing proprietary clinical records; obfuscating network traffic; disrupting healthcare delivery processes; and ransoming the device to turn a profit. IoMT demands better security because, unlike other industries, a security breach in a healthcare network can quite literally become a matter of losing lives [46]. Security requirements for the IoMT systems are more rigorous than that of the typical IoT-based infrastructures [47–49]. Based on the service demands above, security for IoMT systems mainly focuses on the following metrics.

- **Confidentiality/Privacy**. The ability to keep the data private while being gathered, transmitted, or stored. In addition, they must only be accessible to authorized users. Collection and storage of patient

health data must comply with legal and ethical privacy regulations, such as General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) [50], in which only authorized individuals can have access to those data. To prevent breaches of data, adequate measures must be adopted to ensure the confidentiality of the health data associated with individual patients. The importance of such measures cannot be overemphasized, as the data stolen by cyber criminals could be sold in illegal markets, causing the patients to suffer from not only privacy violation but also possible financial and reputational damages.

- **Integrity.** This is related to the capability of protecting the data from any unauthorized tampering during the collection, transmission, and storage stages. For IoMT systems, the purpose of the data integrity requirement is to ensure that the data arriving at the intended destination have not been compromised in any way during the wireless transmission [51]. Attackers could gain access to and modify patient data by taking advantage of the broadcast characteristic of the wireless network, and which could lead to severe implications in life-threatening cases. To guarantee that the data have not been compromised, the capacity to detect potential unauthorized distortions or manipulations of the data is critical. Therefore, appropriate mechanisms of data integrity must be implemented to prevent alteration of transferred data by malicious attacks. Moreover, the integrity of the data stored in the medical servers also needs to be ensured, which means the data cannot be tampered with.
- **Availability.** Services and data must be accessible when they are required to the relevant users. Such services and data, provided by the medical servers and devices, will become inaccessible if Denial of Service (DoS) attacks occur. Any inaccessible data or services could lead to life threatening incidents, such as unable to provide prompt alert in the case of a heart attack. Therefore, to accommodate the possibility of availability loss, the healthcare applications must be always-on to ensure data availability to the users and emergency services [52].
- **Authenticity.** The capability to validate the identity of a user accessing the system. Mutual authentication is the most secure form where both the server and the client authenticate each other before any secure data/key exchange. As patients' data is often stored and aggregated in the personal server level before being forwarded to the medical servers in the IoMT systems, it is essential to ensure that the data is well protected while on the personal servers. Generally, two types of authentication schemes must be deployed to ensure security and privacy in the personal server level, namely device authentication and user authentication. Personal server (i.e. a smart phone) shall perform authentication before accepting data sent from the medical devices and sensors. False information from malicious devices about patients' physical conditions could have severe negative impacts on the clinical diagnosis and care decisions, therefore, device authentication must be implemented in any IoMT systems [53]. The data stored either temporarily or permanently on the personal servers should only be accessed by the patients and medical staff, such as caregivers, therefore, effective user authentication schemes are required [54]. A popular solution to user authentication in the personal server level is the use of biometrics, which is particularly applicable in the IoMT systems, as most of the biometrics can be easily collected from medical and healthcare devices worn by or implanted in the human body.
- **Anonymity.** The capability to keep the patients'/physicians' identities hidden from unauthorized users when they interact with the system. Patient sensitive data can be divided into three categories: explicit identifiers, quasi-identifiers, and privacy attributes. Explicit identifier can uniquely indicate a patient, such as an ID number, name, and cell phone number. A combination of quasi-identifiers can also uniquely indicate a patient, such as age, birth data, and address. Privacy information refers to sensitive attributes of a patient, including illness and income. In the process of data publication, while considering the distribution characteristics of the original data, it is necessary to ensure that the individual attributes of the new dataset are properly processed, so as to protect the patient's privacy. At present, random perturbation technology and data anonymous technology are usually used to solve these issues [55].

Having comprehensive and integrated end-to-end solutions for the IoMT systems is key for the research and industry. We then review and compare the state-of-the-art security strategies through the three layers of the IoMT system architecture. The remainder of this article is organized as follows. From Sections 3 to 5, we present the potential risks and the corresponding state-of-the-art security strategies



**Figure 3.** The classification of sensing layer security for IoMT systems.

in the sensing layer, the network layer, and the cloud infrastructure layer, respectively. Specifically, we highlight the biometrics-based technologies on authentication and key management for their significance and uniqueness reflected in IoMT systems. The challenges and potential research directions on existing problems are summarized in Section 6. Finally, we conclude this paper in Section 7.

### 3 State-of-the-art Security Strategies in IoMT Sensing Layer

The sensing layer is responsible for acquiring and collecting data from physical devices and is closely related to medical devices in an IoMT environment. According to the World Health Organization [56], “there are an estimated two million different kinds of medical devices on the world market, categorized into more than 7000 generic devices groups.” These devices come in different forms and sizes: from home monitoring gadgets to huge on-site devices, those leads to the IoMT ecosystem becoming very complex and involve a wide variety of physical devices that need to prioritize security to ensure optimal performance throughout its lifecycle while developing, configuring, and updating. Therefore, this chapter discusses the threats and solutions for the device level, which take more attention to the hardware and the onboard software/system security. The taxonomy is shown in Figure 3.

#### 3.1 Hardware-based Security

Hardware security is vulnerability protection that comes in physical devices, machines, and peripherals. A hardware attack is an exploitable weakness in a device’s hardware that can be used to gain physical or remote access to the device to perform malicious activities.

##### 3.1.1 Electron Microprobe

Electronic Microprobe refers to techniques that allow an attacker to directly observe some or all of the sensitive information, such as plaintext or encryption keys. Using modern integrated circuit editing

techniques, attackers could remove the protective layer and expose the internal chip to the air. Then, through a fine-tip probe, analyze and collect the electrical properties, signals, and data from the interest area. Integrated circuits designed for safety-critical applications, such as microcontrollers and security tokens in mobile devices, are among the most common victims of such attacks [57–59]. Electronic Microprobe is classified as an invasive attack along with fault injection and reverse engineering, as they both require complete encapsulation removal and circuit wiring exposure. Today’s most commonly used and powerful electron probe tool is the Focused Ion Beam (FIB) [60, 61]. Through FIB technology, attackers can achieve sub-micron or even nano-level precision [62]. These micro-probing attacks are challenging to defend against because traditional integrated circuit design processes do not place anything under the silicon substrate. Both methods are passive, making them difficult to detect. However, both ways require observing the emission of photons, which makes them limited by the wavelength of the emitted photons.

### 3.1.2 Reverse Engineering

Invasive attacks require direct access to the inner part of the device. Reverse engineering is the analysis process that allows one to fully understand a device’s design by extracting its inner structure information or knowledge [63]. The attacker could understand the internal design structure of the chip through an electron microscope or even directly analyze the data in the corresponding storage area of the chip using laser scanning. For example, many IoT devices have older OS or firmware versions that are now outdated or patched when vulnerabilities in later versions are discovered or fixed. Through these synergies or firmware, attacks can directly target these unpatched vulnerabilities [64]. A helpful method [65] is to provide anti-reverse engineering by executing encrypted code in the hypervisor and protecting the decryption keys.

### 3.1.3 Fault Injection

A fault injection attack is an external physical attack. By establishing a specific fault model and adopting strategies and methods, circuit faults are artificially generated and introduced into the target system. And collect and analyze the collected data through failure analysis techniques such as Differential Failure Analysis (DFA), Crash Failure Analysis (CFA), and Invalid Failure Analysis (IFA) to gain valuable information.

Hardware-based fault injection is a typical mainstream attack method, such as voltage glitch, clock glitch, electromagnetic, and laser fault injection. A practical method against voltage glitch attacks is to use on-chip voltage regulators. In [66], the authors analyze the effect of capacitor size and voltage regulator phase number on the resilience of cryptographic circuits to fault injection attacks. The effectiveness of the proposed method against voltage glitch attacks is demonstrated through extensive simulations of the S-box of the Advanced Encryption Standard (AES) [67] cipher algorithm.

### 3.1.4 Hardware Trojan

Attackers exploit hardware or use hardware mechanisms to access data or software running on a chip through malicious modifications to the original circuitry [68]. HT can infect any IC, such as Application Specific Integrated Circuits (ASICs), System on Chips (SoCs), Field Programmable Grid Arrays (FPGAs), and Digital Signal Processors (DSPs), resulting in catastrophic damage to the device at the hardware level.

For example, an attacker who masters the internal hardware architecture can insert a hardware Trojan during the chip manufacturing process to destroy data, causing severe harm to medical devices [69]. Hardware Trojans have become a significant security risk for integrated circuits (ICs), as most are manufactured in outsourced manufacturing facilities. Third-party vendors can use uncertified intelligence cores such as Trojans to perform malicious activities, including leaking information from medical devices. In the following subsections, we will explain hardware security issues in detail.

## 3.2 Software-based Security

In this type of security issue, any inherent vulnerability in the device software can be exploited to perform a range of attacks. The attack taxonomy mainly includes malware, brute force cracking, and buffer overflow attacks.

### 3.2.1 Malware

By deploying a piece of malicious code (e.g., Mirai), attackers could intercept data stored inside the device's system to take control of the victim's system or damage it. Often, attackers will fake firmware updates, drivers, or security patches to distribute malware, which may lead to attacks on confidentiality, integrity, authenticity, and availability of the data and other resources of the system. In the presence of such attacks, the sensitive data of IoMT may be disclosed, altered, or even may not be available to authorized users. Therefore, it becomes essential to protect the IoMT environment from malware attacks. Recent research has shifted interest in malware detection from static or dynamic analysis-based approaches [70, 71] to extracting valid semantics at the application programming interface (API) level. For instance, in [72], authors proposed a scalable and event-aware Android malware detection system (EveDroid), which exploits the behavioural patterns in different events to effectively detect new malware based on the insight that events can reflect apps' possible running activities.

### 3.2.2 Brute Force

In this type of attack, the attacker will try to guess the authentication credentials of the intelligent device, and they will systematically check all possible passwords and passphrases until the correct one is found. For example, some devices (e.g., IP cameras and routers) are manufactured with default user credentials, which could gain access to the device easily by referring to the default password lists available on the internet. Traditional cryptography methods are effective against this attack. However, it has not yet proven lightweight and fast enough for IoT device authentication. Therefore, a hardware-based security method, so-called Physically Unclonable Functions (PUFs) [73], has emerged recently to satisfy the demand for IoT devices' security, which is based on the characteristic, i.e., PUF leverages the randomness of the manufacturing process to create a physically unclonable unique identifier. For instance, authors [74] proposed a PUF-based identity-preserving protocol for IoT device authentication (PUF-IPA) to prevent an adversary from brute forcing the device's PUF to acquire challenge-response pairs (CRPs) essentially locking out the device from unauthorized model generation.

### 3.2.3 Buffer Overflow

By sending crafted input, attackers could cause the application to execute arbitrary code, which causes the program or process to attempt to write more data into a fixed-length buffer block and leads to a buffer overflow. Buffer overflows remain one of the major security threats plaguing cyberspace for decades, due to the ubiquity of the software vulnerabilities it exploits and the low complexity of launching them. For instance, the first buffer overflow attack "Morris worm" occurred two decades ago, and it brought down more than 6000 web servers around the world. Currently, most researches are software-based. Wang et al. [75] proposed Polymorphic Stack Smashing Protection (P-SSP), whose core idea is to re-randomize the canaries for a new process/thread or a new function call. Other approaches based on hardware are increasing gradually to solve the buffer overflow issues. In [76], authors presented a security hardware design whose architecture includes program off-line behaviour analysis (POLBA) and hardware real-time behaviour monitoring (HRTBM) to detect buffer overflow attacks. Experimental result shows that it can detect a wide variety of buffer overflow attacks with simple hardware design and reasonable overhead penalties.



### 3.3 Firmware Security

Firmware attacks typically execute arbitrary malicious code on embedded devices by exploiting dynamic memory regions via improper input validation or poor physical security vulnerability. Two flavours of firmware attacks exist static and dynamic [77].

- *Static Firmware Attack* - focuses on modifying the firmware code residing in the memory region or during run time as part of the firmware update or patching process. Firmware update is a ubiquitous feature found in modern embedded devices. Previous research work has shown that the firmware update feature of numerous embedded devices is not adequately protected by proper user authentication [78–80]. Many devices that require certification to allow firmware updates are vulnerable to simple management interface bypass attacks [81]. Firmware modification attack is one of the most dangerous attacks, as it has been shown to occur on different embedded systems such as telecommunication infrastructure, SCADA and PLC systems, laptop battery controllers, medical devices, network interface cards and automated teller machines (ATM) [82]. Ling et al. [83] injected malicious code into a smart plug, enabling them to control it. The compromised firmware opens a reverse loop back channel to the attacker’s server and generates a reverse shell. Thus, attackers gain remote access to the plug and may carry out more attacks.
- *Dynamic Firmware Attack* - exploits the dynamic memory regions (stack and heap) to circumvent secure boot and attestation, e.g., code injection [84], code reuse attacks [85]. An attacker achieves malicious intent by diverting the control flow of the firmware to malicious code and executing it [86]. Several solutions to defend against such attacks include control-flow integrity (CFI) [87], randomization-based [88] and enforcement-based [89] methods.

### 3.4 Side Channel Security

Side-channel attack (SCA) specifically refers to a non-intrusive attack on the cryptographic algorithm, and the cryptographic algorithm is cracked through the leakage of side-channel information during the operation of the encrypted electronic device. Due to the different attack sources, side channel attacks can generally be divided into the following categories (but not limited to): Timing SCA, Cache SCA, Power-monitoring SCA, Electromagnetic SCA, Acoustic cryptanalysis, and Optical SCA.

#### 3.4.1 Timing SCA

For this type of side-channel attack, the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. Therefore, defences against such attacks usually require software optimizations and hardware redesigns to prevent threats from timing vulnerabilities. In [90], authors believe that devices such as GPUs have an exposure that relies on the timing information of the data, which attackers can exploit to recover encryption keys. Therefore, they propose a hierarchical Miss Status Holding Register (MSHR) design and a software-based approach to permute the organization of critical data structures to address vulnerabilities due to GPU coalescing units.

#### 3.4.2 Cache SCA

The cache attacks are based on the attacker’s ability to monitor cache accesses made by the victim in a shared physical system. For example, an L1 cache-based attack learns AES and asymmetric cryptography algorithm keys by analyzing the timing variance of cache usage. Recent research has shown that CPU caches, including last-level (LL) cache, are also vulnerable to attack. Cache randomization has recently been revived as a promising defence against conflict-based cache side-channel attacks for the above issues. In [91], the authors find out in the experiments that an attacker can easily find a usable eviction set within the chosen remap period of CEASER-S [92] and increase the number of partitions without dynamic remappings, such as ScatterCache [93], cannot eliminate the threat. But, the issues could be fixed within the current performance budget, and randomized set-associative caches can be sufficiently strengthened and possessed.

### 3.4.3 Power-monitoring SCA

Power-monitoring SC is one of the most common side-channel attacks. The attacker measures the power consumption [94] of the encryption device under test (DUT) and performs subsequent simple (SPA) or differential power analysis (DPA) of the obtained traces to decipher the secret key. For example, attackers target FPGA-based convolutional neural network accelerators by monitoring power and managing to recover input images from the collected power traces without knowing the detailed parameters in the neural network [95]. This is a devastating blow to the data security of online medical image analysis. One solution is to use noise insertion in power consumption measurements to defend against power side-channel attacks. In [94], the author shows that noise injection in the AS domain achieves SCA immunity with extremely high efficiency. Others solutions are balancing the power consumption of the rising and falling transitions and isolating the supply from the encryption engine. In [96], authors analyze the DPA resilience of FinFET cryptocircuits and design a 4-bit substitution box (Sbox-4) of PRIDE algorithm for new devices to be used in low-power applications. Besides, in [97], the authors presented a security countermeasure based on switching DC-DC regulators.

### 3.4.4 Electromagnetic SCA

Modern digital computer systems have many components that rely on electrical impulses, especially the CPU and RAM, to operate according to a clock signal in a coordinated sequential manner. Deduced from Maxwell's equations, the time-varying current could generate a corresponding electromagnetic field, containing a wealth of side-channel information related to software execution and data processing. The electromagnetic side-channel attacks are based on leaked electromagnetic radiation, which can be used to infer cryptographic keys using techniques equivalent to those in power analysis or non-cryptographic attacks, e.g., radiation monitoring attacks. To avoid such attacks, some researchers work on protecting associated encrypted currents. In [98], the authors utilize a signature attenuation hardware (SAH) encapsulating the crypto core locally within the lower metal layers such that the critical correlated crypto current signature is significantly attenuated before it passes through the higher metal layers to connect to the external pin.

### 3.4.5 Acoustic Cryptanalysis

Acoustic side-channel Attack, exploits sounds produced during a computation, which usually can be divided into two types: active and passive. For instance, just like radar and sonar systems, sound waves which are inaudible to the human ear can be emitted by the device's speakers, and access to equipment is obtained by tracking the movements of the human body, arms, hands, and even fingers [99]. And, by exploiting the sound that emanates from the pressed key, attackers could easily obtain the password [100].

### 3.4.6 Optical SCA

Optical emissions from semiconductors can leak important information about embedded devices, posing a major threat to their security. Attackers could extract sensitive information from a circuit by detecting that a switching transistor emits some light in the form of several photons in a short period of time. Reference [101] describes the first attack utilizing the photonic side channel against a public-key crypto-system in a "real-world" programming environment. The authors evaluate optical SCA with three common implementations of Rivest-Shamir-Adleman (RSA) [102] modular exponentiation and find that the key length had a marginal impact on resilience to the attack. For eliminating such attacks as Laser Logic State Imaging (LLSI), authors proposed low-cost, circuit-based self-timed sensors to detect critical steps taken by attackers when performing LLSI attacks on two attack surfaces, i.e., system clock (freezing) and supply voltage (modulation).

This section mainly focuses on IoMT devices and peripherals security issues. A clear summary of the security issues in the sensing layer has been shown in Table 3, including compromised features,

**Table 3.** IoMT Devices and Peripherals Security Taxonomy of State-of-the-art

Security Issues		Compromised Features	Mitigation	Representative Solutions
Software-based Security	Malware	Confidentiality	Anomaly detection	[70–72]
	Brute Force	Authenticity	Cryptography-based methods	[73], [74]
	Buffer overflow	Availability Integrity	Anomaly detection, re-randomize	[75], [76]
	Static Firmware Attack	Authenticity	Cryptography-based methods	[77–83]
	Dynamic Firmware Attack	Availability Integrity	Anomaly detection, Re-randomize	[77, 86–89]
Hardware-based Security	Electron Microprobe	Privacy Authenticity	Cryptography-based methods, Hardware redesigns	[57–62]
	Reverse Engineering	Confidentiality	Cryptography-based methods, Hardware redesigns	[63–65]
	Fault Injection	Confidentiality	Hardware redesigns	[66]
	Hardware Trojan	Confidentiality Privacy Authenticity	Cryptography-based methods, Hardware redesigns	[68], [69]
Side Channel Security	Timing	Confidentiality Authenticity	Software optimizations, Hardware redesigns	[90]
	Cache	Confidentiality	Anomaly detection, Re-randomize	[91–93]
	Power-monitoring	Confidentiality	Hardware redesigns	[94–97]
	Electromagnetic	Confidentiality	Cryptography-based methods, Hardware redesigns	[98]
	Acoustic cryptanalysis	Confidentiality	Hardware redesigns	[99], [100]
	Optical	Confidentiality	Hardware redesigns	[101]

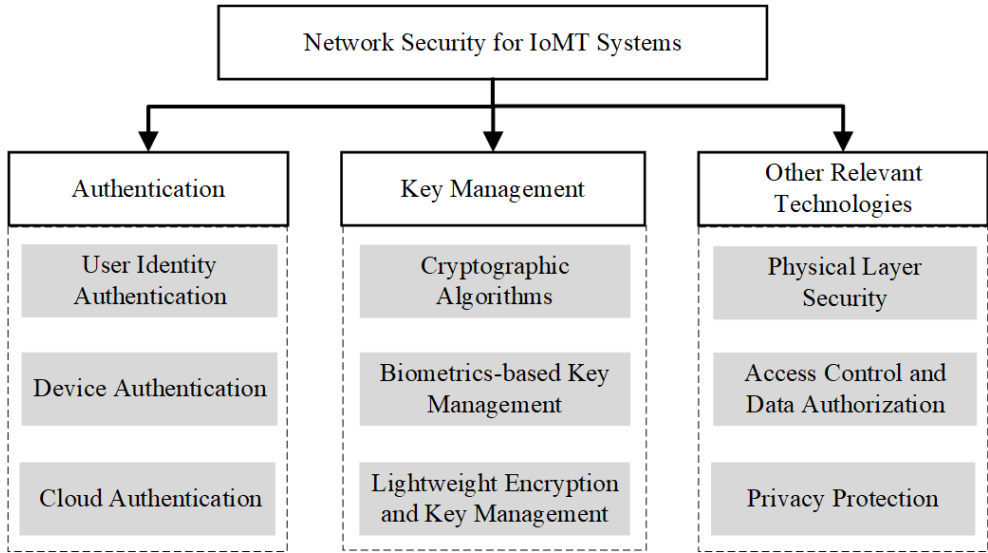
mitigation, and corresponding solutions. The security of IoMT devices still needs to face threats from the device itself and outside. The state-of-the-art work is mainly to continuously update the hardware and software design to adapt to emerging security threats.

## 4 State-of-the-art Security Strategies in Network Layer

Through recent innovations in electronics, wired and wireless communications, many diverse communication technologies and network structures have been introduced in IoMT systems which may help IoMT systems achieve optimum performance. As mentioned above, the sensors require connectivity to the gateways and the platforms established via networks communicating and storing information either locally or centrally. The communication is over wired and wireless medium and can be either short range or long range. Furthermore, various protocols for communications have been widely applied as mentioned above. Considering that the communications fundamentally rely on the backbone networks and infrastructures, thus the technologies of network security on this level generally applies to all usage scenarios. A major component of IoMT systems is wireless sensor networks, consisting of a large number of sensors connected via wireless communication technology that can collaborate to collect information of the covered area and allow external legitimate users to access the real-time data. The sensing data is mostly transmitted over public network connections, besides the sensors are often deployed in unattended or even hostile environment, which makes WSNs vulnerable to attack. Therefore, for the specific use of IoMT systems, we mainly discuss the security threats and countermeasures that may exist mostly in the sensor-based networks and the connections via wireless medium. The taxonomy is as shown in Figure 4.

### 4.1 Authentication

In IoMT systems, the security problem of data protection can be solved if the data source is authenticated through identifying malicious users and devices. Authentication refers to the identification of








**Figure 4.** The classification of network security for IoMT systems.

individual or group identity of users or devices by certain techniques. Normally, one-factor authentication uses one authentication technique to protect the system. In IoMT systems requiring higher level security, multi-factor authentication employs more factors to protect the system. This technique helps the system be resistant to cyberbreaks if one of the factors is compromised.

#### 4.1.1 User Authentication

For user-wise authentication, typically three types of information are employed: (1) Password-based authentication, based on “What You Know”; (2) Physical-based authentication, based on “What You Have”; (3) Biometrics-based authentication, based on “What You Are”. Considering that the biometric signals can be of specific availability and accessibility in IoMT systems, the biometrics-based authentication methods then play a unique and important role in user authentication which we will emphatically introduce herein.

- *Password-based authentication:* Static passwords [103, 104] can remain unchanged and be reused by users for a long time. The advantages of static passwords include its high availability, ease of use, wide application range, and simple deployment. Yet static passwords do not contain any of the inherent attributes of users and need to be remembered, stored and transmitted, which may cause severe security risks.
- *Physical property-based authentication:* Physical property-based authentication is implemented through the authorized hardware and software tokens and the information carried by them, such as smart cards [105], dynamic password [106, 107] and digital signature [108]. Instead of remembering the passwords, users need to carry the relevant hardware and software tokens personally. However, different companies manufacture their own devices, which prevented the scalability of tokens. In addition, it is very inconvenient to carry multiple tokens all the time and ensure that they are not lost. Smart card relies on physical keys, which are usually utilized as a second factor in multi-factor authentication methods, with the elliptic-curve cryptography (ECC) keys as the first factor for authentication [109]. In IoMT settings, the medical staff must first enter a key and then use their smart cards to access the system. Digital signature is generally used to verify the data/command authenticity by the user’s private and public keys for signature and verification, respectively. In IoMT systems, digital signatures can be integrated into the sensor’s firmware with an add-on software shim, intercepting

		Collectability	Security	Cost	Interference
Iris		Medium	Very High	High	Light
Voice print		High	High	Low	Cold
Finger print		High	Medium	Medium	Finger wear
Face		Very High	Medium	Medium	Age, Light, Shield
ECG		Medium	Very High	Low	Age, Cardiac disease

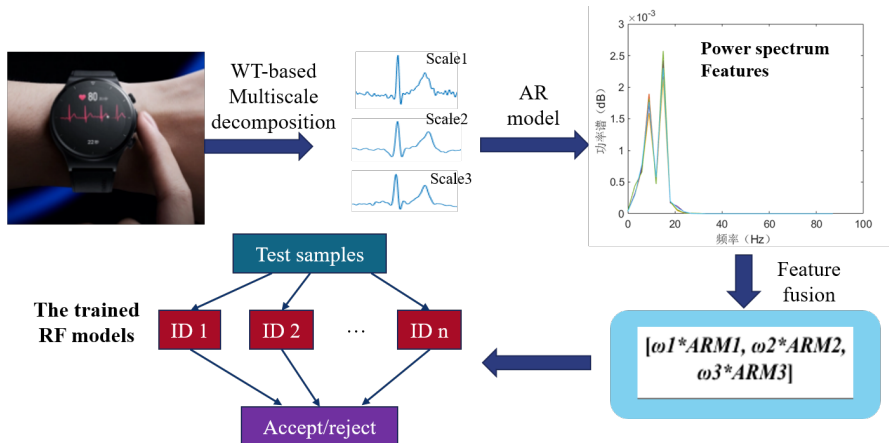
**Figure 5.** Comparison of several typical biometric features.

and validating the sensor's wireless communications [110]. The x-auth-token field in the hypertext transfer protocol (HTTP) header can also be used as a software token embedded in the user Web browsers [111]. Likewise, RFID can be used as a hardware token for secure logistic management of sensors in a hospital information system [112].

- *Biometrics-based authentication:* A typical authentication technology in IoMT is biometrics-based, utilizing user's unique biometric characteristics to prove its identity. Common biometrics mainly include physiological characteristics and behavioral characteristics. Physiological features are related to the user's physical shape, such as fingerprints [113, 114], facial features [115, 116], geometric features of hands and iris, etc. Behavioral characteristics are related to user behavior habits, such as signature (handwriting), speaking mode, gait, touch screen habit, etc. [117–119]. The biometrics-based authentication technology does not require users to remember or store specific identity information, besides it can establish a one-to-one correspondence between individuals and identities. Compared with other technologies, biometrics-based authentication is more secure, convenient and available. A brief comparison on several kinds of typical biometric features exploited for authentication is shown in Figure 5.

In medical care scenarios, either the professionals or the patients are permitted to access the medical records by using their biometrics only. The most commonly used biometric factors include fingerprint, face recognition, electrocardiogram (ECG) and electroencephalogram (EEG) that are handy in case of emergencies. The performance of the fingerprint-based sensors relies on the extraction algorithm exploited [120]. Fingerprint authentication has more credibility and a much longer history compared to face recognition, where systems can authenticate users by scanning their faces. ECG/EEG-based authentication have been developed in recent years, although in contrast with fingerprint-based technology, ECG/EEG-based authentication increases the computational overhead during transmission [121]. ECG/EEG signals are still the main physiological signals collected by the body sensor network [122, 123]. On the one hand, signals need to be collected from the living body, which is difficult to be simulated by other devices; on the other hand, the time series signals are easy to process.

Authentication depends primarily on the choice of the utilized feature(s). In past studies numerous features - temporal (locations and intervals among waves), amplitude (height of waves' peaks) and morphological differences (shapes, proportions, slopes and angles) - have been proposed to recognize individuals, requiring accurate detection of fiducials and the achieved results are dependent on the recognition procedure. Fiducial based approaches benefit of well-established normalization algorithms to compensate for changes in ECG signal due to the heart rate variability [124, 125] but they are commonly affected by the performance of the fiducials detection algorithms. To overcome



**Figure 6.** Flow chart of the multi-scale power spectrum feature extraction and identification in [126].

the problem, non-fiducial based approaches offer a promising alternative to reduce error rate and computational effort. New approaches that do not require fiducials recognition, have been reported: autocorrelation based features, phase pace analysis, and frequency based features. They do not require the identification of ECG waves and have the advantage to potentially take into account fine features which could be lost using fiducials. To get a better understanding of non-fiducial authentication, some representative works on the basis of different biometric features are described here in detail. In [126], the researcher for the first time proposed a multi-scale power spectrum feature extraction method based on wavelet transform (WT) and artificial recognition (AR) model (as shown in Figure 6). Through a one-to-one random forest classifier combination, a more accurate identity authentication is able to be implemented.

A typical behavioral characteristic, gait, has also been widely used for authentication. However, the gait recognition performance deteriorates dramatically when the walking speed varies. To address this issue, both the speed-adaptive gait cycle segmentation method and individualized matching threshold generation method were proposed [127]. Moreover, as the intra-subject gait fluctuation in older people is more significant than in young people due to changes associated with aging, gait-based identity recognition of the aged is more challenging. Researchers in [128] proposed a gait template synthesis method to reduce the intra-subject gait fluctuation of elderly and defined an arbitration-based score-level fusion method to improve recognition accuracy. Two matching algorithms are used to make preliminary decisions; if there are inconsistencies in the preliminary decisions, the third matching algorithm is used to provide the final decision.

- **Multi-factor authentication:** Recently, more and more enterprises and researchers [129, 130] use the user's biometric characteristics as a factor in the multi-factor authentication technology. Research in this area focuses on how to effectively and quickly extract, measure, and compare unique parts of biometrics, and then treat them as a special identity of the user. For example, while using shared keys as a first factor, face recognition can be the second factor in continuous role-based authentication [131]. By continuously scanning the user's face, this technique helps keep the connection between the sensor and the medical controller in the gateway layer secure. It can prevent the medical staff with lower privileges from accessing the patient's data in the absence of a higher privileged medical staff that has authenticated himself/herself but has not logged out from the system. However, due to the limited and unchangeable property of biometric characteristics, the security threat caused by biometric data leakage is irreversible. As a result, more and more users are afraid to upload their biometric data to remote servers that could be maliciously stolen.

### 4.1.2 Device Authentication

For device-wise authentication, the characteristics of the device itself are commonly considered.

- *Digital fingerprints:* Device device fingerprint is used as a label to confirm the identity in device authentication. Similar to the concept of human fingerprint, device fingerprint refers to the device identification composed of feature information. Based on the source of information, device fingerprints can be classified into software fingerprints and hardware fingerprints. The feature information of software fingerprint comes from device ID, browser information and device software environment [132–134]. Hardware fingerprint comes from the hardware structure [135], RF device [136, 137], accelerometer [138], gyroscope [139], microphone [140], speaker [141], camera [142], Bluetooth [143] or the combination of the above devices [144, 145].

The most commonly used physical attribute of a device is a Physical Unclonable Function (PUF). It is a physical change collected naturally in the production process but can not be cloned. Besides, it is difficult to predict for external attackers. Therefore, PUF is often used as the "digital fingerprint" of the device and combined with cryptography technology to ensure the security of the device. These studies [146, 147] take PUFs as one of the authentication factors and propose a multi-factor authentication scheme for privacy protection of Internet of Things devices or other applications.

- *Context awareness:* Context awareness-based authentication is able to establish the secure communication between devices and between devices and networks by verifying physical proximity. It can be divided into validation using the inherent properties of the device [148–150] and validation using human behavior [151–153]. Some researchers [154, 155] put forward that certain behavioral characteristics of users can be taken as one of the factors to authenticate a user. In these studies, the author uses smart devices (e.g., Wi-Fi, smart TV, monitoring equipment, etc.) to obtain the physiological and behavioral characteristics of users in their daily use of these devices, and extracts representative behavioral characteristics from them.

### 4.1.3 Cloud Authentication

Cloud authentication can provide identity authentication that verifies the pairing relationship between an IoMT device and human users. The strong user authentication method can firmly restrict illegal access to the cloud provider and it is also the key requirement to ensure cloud security. It is the mandatory requirement for the cloud to ensure only permitted users can access the resources and services.

- *Unauthorized User* Cloud computing provides resources and services open for public use. When the patients migrate their medical data to the public cloud, they will lose tight control of the data. The unauthorized users can deliberately access the cloud data to obtain sensitive information for various reasons. For example, the cloud service provider can guess the user is ill by collecting the information about the users' access to certain medical products. Therefore, access permission should be carefully given to the specific users who manage the cloud [156]. Sethi et al. [157] proposed deep reinforcement learning-based adaptive approach to prevent unauthorized users along with their attacks. The benefit of this approach is that it can overcome the limitations of transitional intrusion detection systems that cannot handle novel attacks.
- *Eavesdropping* The malicious user can use network eavesdropping to attempt to get access privilege and unauthorized access to the medical data managed in the cloud. The attacker can intentionally infer the users' private data without authorization. Moreover, the data can be made incorrect or unavailable. Chhabra et al. [158] presented a security approach to prevent eavesdropping attacks in the cloud based on Elliptic Curve Cryptography, which can also secure the services deployed in clouds. The widely used access control approaches can also be utilized to avoid this security issue in browser [159].
- *Insecure APIs* Cloud can provide multiple Application Programming Interfaces (APIs) to make them open to add new components to enhance the functions. However, insecure APIs can expose the environment to malicious threats. For instance, Alibaba's identity APIs support users to access the website via their AliPay account, where the users can interact with the login information, and APIs

authorize and fetch the account information. Moreover, poorly coded APIs may also grant unnecessary access to sensitive data. To prevent this issue, the APIs for cloud resources should be carefully designed to check possible vulnerabilities and timely updates should be packed [160, 161].

## 4.2 Key Management

Key management, as the core component of system security based on cryptography, is essential to secure IoMT systems. Symmetric cryptography includes cryptographic algorithm based on a secret/shared key; whilst asymmetric cryptography using two keys: a public and a private, with one of them for encryption/validation, and the other is used for decryption/signature. Symmetric cryptography has become a focused research area of key management due to its short key length and relatively small cost on communication and computation. To implement asymmetric cryptographic algorithms, such as Diffe-Hellman algorithm, a certain amount of resources are demanded. Therefore in IoMT systems which contain a lot of resource-constrained sensors, specific schemes should be developed exploiting the unique characteristic of medical applications. We divide this subsection into three categories: 1) Cryptographic algorithms; 2) Biometrics-based key generation; and 3) Lightweight encryption and key management.

### 4.2.1 Cryptographic Algorithms

Cryptographic hash function (CHF) is a one-way mathematical function that converts an arbitrary size data to a fixed size. Exclusive-OR (XOR) can be used to check if one of its operands is different. Initial parameters (i.e., a sensor ID and a shared key), after being XORed and then hashed, are shared from the key generation server to the sensor and gateway nodes. These nodes can then generate their keys with the help of these parameters. Combining the CHF, a symmetric key, and the XOR operator can secure the communications in IoMT systems using key agreement protocols proposed in [162, 163]. To solve the problem of insecure key sharing in symmetric cryptographic algorithms, CHF function along with ECC keys, can be taken as a secure certificateless channel between the patients and their physicians as well [164]. This idea allows for secure key sharing between the key generation server in the cloud layer and the nodes in the IoMT sensor and network layers, respectively. The ECC public key and initial parameters are hashed using CHF before sending to the nodes. The nodes then generate asymmetric keys. This technique can also overcome the overhead in certificate management for data storage and sharing in the cloud [165]. By dividing the patient's data into subsets and converting them with ECC keys and CHF, they can be securely shared among the system's entities. The average energy consumption in this technique is around 30% less than similar techniques. ECC has gradually been growing in popularity recently due to its smaller key size and ability to maintain security. To meet the confidentiality and integrity requirements of medical applications, a novel enhanced secure sensor association and key management protocol based on ECC and hash chains has been designed [166]. Other than satisfying the privacy demand of patients on medical systems, the proposed protocol is also easy to implement with even higher efficiency.

### 4.2.2 Biometrics-based Key Management

The biometric sensors used to identify users' physical characteristics are the most common technique employed to provide security for IoMT systems. Based on the randomness and high similarity of synchronously detected time-varying physiological signals collected by biometric sensors, dynamic physiological features can be extracted to realize the secure key management, including key generation and key distribution.

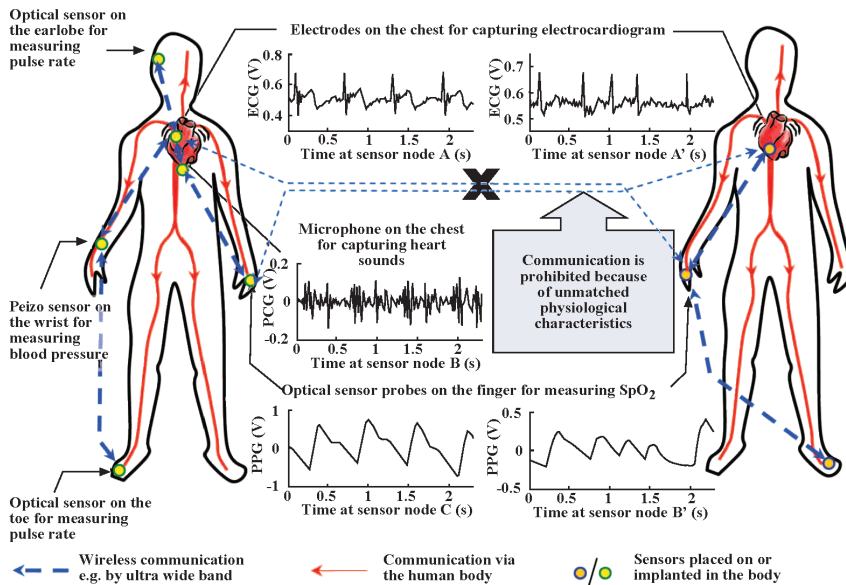
Bio-cryptographic technique is an efficient approach to generating cryptographic keys since it does not require key pre-distribution mechanism or proper network setup to generate the key. In addition, this approach provides an opportunity to re-keying automatically. Bio-cryptographic key generation schemes are normally based on physiological features that are random and unique and are optimal for cryptographic keys [167]. Different researchers used such metric to generate keys that are discussed below. The researchers in [168] proposed a bio-cryptographic key management protocol to secure



communication of implantable and wearable medical devices. To generate secure cryptographic keys, psychological parameters were utilized including blood pressure, ECG and PPG tracked by sensors. Two physiological parameter generation approaches including time-domain generation to derive Inter-Pulse-Interval (IPI) and frequency-domain to derive cross power spectral density (CPSD) are proposed. Both are important candidates to be cryptographic keys due to their randomness and temporal variance characteristics. Similarly, heartbeats based random binary sequences (RBSs) [169] is another approach to secure communication of sensory medical devices. This research used finite monotonic increasing sequence generation mechanism and Hamming distance metric to excerpt entropic bits from IPI derived from ECG. From each signal, 16 random bits could be excerpted and through a concatenation of 8 consecutive IPIs, thus 128-bit RBSs are generated to authenticate users. Gait-based technique uses the human walking pattern to generate unique symmetric keys. A system proposed by Sun and Lo can generate a symmetric key using a set of IoMT sensors attached to the individual's body in just a matter of ten gait-cycles. They claim that their system can generate three times the number of bits per gait cycle than those generated by similar state-of-the-art techniques [170]. The gait cycle is defined as one cycle of movement between two repetitive events while walking. This system employs an artificial neural network (ANN) model to generate 13 bits per gait-cycle, which will generate a 128-bit key in just a matter of ten gait-cycles. This key can be used to secure the communications between the IoMT sensors and the access point or mobile devices in the gateway layer. It outperforms finger-based systems by generating binary keys at different times, which provides randomness to the keys without direct user interaction with the system. Besides key generations, the bio-cryptographic technique also ensures key sharing among nodes having contact with the body. These schemes assure security without necessitating any human interference by eradicating the prospect of overlooking secret keys.

For the sensor-based networks mostly applied in IoMT systems, especially for those located on or in the human body, the nodes are expected to be interconnected, and the body itself can form an inherently secure communication pathway that is unavailable to all other kinds of wireless networks. Researchers explore the use of this conduit in the security mechanism of body-area sensor networks (BSNs); that is, by a biometrics approach that uses an intrinsic characteristic of the human body as the authentication identity or the means of securing the distribution of a cipher key to secure inter-BSN communications [171]. The technique is developed based on a symmetric cryptosystem, which assumes that a robust and secured key distribution scheme is available. In this respect, random numbers produced from physiological signals are used to encrypt and decrypt the symmetric key for secured distribution. In Figure 7, at the transmission terminal, the biometric trait was used to commit the key; at the receiving terminal, the other biosensor would capture its own copy of the trait and use it to decommit the key. If the selected characteristic is unique enough to represent an individual, the encryption key should only be recovered by the trait that is obtained from the same individual. Researchers came up with a specific symmetric bio-cryptosystem for BSN, which considered the generation of the encryption key from physiological signals and its randomness evaluation. This biometric solution is suitable for securing BSN in IoMT because a higher security level can be achieved with less computation and memory requirement. In addition to securing the transmission of the encryption key within the nodes of a BSN, the biometric trait can also be used as an identity for entity authentication (i.e., node-to-node authentication) in a BSN. A possible two-session communication protocol was discussed where the server initiated by sending out the biometric trait together with a nonce to the client for comparison and if matched, the client responded by sending back the nonce together with the variant biometric trait. A communication pathway would only be established if both the server and client found that the received copy matches the copy it has in hand.

Another scheme for key sharing is based on fuzzy pattern recognition, mainly including fuzzy vault for secure key distribution, which is suitable for features from disordered or irregular physiological signals [172, 173]. Shared symmetric key is used to allow communication and require one entity to project security attributes calculated from physiological signals on a polynomial and transfer the attribute points along with chaff points to the other side that would recreate the polynomial centered on some common attributes. This scheme improves security by minimizing the rate of data exchange during the key management process and thus increases network lifetime and energy efficiency [174]. However, the security of such scheme is entirely dependent upon the weak vault size because of the small size of attributes [175, 176] demonstrated that an adversary is capable of estimating appropriate points in the vault.



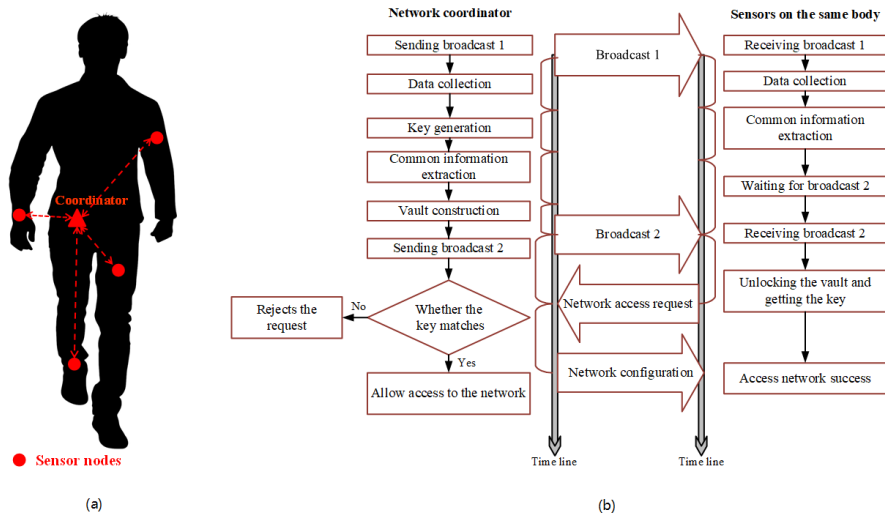
**Figure 7.** An illustration of applying the biometrics approach to secure inter-body area sensor network communications [171].

#### 4.2.3 Lightweight Encryption and Key Management

In IoMT application environment, some terminal nodes have limited resources, including computing resources, storage and communication resources. Traditional symmetric encryption methods, such as Data Encryption Standard (DES) [177] and AES, can ensure the encryption and decryption rate of stored data, but their key management is complicated for constrained nodes. Moreover, traditional asymmetric encryption methods, such as RSA cryptographic algorithm, are not suitable for dealing with the ever-increasing data from a large number of users and devices, although their keys are easy to manage. In this case, lightweight encryption and key management is required, especially in sensor-based networks. For IoMT systems containing a large number of wireless sensors and mobile devices, researchers in [178] designed a key management and authentication protocol based on symmetric cryptography using only hash functions excluding the public key based ECC, in which sensors with limited capabilities only need to perform lightweight symmetric encryption schemes.

Reference [179] and [180] presented a vibration-based lightweight key exchange protocol and ultra-low battery resilient mechanism between external and wearable device. The external device produces key and modifies it into a vibration signal. On the other side, the wearable receives and transforms signals into bit string using the two-feature On-Off Keying (OOK) demodulation mechanism to encrypts further communications. However, the vibration-based scheme has a defect, i.e., an adversary would be capable of extracting keys from vibration signals since they are acoustic and electromagnetic waves that can be captured. In [181], an optical secure communication channel between an implantable medical devices and an external device is introduced, enabling an intrinsically user-perceptible unidirectional data transmission, suitable for physically-secure communication with minimal size and energy overheads.

Biometric features, as one significant characteristic of IoMT systems, can be exploited to support lightweight key management as well. Reference [182] proposed a lightweight noise-based group key generation method exploiting gait features (as shown in Figure 8), which utilizes the noise signals imposed on the raw acceleration signals to generate an M-bit key with high randomness and bit generation rate. Moreover, a signed sliding window coding (SSWC)-based common feature extraction method was



**Figure 8.** An overview of the lightweight noise-based group key generation method exploiting gait features in [182]. (a) Overview of the proposed wearable sensor network; (b) Overview of the network access process.

designed to extract the common feature for sharing the generated M-bit key among devices worn on different body parts. Finally, a fuzzy vault-based group key distribution system was implemented and evaluated using a public dataset.

In biometrics-based security solution, entity identifiers (EIs) of each node in a BSN were generated for securing the distribution of keying materials. Due to slight differences in the biometric traits collected from different parts of the same subject, fuzzy schemes, such as fuzzy commitment and fuzzy vault, were used to protect the transmission of keying materials using generated EIs. One example of generating EIs is to use the IPI calculated from ECG and PPG signals, about 30s of ECG/PPG signals are required to generate a 128-bit EIs in such solutions [183]. Authors in [173] proposed a lightweight and resource-efficient biometrics-based security solutions, especially aiming at the energy-constrained body-area sensor networks. In this study, an improved key distribution solution with the energy distribution information of physiological signals (EDPSs)-based EIs was proposed. Only 5s of ECG/PPG signals are required in the proposed solution, enabling rapid EI generation and key distribution. User-dependent fuzzy vault was proposed to secure key distribution with high recognition rate. The performance of time-varying randomness and identification rate are evaluated to examine EIs' feasibility in securing the transmission of keying materials.

Considering that the IoMT systems need to accommodate various end users including a mass of sensor-based devices, the hierarchical network structures such as fog computing and edge computing are employed to improve the network capacity and efficiency. To cope with the security challenges after introducing fog computing, a new security architecture for fog computing which protects privacy and supports device-to-device (D2D) communication is designed in [184]. On this basis, three corresponding two-factor anonymous authentication protocols are proposed, which adopt one-way function, XOR operation and other lightweight methods, all suitable for edge devices with limited computing capacity. In another multi-factor authentication method, a pattern-based technique uses a tab pattern generated to be performed by the patient to control the sensor [185]. This technique can keep the sensor communication turned off until a specific pattern is performed, preserving the sensor's battery power. After successfully passing the first factor with the medical controller in the gateway layer, the controller sends a random tab pattern as a second factor to the user before executing a sensitive command.

## 4.3 Other Relevant Technologies

### 4.3.1 Physical Layer Security

In IoMT environment, data transmission is mainly based on wireless networks, especially in WSNs. However, wireless network is vulnerable to eavesdropping, interference, forgery and other threats. Traditional network security mechanism requires complex interaction protocol design and extra bandwidth resources. In this case, a new mechanism to realize communication security emerges, by using physical layer signals of wireless network. Physical layer security mechanism utilizes the characteristics of physical channels, such as time variability and mutuality, and has the advantages of low energy consumption, high security and low computational complexity.

Nowadays with 5G communications, technologies such as Multiple-input multiple-output (MIMO) and Orthogonal Frequency Division Multiplexing (OFDM) are conducive to construct physical layer security scheme [186]. Physical layer security is derived from information theory security, and current research focuses on identity authentication, channel coding, shared keys, multi-party computation, etc.. Wyner [187] was the first to point out that secure message transmission could be realized by designing appropriate codes in insecure channels, which was also the first time that the concept of secure coding was put forward. Against unauthorized users, a cooperative strategy with a helper's interaction based on the wiretap channel capacity was proposed in [188]. Maurer [189] first proposed the use of channels to achieve key generation and distribution. In [190], information theory method is used to generate and distribute secure keys, which were extracted and generated from communication channels. The random character of wireless channel is used to generate secure key independently through multipath [191, 192].

Wireless signal characteristics are utilized to secure IoMT systems by generating keys without prior connections. The radio signal strength (RSS) is one of these characteristics, and it measures the received signal power, which varies based on the medium it passes through. Implantable medical devices can be excellent candidates for this technique specifically since the RSS value variation inside the human body is different from outside the body [193]. The proposed technique uses the randomness in RSS values to generate a shared key. This key can be used to secure the communication between a headless cardiac pacemaker and a subcutaneous (under-the-skin) implant without prior knowledge of the keys. In this technique, two bits can be extracted from a single cardiac cycle (a beat) with a 128-bit key in 60 seconds if we consider the average human heart rate of 64 beats per minute (bpm).

### 4.3.2 Access Control and Data Authorization

By restricting access to the key resources, unauthorized users are prevented from intruding or damaging the access to the systems and the data. In this way, network resources can be legally used. A role-based access control strategy was proposed in which the motivation is that different roles are endowed with different access control permissions. In view of the spatial-temporal relevance of data, Ray et al. [194] introduced location information grounding on role-based access control (RBAC) policy. The location of user's determines whether it has the right of data access. The scale-based space-time RBAC model proposed by Zhang et al. [195] enhances the expressiveness of access control policies and the security of the model. Attribute-based access control (ABAC) [196] sets access permissions by comprehensively considering various attributes, such as users, resources, and environments. In contrast to the user-centric approach in RBAC, ABAC takes into account all dimensional attributes to achieve fine-grained access control. On the basis of ciphertext attribute encryption, researchers in [197] proposed a method that formalized public and private keys into permissions and implemented access control by designing these keys. Ruj et al. [198] proposed an access control framework that can realize privacy protection and authentication for big data in the cloud. Especially, hierarchical access control is employed to allow hierarchical access to data of patients which is privacy-sensitive. One representative approach utilizes a hierarchical role-based model to provide authorization based on the user's role [199]. For example, all authenticated nurses can administer medicines, but prescribing a new medication requires a person authenticated as a doctor. The model supports a relatively low complex hierarchical security scheme that encrypts the patients' data and only decrypts part of the data to which the user is authorized.

As the system architecture shown in Section 2, data from sensor-based end user networks are mostly uploaded to cloud servers through gateway nodes (such as mobile phones, tablets, etc.). In [200], authors pointed out that it is difficult for mobile networks and cloud computing to ensure data security and privacy. Homomorphic encryption (HE) preserves data confidentiality and allows limited mathematical operations to be done on encrypted data. This technique protects the patient's data privacy and stores them as ciphertext in the cloud layer to do mathematical operations, such as data integrity. However, it differs from other techniques for allowing the patient only to see their own data but not the professionals except during emergencies. In other words, it applies for certain IoMT sensors, such as a smartwatch, which allows the data to be encrypted at all times and only seen by the patient except in emergencies where the patient's data can be sent to the professionals to diagnose. There are three different schemes for HE: 1) partial HE (PHE); 2) somewhat HE (SHE); and 3) fully HE (FHE). PHE supports one mathematical operation for an unlimited number of times, while SHE supports only a limited number of operations. FHE supports an unlimited number of operations, and therefore, it can be suitable for fast aggregation of data without compromising data confidentiality [201]. Hence, it is ideal for healthcare monitoring systems in hospitals. Optimal HE is a modification of FHE. It differs from FHE in that it is based on the step-size firefly optimization (SFFO) algorithm in which the key with the maximum breaking time is selected [202]. This technique reduces the computation time and increases the breaking time by 2%–8% compared to other HE and non-HE techniques individually.

### 4.3.3 Privacy Protection

During communications via IoMT networks, especially via wireless networks, each interaction of users inevitably generates a large amount of personal data, which is easy to be attacked by malicious attackers in the process of data sharing, posing a serious threat to privacy. Two categories of technology are described as below, from the aspects of data communications.

- *Data transmission-based:* Data distortion technology [203] realizes privacy protection by perturbation of the original data. The distorted data should meet the following requirements: first, the attacker cannot discover the original data. In other words, attackers cannot reconstruct the original data from the published distorted data. Second, the distorted data still maintain some original properties, that is, information derived from the distorted data is equivalent to the information derived from the original data, which ensures the feasibility of some applications based on the distorted data. At present, privacy protection technologies based on data distortion include randomization, blocking, information exchange, condensation, etc..
- *Network structure-based:* In IoMT systems, the heterogeneous network consists of distributed structures. Secure multiparty computation (SMC) [204] is extensively applied in distributed environment. Typically, privacy protection can be described as the SMC problem in the absence of a trusted third party [205, 206]. That is, each of the two or more sites is only aware of its own input and the output of computation for all data, and does not disclose any information. Distributed clustering uses encryption technology to secure data transmission. The key of this method is to ensure the security of distance calculation between data.

To conclude this section, a brief summary of network tier security is listed in Table 4 as below. We mainly focus on the connectivity between the sensing tier and the cloud infrastructure tier, where typical technologies of authenticated visiting, encrypted data sharing and reliable system maintenance for IoMT applications have been sorted to provide a comprehensive understanding. In general, most of the common security solutions for existing network systems are applicable for IoMT systems. On the one hand, it is not necessary to apply too many alterations to the devices/servers of IoMT systems; on the other hand, novel technologies are required to adapt the specific IoMT applications. For authentication and key generation in the personal server level, the use of biometrics is particularly applicable in the IoMT systems, as most of the biometrics can be easily collected from medical and healthcare devices worn by or implanted in the human body. These technologies can offer a significant advantage to IoMT systems with the unique strength of biometrics. Considering a wide range of restricted devices, secure but lightweight schemes should be designed. Yet the existing solutions always have to make compromises in security performance for limited capabilities.

**Table 4.** IoMT Network Security Taxonomy of State-of-the-art

Security Issues		Compromised Features	Mitigation	Representative Solutions
Authentication	Unauthorized users, Eavesdropping	Authenticity	User Identity Authentication	[103–131]
	Spoofing, Impersonation	Confidentiality / Privacy	Device Authentication	[132–155]
	Insecure APIs		Cloud Authentication	[156–161]
Key Management	Information leakage, Sniffing, Eavesdropping	Confidentiality / Privacy	Cryptographic Algorithms	[162–166]
	Tampering, Relay, Replay	Integrity	Biometrics-based Key Management	[167–176]
	Resource depletion	Availability	Lightweight Encryption and Key Management	[173, 178–185]
Other Relevant Technologies	Unauthorized users, Eavesdropping	Confidentiality / Privacy	Physical Layer Security	[186–193]
	Relay, Replay	Anonymity	Access Control and Data Authorization	[27, 194–201]
	Interruption		Privacy Protection	[203–206]

## 5 State-of-the-art Cloud Security for IoMT Applications

Cloud is the infrastructure of the Cloud-based IoT system, which consists of computation and storage resources to process and store the data fetched from the sensors. The cloud is designed as scalable, geographically independent, transparent to users, and on-demand provisioned resources. Due to these attractive features, the cloud has been applied as the prevalent platform for many IoT devices, including IoMT devices targeted for the medical area. The Cloud can serve with the functions as (1) identity authentication that verifies the pairing relationship between an IoMT device and human users, (2) data storage that stores the data collected by the IoMT devices and their operational data, such as log data and runtime data, (3) data analysis that processes the fetched data or provides the analyzed data with visualized results. Based on the investigation, we have classified the cloud security for IoMT applications as hardware security, cloud storage security, and virtualized platform security. The taxonomy based on the classification is shown in Figure 9.

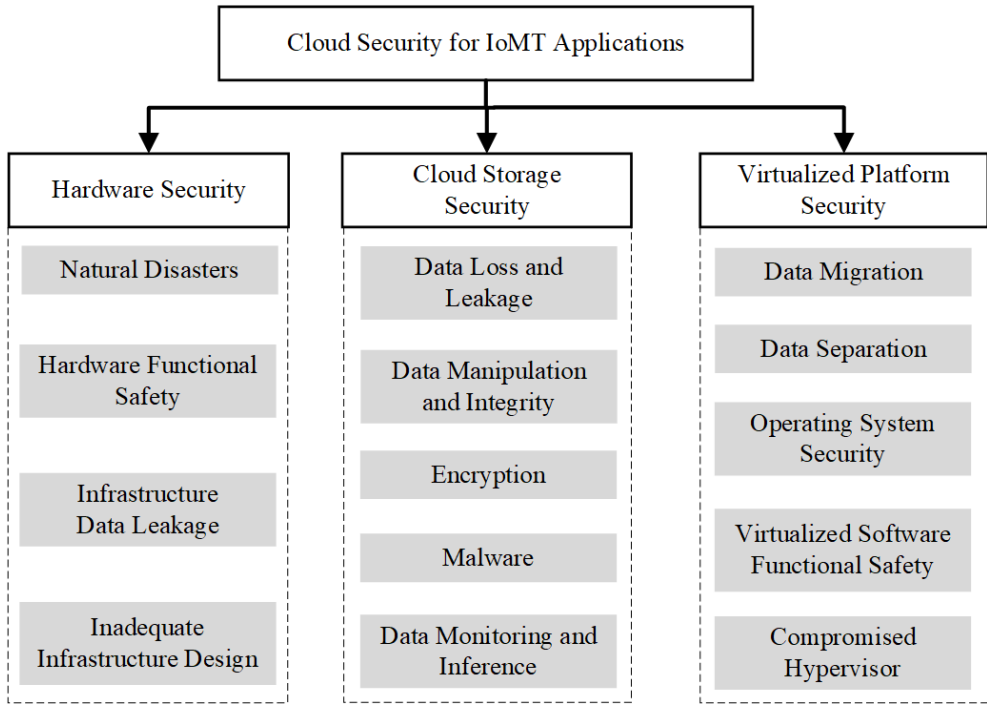
### 5.1 Hardware Security

In this section, we discuss the security issues related to hardware that supports the physical environment of the Cloud. Moreover, potential solutions are also given.

#### 5.1.1 Natural Disasters

Natural disaster happens occasionally due to the geographical location and seasonal climate. The hardware in cloud data centers can be exposed to disasters (extreme weather) like thunderstorms, floods, and earthquakes, which can all influence the availability of the cloud infrastructure and the services running on it. Amazon cloud data centers have experienced a power outage in Sydney data center in 2016, making various bank cards of many users temporarily useless<sup>1</sup>. For the eHealth system that manages the medical data can also face this problem if the disaster happens. Therefore, the locations of cloud data centers should be carefully selected to avoid the natural influence [207], and disaster recovery solutions should be prepared [208].

<sup>1</sup><https://www.smh.com.au/technology/web-chaos-mostly-over-after-amazon-web-services-hit-by-power-outage-during-sydney-storm-20160606-gpc707.html>



**Figure 9.** The classification of cloud security for IoMT applications

### 5.1.2 Hardware Functional Safety

This kind of safety issue lies in functionalities of hardware, ranging from switches to physical servers in cloud data centers, which can make the cloud services inaccessible [209] [210] and functionality degradation. The US cloud storage supplier, Swisssdisk, has suffered from an unplanned and unpredictable catastrophic hardware failure, resulting in the users cannot access their data. After that, the company decided to spend considerable resources on a more state-of-the-art platform. Resource replication and erasure coding are prevalent approaches to ensure hardware availability [211]. Trade-offs exist in these approaches in terms of durability, network bandwidth, energy consumption, and recovery performance. To avoid the issues in hardware functional safety, it is also required the hardware development process to be adapted to the requirements of some standards, such as ISO 26262 for functional safety of electrical or electronic systems.

### 5.1.3 Infrastructure Data Leakage

This kind of issue represents the key administration information that is leaked to the malicious users, which leads to the misuse of cloud resources. Digital currency mining, email spam, and phishing attempts are some representative examples. When the attacker can access the hardware resources directly, the cloud provider can bear the immense loss. For instance, an attack uses the leaked data to get the full privilege of cloud resources and launches a set of power virtual machines to run the currency mining tasks, which can consume a huge amount of resources and electric power. Kiara et al. [212] proposed authentication methodology and multifactor user authentication (e.g. special keyboard and server-side authentication code to prevent infrastructure data leakage by unauthorized access. Chen et al. [213] presented an infrastructure framework for community medical internet of things, which includes transmission protection, storage protection, and access control based on different encryption schemes.

### 5.1.4 Inadequate Infrastructure Design

This issue is caused by the cloud provider failing to notice the potential bursts in the number of users, which leads to insufficient resource provisioning for the applications. For instance, huge traffic comes into the single point of the critical physical node, leading to unacceptable delays and SLA violations. The Sina Weibo application can always meet requests burst due to hot topics [214], and this can also happen in the IoMT application, such as many users accessing the same application by checking their information. To address this issue, property resource scheduling policies should be designed, such as auto-scaling approaches that can dynamically add/remove resources in cloud data centers [215], and accurate workload prediction algorithms that can forecast future trends [216].

## 5.2 Cloud Storage Security

In this section, we discuss the security issues related to cloud storage as well as the promising solutions to address the corresponding issues.

### 5.2.1 Data Loss and Leakage

Data loss and leakage in cloud storage can result from intrusion action or disk corruption without redundancy. This serious security issue can significantly influence the privacy, trust and affect the service level agree negotiated with cloud users. The data leakage can affect the normal maintenance of IoMT applications, e.g. the administration password is leaked, where the malicious users can leverage the permission to operate data stored in the cloud. Kaur et al. [217] have discussed some existing approaches to protect data leakage, which include techniques such as local scanning of data and remote scanning. The agents installed on the devices will conduct the examination regularly to avoid data loss and leakage.

### 5.2.2 Data Manipulation and Integrity

A malicious attacker that has got the privileged access to the cloud infrastructure can have a variety of techniques to achieve their objectives. To manipulate the data in cloud storage, an attacker who gets the full controls over the data blocks, can read, insert, modify, and even corrupt the data in cloud storage. Full control over the storage allows the attacker great power to injure the confidentiality, integrity, and availability of customer data. As a result, we observe that this kind of attack has become the mainstream to hurt cloud storage security. Huang et al. [218] designed an attribute-based proxy re-encryption algorithm to avoid data manipulation for the eHealth system based on blockchain. Taking advantage of the traceable and tamper-resistant features of blockchain, any entity that had an illegal manipulation of data will be held accountable for the evidence. Manipulation can hurt the data integrity that refers to the integrity of customer data. However, in the cloud computing environment, the users access their data stored in the cloud in a distributed manner, which can suffer from the consistency issue under the security property. Although the cloud applications can rely on the guarantees of cloud service providers to some extent, the vulnerabilities can also be brought by incomplete security examinations, such as the errors caused by the global clock. Pandey et al. [219] investigated data integrity techniques in the medical area, which can leverage blockchain-based approaches [220] and masked authenticated messaging [221].

### 5.2.3 Encryption

In cloud environments, it is required to keep sensitive data secret while providing normal utilization of data. Encryption is the essential mechanism to ensure data confidentiality by protecting data, communication, and activities in the cloud from malicious users that aim to disrupt the normal running of the cloud. A significant amount of work has been investigated to achieve confidentiality while also targeting other properties like integrity, availability, authenticity, and privacy [222]. Cryptographic technique based on attribute-based encryption aims to provide privacy and fine-grained access control, including proxy re-encryption, revocation mechanism and hierarchical attribute based encryption [223] [224] [225] [226].



### 5.2.4 Malware

The malware refers to the malicious programs injected into cloud storage, which can make the host join into the zombie network and keep adding new hosts into the network. The hosts can be either physical machines or virtual machines in the cloud environment. It is reported that half of the downloaded malware can disable the local security in one minute. Threats that combine the new technique and traditional evasive attack are quite popular in harming security, which even makes a term named malware-as-a-service. A significant amount of effort has been devoted to detecting the malware efficiently [227], for instance, Watson et al. [228] proposed an online anomaly detection approach based on the support vector machine with high detection accuracy. The approach can also detect new malware without prior knowledge of functionalities. Yadav et al. [229] presented a consolidated weighted fuzzy k-means clustering method to identify malware with high precision.

### 5.2.5 Data Inference

In addition to the manipulation of data, a malicious attacker can also observe and analyze the access pattern of users to predict the data that the user stores in the cloud, which is called data monitoring and inference. The standard encryption approach cannot function well to hide the access pattern. Therefore, with this kind of attack, the attackers aim to compromise the confidentiality of the data used by the cloud customers. Inference represents the data mining approach to explore the data hidden behind the common users. In a cloud storage scenario, the data inference indicates the database system technique to injure databases. The attackers aim to infer the sensitive data from the databases with a high-level perspective. This kind of attack can compromise the entire database. If inference problems are not addressed properly, the sensitive information may be exposed to outside users. To ensure efficient and fine-grained access to electronic health records, Zhang et al. [230] proposed a multi-phase access policy to achieve an inference attack-resistant system. Each data attribute in records is encrypted individually, and the Cloud will execute the computational intensive data without knowing the sensitive data. Ma et al [231] proposed an inference-aware mechanism in multi-task learning, which can resist the inference attack through the immediate results. Deznabi et al. [232] analyzed the genomic data based on the Markov decision process and provided a message-passing algorithm to avoid inference attacks on genomic privacy.

## 5.3 Virtualized Platform Security

In this section, we discuss the security issues related to the virtualized platform that provides the physical or virtual resources to support the execution of IoMT applications, and the corresponding solutions are also highlighted.

### 5.3.1 Data Migration

VM live migration is a significant feature in a traditional cloud computing environment to move VM from one place to another, which can optimize resource usage. For the cloud-native applications that shifted the monolithic applications into light-weight ones, containers developed via microservice architecture can also be migrated/rescheduled from one physical host to another. However, security problems can be triggered during the migration process, for example, the data is not transferred completely and leads to consistency problems, which can also be attacked by malicious users to make useless migration to consume resources and undermine system performance. Shakya et al. [233] proposed a framework for security analysis and security protection during data migration. Sighom et al. [234] discussed a set of encryption approaches to investigate the elements that can affect system performance. After that, they also proposed an enhanced model based on existing protocols with provable security assessments.

### 5.3.2 Data Separation

Cloud supports multi-tenant scenarios by sharing resources for multiple users. To leverage the power of the cloud, generally, the users need to migrate their data to cloud. However, some users avoid putting sensitive data to the public cloud, which requires data separation [235]. The data separation aims to ensure the data is well partitioned, i.e. the user can access the data in his domain and cannot be used in other domains. However, during the process of separating data, the sensitive information can be leaked and have high risks. If the data is separated in physical devices, the data can have loss or disclosure due to the data is not fully formatted or used by other tenants, which can increase the costs. Meanwhile, due to the geo-location feature of data, the complexity to handle the security of the data separation is also increased. A significant amount of recent research has contributed to the area of mobile edge/cloud computing area, which can efficiently address this issue. For example, Wu et al. [236] [237] proposed data separation approaches based on neural networks to transfer data between cloud and mobile devices. In this way, the sensitive data can be managed locally.

### 5.3.3 Operating System Security

With the heterogeneous nature of cloud computing, different kinds of operating systems (OS) working together can bring a set of security issues. For instance, vulnerabilities exist widely in preventing operating systems to function normally, such as Windows, Linux, and iOS. These operating systems need to update or patched frequently to solve the security problems. In the desktop OS, the remote code execution vulnerability bug can allow the remote unauthenticated attacker to run codes by sending network packets and getting the control of the OS. In the mobile OS, the increasing popularity of smartphones can also bring more attacks on the phones, the common issues include insecure data storage, broken cryptography. In 2015, the iPhone OS was reported that a severity issue allows the attacker to execute codes in privilege mode or cause DoS attack<sup>2</sup>. Xu et al. [238] proposed a virtualized education platform that provides a private experiment environment. The proposed platform is based on a software-defined network to secure access via OpenVPN. In practice, most of the vulnerabilities are solved by commercial enterprises and open source communities.

### 5.3.4 Virtualized Software Functional Safety

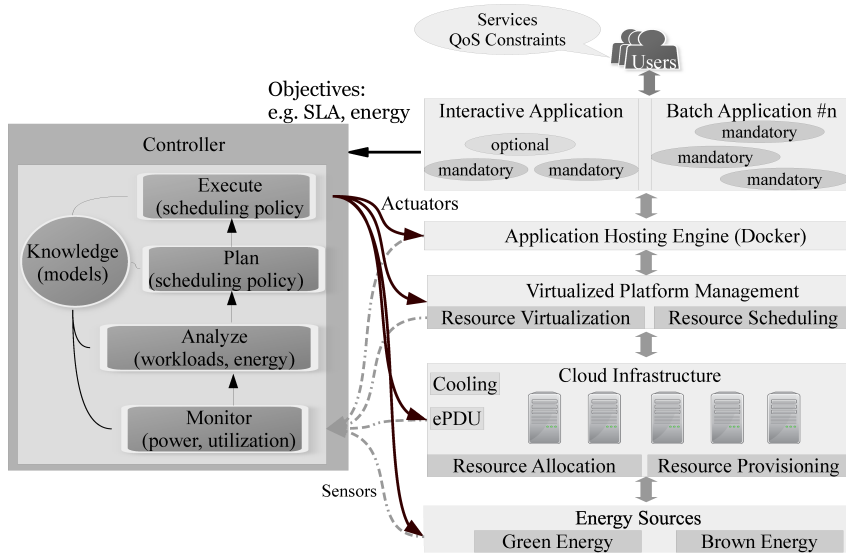
Cloud services allow users to publish and share the image of virtualized instances that implement software functions and contain program codes, such as VM images and container images (e.g. Docker image published in Docker Repository) [240] as shown Figure 10. However, the threat lies in that the shared image can be used to trick the victims by using malicious functions to harvest sensitive data stored in the images (e.g. the default user names and passwords stored in the property files) [241]. Therefore, this kind of attack can both influence integrity and confidentiality. To address this security issue, Wei et al. [242] proposed an image management system to control access to VM images and track the provenance of VM images. For the security in a container image, Fotis et al. [243] introduced a mechanism to protect Docker container images via the enforcement of access policies. Kwon et al. [244] proposed a vulnerability diagnostic system for Docker images by analyzing and detecting abnormal behaviors.

### 5.3.5 Compromised Hypervisor

The compromised hypervisor represents the threat that the attacker aims to control the hypervisor that isolates the cloud users and the virtualized environment [245], such as virtual machines or containers. Such kind of security issues can significantly influence the system security by stealing the visibility permission of users' data and resources and even manipulating the users' data. With the control of the hypervisor, the attacker can be quite powerful by leveraging the capability of VMs and containers.

---

<sup>2</sup><https://www.cvedetails.com/vulnerability-list.php>



**Figure 10.** A prototype system that manages virtual machines and containers in [239].

Therefore, confidentiality, integrity, and availability can all be undermined after gaining partial or full control of the hypervisor.

Lin et al. [246] proposed a VM protection approach for compromised hypervisors based on privilege level execution, which can make effective VM isolation and data-driven VM monitoring to present users' sensitive information in VMs. The advantage of this approach is that it is independent of platforms and can be widely applied to various cloud providers. Li et al. proposed HypSec [247] to retrofit a commodity hypervisor by leveraging microkernel principles to protect the confidentiality and integrity of VMs, which partitions the hypervisor into an untrusted host that is only responsible to perform the functionalities without touching with sensitive data. While the sensitive data can be accessed by the trusted cores. The limitation of this work is that it needs to bring some extra costs. Also based on the partitioning approach, Liu et al. [248] introduced another approach that can separate the fundamental and crucial privilege into the trusted environment to monitor hypervisor. The benefit of this approach is that it does not rely on a higher privilege than the hypervisor. The security in the hypervisor based on the container has also started to attract research attention, as it is a trend to shift the virtualized environment based on VMs into containers. Khalimov et al. [249] have explored to use of the container-based environment as an alternative to the hypervisor-based sandbox for security analysis.

In conclusion, cloud security related to IoMT has attracted the attention of researchers from wide perspectives. To give a clear view, a summary of the Cloud security issues, compromised features, mitigation, and corresponding solutions is given in Table 5. We note that the security approaches for hardware, cloud storage, and virtualized platform have been standardized across the cloud layer comprised of well-known security techniques including resource replication, masked authenticated messaging, admission control, and transmission protections that are applied for common scenarios. Apart from this point, we also find that there exists a set of security mechanisms for new threats that are unique to cloud security, such as malicious VM images and cloud-side encryption for authorization, authentication, and confidentiality methods, which indicates future research directions. There are also emerging problems that current solutions are not working well, such as identifying and dealing with malicious container images for IoMT services in a cloud-native environment.

**Table 5.** Cloud Security Taxonomy of State-of-the-art

	Security Issues	Compromised features	Mitigation	Representative Solutions
Hardware Security	Natural disasters	Availability	Disaster recovery solutions	[208], [207]
	Hardware functional safety	Availability	Resource replications, erasure coding	[211]
	Infrastructure data leakage	Confidentiality	Transmission protection, access control	[212], [213]
	Inadequate infrastructure design	Availability	Auto-scaling, workloads prediction	[215], [216]
Cloud Storage Security	Data loss and leakage	Integrity	Local and remote scanning	[217]
	Data manipulation and integrity	Integrity	Blockchain, masked authenticated messaging	[218–221]
	Malware	Confidentiality	Anomaly detection	[227–229]
	Data monitoring and inference	Privacy	Inference-ware mechanism	[217, 230–232]
Virtualized Platform Security	Data migration	Integrity	Transmission protocol	[233], [234]
	Data separation	Integrity	Task offloading, federated learning	[236], [237]
	Operating system security	Confidentiality	Vulnerabilities packing	[238]
	Virtualized software functional safety	Privacy	VM image provenance tracking	[242–244]
	Compromised hypervisor	Availability	Privilege management	[246–249]

## 6 Challenges and Research Directions

Although the existing work has investigated the diverse perspective of security issues in IoMT applications, supported network and cloud infrastructure, some research gaps and challenges are only partially addressed. Some challenges are summarized as below:

- **Identification of Malicious Container Images.** Cloud-native has been regarded as the new generation of cloud computing and has shifted the monolithic applications into light-weight and self-contained microservice-based applications. The applications including IoMT services can be deployed on VM or container images, which may be attacked by malicious users. However, limited research has been conducted for the security issues in container-based environment, and the identification of the malicious container images is still a challenge for the cloud-based scenario that supports IoMT services.
- **Regulations and Licensing.** When integrating IoMT devices into different medical facilities, adhering to compliance regulations, and securing licensing approvals are mandatory. The majority of the devices aimed at collecting, transmitting, or analyzing information are subjects for compliance regulations and licensing approvals. While manufacturing these devices itself is a time-consuming process, that is not the only challenge IoMT service providers face in healthcare. Regulatory compliance is a considerable hurdle that must be successfully addressed. Ignoring this challenge can lead to an increase in overall risks and legal costs in the future.
- **Tradeoff between Interoperability and Data Security.** A crucial challenge is the lack of systems that help collate and make use of the massive amounts of data collected from medical devices. The different departments in healthcare often run in silos and may not communicate with each other efficiently. In order to garner critical insights from the data that is generated, it is necessary to have systems in place that interact with each other. When integrating IoMT systems, it can lead to extensive medical interoperability amongst crucial devices in the systems. However, data related to patient health and information present inpatient databases like credit card details, addresses, and email IDs are in high demand amongst hackers. IoMT devices are mainly designed with a utility perspective in mind and often make use of legacy software that does not have in-built data security features. Consequently, if the data interoperability is extended, the vulnerabilities exist in devices and different departments in healthcare.
- **Long-term and System-wide Comprehensive Security.** From the perspective of system, integrated security involves multi-elements, multi-agents, multi-levels and multi-links, with significant complexity (including high dimensionality, multi-scale, nonlinear, openness, integrity, interaction, coupling, interactivity and dynamics). The integrated security has become one of the key research direc-

tions and tasks in the field of safety science, which should be one of the major challenges of safety science in the 21st century. In order to cope with the security challenges caused by integrated security problems, security researchers need to update their research concepts, develop research ideas, focus on strengthening the scientific research on complex security, and carry out long-term and system-wide comprehensive security research on complex giant systems (including human beings and human activities) as a whole.

We also discuss a set of research opportunities and future directions:

- **Firmware Upgrades.** IoMT devices must be regularly monitored and patched with critical firmware upgrades, which will optimize the performance of firmware or device drivers, potentially improving the performance of processors or other device hardware. These updates also fix existing glitches, bugs, or new security vulnerabilities.
- **Security-by-design Device.** The security-by-design approach provides application protection through sophisticated data, function and control flow transformations, anti-debug, whitebox cryptography, and active integrity verification. Integrating this security technology with an enterprise security information and event management solution provides an advance warning of threat actor activity before the device or software is affected. Real-time health checks of device software, correlation and forensic analysis of all security data and event feeds help to prevent attacks and automate incident response playbooks.
- **Segmenting Security.** The vast majority of device-to-device communications are superfluous. Security through segmentation represents a best practice. By creating separation between patient data and the rest of the IT network, cyber security experts can better understand network traffic and can improve anomaly detection. As a result, better insights into unusual traffic patterns or movements can then be offered that may indicate the presence of an intruder or a cyber infection.
- **Blockchain-based Techniques.** The current security assurance approaches to prevent data manipulation of cloud services and cloud storage (e.g. the medical data) are mainly based on traditional encryption algorithms. The promotion of blockchain technology has provided an option for traceable and tamper-resistant data, which can prevent the illegal modification of sensitive data. More efforts can be conducted based on blockchain to secure the data in the IoMT scenarios.
- **Microservice-based Applications.** A significant amount of efforts has been devoted to the security of traditional applications, however, more and more applications have been shifted from monolithic applications into microservice based applications. The security issues in the virtualized environment of microservice platform have not been comprehensively investigated, such as container image security and data isolation between containers. More attentions should be paid to this area.
- **Data Management with Federated Learning.** The data management between the users' local device and remote cloud servers is a challenge, as how to partition the data to ensure the user privacy and data processing efficiency is not easy. Federated learning has been regarded as a promising paradigm that keeps the sensitive data locally and outsources the insensitive data to the cloud, e.g. the personal data of patients can be processed by local devices and general information can be trained by the AI models in the cloud. The distributed data can coordinate together to fulfill requirements of medical-oriented tasks.
- **Research Direction of Integrated Security.** Aiming at the integration security problem, it is necessary to carry out some frontier specific research, such as: (1) integration security methodology; (2) The interrelation, function, response and feedback mechanism of various risk factors in integrated security; (3) Integrated security collaborative governance; (4) Prediction, response and response of local and overall security changes of the system; (5) Prevention and resolution of systemic security risks; (6) System security risks emerge.

## 7 Conclusion

IoMT is playing an undeniably useful role in precision health, by improving timeliness and quality of care while reducing patient care complexities and costs, especially in helping manage the pandemic crisis. As data security and prediction accuracy have been the main concerns in this area, the related

security issues need to be taken seriously, making it vitally important to develop and implement successful security strategies in IoMT systems. In this paper, a comprehensive review of papers discussing IoMT systems and the corresponding security and privacy problems has been presented. An overview of IoMT systems from the aspect of hierarchical system architecture has been portrayed and an assessment of security metrics based on the performance demands of network services was detailed. The state-of-the-art security techniques in this area have been discussed with respect to the potential security risks. The security issues and solutions from the sensing layer, the network layer to the cloud infrastructure layer in IoMT systems have been conducted and analyzed in detail to make them compliant with the system architecture and performance demands of various network services. Particularly, biometrics-based technologies on authentication and key management were highlighted in this paper for their significance and uniqueness reflected in IoMT systems, with the most significant impact, and also the most room for research and further improvement. The challenges and future research directions revealed a great potential on extensive uses by the employment of emerging technologies for security.

### **Conflict of Interest**

The authors declare that they have no conflict of interest.

### **Data Availability**

No data are associated with this article.

### **Authors' Contributions**

Nan Li carried out the layout of the survey and the review of network layer;  
Minxian Xu carried out the review of cloud infrastructure layer, participated in manuscript preparation;  
Qimeng Li carried out the review of sensing layer, participated in manuscript preparation;  
Jikui Liu contributed to the analysis on precision health and biometric feature extraction, participated in manuscript preparation;  
Shudi Bao helped perform the analysis on biometrics-based key management with constructive discussions;  
Ye Li, Jianzhong Li and Hairong Zheng conceived the survey, and participated in its design and coordination and helped to draft the manuscript.  
All authors read and approved the final manuscript.

### **Acknowledgements**

We thank Yuanyuan Liu and the anonymous reviewers for their helpful comments.

### **Funding**

This work was supported in part by the National Natural Science Foundation of China under Grants 62072451, 62102409 and 62073310; and in part by the Shenzhen Science and Technology Program under Grant RCBS20210609104609044.

### **References**

- [1] *The precision medicine initiative* (2016), <https://obamawhitehouse.archives.gov/precision-medicine>
- [2] S.S. Gambhir, T.J. Ge, O. Vermesh, R. Spitler, *Toward achieving precision health*, *Science translational medicine*, **10**(430), pp.eaao3612 (2018)

- [3] J.R. Vermeesch, T. Voet, K. Devriendt, *Prenatal and pre-implantation genetic diagnosis*, Nature Reviews Genetics, **17**(10), pp.643–656 (2016)
- [4] R.K. Pathinarupothi, P. Durga, E.S. Rangan, *IoT-based smart edge for global health: Remote monitoring with severity detection and alerts transmission*, IEEE Internet of Things Journal, **6**(2), pp.2449–2462 (2019)
- [5] U. Satija, B. Ramkumar, M.S. Manikandan, *Real-time signal quality-aware ECG telemetry system for IoT-based health care monitoring*, IEEE Internet of Things Journal, **4**(5), pp.815–823 (2017)
- [6] Z. Yang, Q. Zhou, L. Lei, K. Zheng, W. Xiang, *An IoT-cloud based wearable ECG monitoring system for smart healthcare*, Journal of Medical Systems, **40**(286) (2016)
- [7] L. Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M.L. Stefanizzi, L. Tarricone, *An IoT-aware architecture for smart healthcare systems*, IEEE Internet of Things Journal, **2**(6), pp.515–526 (2015)
- [8] P. Castillejo, J.F. Martinez, J. Rodriguez-Molina, A. Cuerva, *Integration of wearable devices in a wireless sensor network for an E-health application*, IEEE Wireless Communications, **20**(4), pp.38–49 (2013)
- [9] Y.A. Qadri, A. Nauman, Y.B. Zikria, A.V. Vasilakos, S.W. Kim, *The future of healthcare Internet of Things: A survey of emerging technologies*, IEEE Communications Surveys & Tutorials, **22**(2), pp.1121–1167 (2020)
- [10] M. Masud, G.S. Gaba, S. Alqahtani, G. Muhammad, B.B. Gupta, P. Kumar, A. Ghoneim, *A lightweight and robust secure key establishment protocol for Internet of Medical Things in covid-19 patients care*, IEEE Internet of Things Journal, **8**(21), pp.15694–15703 (2021)
- [11] H. Lin, S. Garg, J. Hu, X. Wang, J. Piran, M.S. Hossain, *Privacy-enhanced data fusion for covid-19 applications in intelligent Internet of Medical Things*, IEEE Internet of Things Journal, **8**(21), pp.15683–15693 (2021)
- [12] T. Yang, M. Gentile, C.F. Shen, C.M. Cheng, *Combining point-of-care diagnostics and Internet of Medical Things (IoMT) to combat the covid-19 pandemic*, Diagnostics, **10**(4), pp.224–226 (2020)
- [13] J. Liu, F. Miao, L. Yin, Z. Pang, Y. Li, *A noncontact ballistocardiography-based iomt system for cardiopulmonary health monitoring of discharged covid-19 patients*, IEEE Internet of Things Journal, **8**(21), pp.15807–15817 (2021)
- [14] F. Firouzi, A.M. Rahmani, K. Mankodiya, M. Badaroglu, G.V. Merrett, P. Wong, B. Farahani, *Internet-of-Things and big data for smarter healthcare: From device to architecture applications and analytics*, Future Generation Computer Systems, **78**(2), pp.583–586 (2018)
- [15] J. Joyia, R.M. Liaqat, A. Farooq, S. Rehman, *Internet of medical things (IoMT): Applications benefits and future challenges in healthcare domain*, Journal of Communications, **12**(4), pp.240–247 (2017)
- [16] A.J. Jara, M.A. Zamora-Izquierdo, A.F. Skarmeta, *Interconnection framework for mHealth and remote monitoring based on the Internet of Things*, IEEE Journal on Selected Areas in Communications, **31**(9), pp.47–65 (2013)
- [17] P. Verma, S.K. Sood, *Fog assisted-IoT enabled patient health monitoring in smart homes*, IEEE Internet of Things Journal, **5**(3), pp.1789–1796 (2018)
- [18] A. Redondi, M. Chirico, L. Borsani, M. Cesana, M. Tagliasacchi, *An integrated system based on wireless sensor networks for patient monitoring localization and tracking*, Ad Hoc Networks, **11**(1), pp.39–53 (2013)

- [19] Y. Fan, Y. Yin, L. Xu, Y. Zeng, F. Wu, *IoT-based smart rehabilitation system*, IEEE Transactions on Industrial Informatics, **10**(2), pp.1568–1577 (2014)
- [20] C. Occhiuzzi, C. Vallese, S. Amendola, S. Manzari, G. Marrocco, *NIGHT-care: A passive RFID system for remote monitoring and control of overnight living environment*, Procedia Computer Science, **32**, pp.190–197 (2014)
- [21] L. Liu, E. Stroulia, I. Nikolaidis, A. Miguel-Cruz, A.R. Rincon, *Smart homes and home health monitoring technologies for older adults: A systematic review*, International Journal of Medical Informatics, **91**, pp.44–59 (2016)
- [22] C.F. Pasluosta, H. Gassner, J. Winkler, J. Klucken, B.M. Eskofier, *An emerging era in the management of Parkinson’s disease: Wearable technologies and the Internet of Things*, IEEE Journal of Biomedical and Health Informatics, **19**(6), pp.1873–1881 (2015)
- [23] G. Yang, L. Xie, M. Mäntysalo, X. Zhou, Z. Pang, L. Xu, S. Kao-Walter, Q. Chen, L. Zheng, *A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box*, IEEE Transactions on Industrial Informatics, **10**(4), pp.2180–2191 (2014)
- [24] Cynerio, *Health it security* (2022), <https://healthitsecurity.com/news/53-of-connected-medical-devices-contain-critical-vulnerabilities>
- [25] D. He, R. Ye, S. Chan, M. Guizani, Y. Xu, *Privacy in the Internet of Things for smart healthcare*, IEEE Communications Magazine, **56**(4), pp.38–44 (2018)
- [26] M. Masud, G.S. Gaba, K. Choudhary, M.S. Hossain, M.F. Alhamid, G. Muhammad, *Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare*, IEEE Internet of Things Journal, **9**(4), pp.2649–2656 (2022)
- [27] M. Kumar, S. Chand, *A secure and efficient cloud-centric Internet-of-medical-things-enabled smart healthcare system with public verifiability*, IEEE Internet of Things Journal, **17**(10), pp.10650–10659 (2020)
- [28] C.L. Stergiou, K.E.P.B.B. Gupta, *IoT-based big data secure management in the fog over a 6G wireless network*, IEEE Internet of Things Journal, **8**(7), pp.5164–5171 (2021)
- [29] A.P.G. Lopes, P.R.L. Gondim, *Mutual authentication protocol for D2D communications in a cloud-based E-health system*, Sensors, **20**(7), pp.2072–2095 (2020)
- [30] B.D. Deebak, F. Al-Turjman, *Smart mutual authentication protocol for cloud based medical healthcare systems using Internet of medical things*, IEEE Journal on Selected Areas in Communications, **39**(2), pp.346–360 (2021)
- [31] R. Cao, Z. Tang, C. Liu, B. Veeravalli, *A scalable multicloud storage architecture for cloud-supported medical Internet of Things*, IEEE Internet of Things Journal, **7**(3), pp.1641–1654 (2020)
- [32] Z. Ning, P. Dong, X. Wang, X. Hu, L. Guo, B. Hu, Y. Guo, T.Q.R.Y.K. Kwok, *Mobile edge computing enabled 5G health monitoring for Internet of medical things: A decentralized game theoretic approach*, IEEE Journal on Selected Areas in Communications, **39**(2), pp.463–478 (2021)
- [33] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, R. Jain, *Recent advances in the internet-of-medical-things (IoMT) systems security*, IEEE Internet of Things Journal, **8**(11), pp.8707–8718 (2020)
- [34] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, C. Douligeris, *Security in IoMT communications: A survey*, Sensors, **20**(17), pp.4828 (2020)
- [35] G. Hatzivasilis, O. Sountatos, S. Ioannidis, C. Verikoukis, G. Demetriou, C. Tsatsoulis, *Review of security and privacy for the Internet of Medical Things (IoMT)*, in 2019



- 15th international conference on distributed computing in sensor systems (DCOSS)*, pp. 457–464 (IEEE, 2019)
- [36] J.J. Hathaliya, S. Tanwar, *An exhaustive survey on security and privacy issues in healthcare 4.0*, *Computer Communications*, **153**, pp.311–335 (2020)
- [37] A.I. Newaz, A.K. Sikder, M.A. Rahman, A.S. Uluagac, *A survey on security and privacy issues in modern healthcare systems: Attacks and defenses*, *ACM Transactions on Computing for Healthcare*, **2**(3), pp.1–44 (2021)
- [38] T. Yaqoob, H. Abbas, M. Atiquzzaman, *Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices - A review*, *IEEE Communications Surveys & Tutorials*, **21**(4), pp.3723–3768 (2019)
- [39] D. Smith, K. Simpson, *Functional safety* (Routledge, 2004)
- [40] J. Wu, *Development paradigms of cyberspace endogenous safety and security*, *Science China Information Sciences*, **65**(5), pp.1–3 (2022)
- [41] J. Wu, *Cyberspace endogenous safety and security*, *Engineering*, (2021)
- [42] N. Fatema, R. Brad, *Security requirements, counterattacks and projects in healthcare applications using WSNs - a review*, *International Journal Computer Networking and Communication*, **2**(2), pp.1–9 (2014)
- [43] E. Clausing, M. Schiefer, U. Lösche, *Tech. rep.*, Independent IT-Security Institute (2015)
- [44] X. Cao, D.M. Shila, Y. Cheng, Z. Yang, Y. Zhou, J. Chen, *Ghost-in-ZigBee: Energy depletion attack on zigbee-based wireless networks*, *IEEE Internet of Things Journal*, **3**(5), pp.816–829 (2016)
- [45] S.S. Gill, M. Xu, C. Ottaviani, P. Patros, R. Bahsoon, A. Shaghghi, M. Golec, V. Stankovski, H. Wu, A. Abraham et al., *AI for next generation computing: Emerging trends and future directions*, *Internet of Things*, **19**, pp.100514 (2022)
- [46] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, G. Wang, *Security and privacy in the medical Internet of Things: A review*, *Security and Communication Networks*, **2018**, pp.1–9 (2018)
- [47] P. Kasyoka, M. Kimwele, S.M. Angolo, *Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system*, *Journal of Medical Engineering & Technology*, **44**(1), pp.12–19 (2020)
- [48] M. Bromwich, R. Bromwich, *Privacy risks when using mobile devices in health care*, *Canadian Medical Association Journal*, **188**(12), pp.855–856 (2016)
- [49] V.L. Raposo, *Electronic health records: Is it a risk worth taking in healthcare delivery?*, *GMS Health Technology Assessment*, **11**(2), pp.1–9 (2015)
- [50] G. Mooney, *Is HIPAA compliant with the GDPR?* (2018), <https://blog.ipswitch.com/is-hipaa-compliant-with-the-gdpr>
- [51] S. Pearlman, *What is data integrity and why is it important?* (2019), <https://www.talend.com/resources/what-is-data-integrity/>
- [52] T. Bienkowski, *GDPR is explicit about protecting availability* (2018), <https://www.netscout.com/blog/gdpr-availability-protection>
- [53] P. Crilly, V. Muthukumarasamy, *Using smart phones and body sensors to deliver pervasive mobile personal healthcare*, in *Proceedings of the 6th International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pp. 291–296 (2010)
- [54] A. Kogetsu, S. Ogishima, K. Kato, *Authentication of patients and participants in health information exchange and consent for medical research: A key step for privacy protection respect for autonomy and trustworthiness*, *Frontiers in Genetics*, **9**(167)

- (2018)
- [55] G. Kambourakis, *Anonymity and closely related terms in the cyberspace: An analysis by example*, Journal of Information Security and Applications, **19**(1), pp.2–17 (2014)
  - [56] *Medical devices* (2022), [https://www.who.int/health-topics/medical-devices#tab=tab\\_1](https://www.who.int/health-topics/medical-devices#tab=tab_1)
  - [57] V. Ray, *Freud applications of fib: Invasive fib attacks and countermeasures in hardware security devices*, in *East-Coast Focused Ion Beam User Group Meeting* (2009)
  - [58] C. Tarnovsky, *Security failures in secure devices*, Black Hat DC Presentation, **74** (2008)
  - [59] Q. Shi, N. Asadizanjani, D. Forte, M.M. Tehranipoor, *A layout-driven framework to assess vulnerability of ICs to microprobing attacks*, in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 155–160 (IEEE, 2016)
  - [60] S.E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, M. Tehranipoor, *A survey on chip to system reverse engineering*, ACM journal on emerging technologies in computing systems (JETC), **13**(1), pp.1–34 (2016)
  - [61] U.J. Botero, R. Wilson, H. Lu, M.T. Rahman, M.A. Mallaiyan, F. Ganji, N. Asadizanjani, M.M. Tehranipoor, D.L. Woodard, D. Forte, *Hardware trust and assurance through reverse engineering: A survey and outlook from image analysis and machine learning perspectives*, arXiv preprint arXiv:2002.04210, (2020)
  - [62] V. Sidorkin, E. van Veldhoven, E. van der Drift, P. Alkemade, H. Salemink, D. Maas, *Sub-10-nm nanolithography with a scanning helium beam*, Journal of Vacuum Science & Technology B: Microelectronics and Nanometer Structures Processing, Measurement, and Phenomena, **27**(4), pp.L18–L20 (2009)
  - [63] M. Fyrbiak, S. Wallat, P. Swierczynski, M. Hoffmann, S. Hoppach, M. Wilhelm, T. Weidlich, R. Tessier, C. Paar, *HAL—the missing piece of the puzzle for hardware reverse engineering, trojan detection and insertion*, IEEE Transactions on Dependable and Secure Computing, **16**(3), pp.498–510 (2018)
  - [64] A. Costin, J. Zaddach, A. Francillon, D. Balzarotti, *A {Large-Scale} Analysis of the Security of Embedded Firmwares*, in *23rd USENIX Security Symposium (USENIX Security 14)*, pp. 95–110 (2014)
  - [65] R. Ben Yehuda, N.J. Zaidenberg, *Protection against reverse engineering in ARM*, International Journal of Information Security, **19**(1), pp.39–51 (2020)
  - [66] A. Vosoughi, S. Köse, *Leveraging On-Chip Voltage Regulators Against Fault Injection Attacks*, in *Proceedings of the 2019 on Great Lakes Symposium on VLSI, GLSVLSI '19*, pp. 15–20 (Association for Computing Machinery, New York, NY, USA, 2019), <https://doi.org/10.1145/3299874.3317978>
  - [67] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Fotti, E. Roback, *Report on the development of the advanced encryption standard (AES)*, Journal of Research of the National Institute of Standards and Technology, **106**(3), pp.511–577 (2001)
  - [68] M. Tehranipoor, F. Koushanfar, *A survey of hardware trojan taxonomy and detection*, IEEE Design Test of Computers, **27**(1), pp.10–25 (2010)
  - [69] T. Wehbe, V.J. Mooney, A.Q. Javaid, O.T. Inan, *A novel physiological features-assisted architecture for rapidly distinguishing health problems from hardware Trojan attacks and errors in medical devices*, in *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 106–109 (IEEE, 2017)
  - [70] R. Jordaney, K. Sharad, S.K. Dash, Z. Wang, D. Papini, I. Nouretdinov, L. Cavallaro, *Transcend: Detecting concept drift in malware classification models*, in *26th USENIX Security Symposium (USENIX Security 17)*, pp. 625–642 (2017)

- [71] H. Cai, N. Meng, B. Ryder, D. Yao, *Droidcat: Effective android malware detection and categorization via app-level profiling*, IEEE Transactions on Information Forensics and Security, **14**(6), pp.1455–1470 (2019)
- [72] T. Lei, Z. Qin, Z. Wang, Q. Li, D. Ye, *Evedroid: Event-aware android malware detection against model degrading for IoT devices*, IEEE Internet of Things Journal, **6**(4), pp.6668–6680 (2019)
- [73] M.N. Aman, K.C. Chua, B. Sikdar, in *Cryptographic Security Solutions for the Internet of Things* (IGI Global, 2019), pp. 117–141
- [74] M.A. Qureshi, A. Munir, *PUF-RAKE: A PUF-based robust and lightweight authentication and key establishment protocol*, IEEE Transactions on Dependable and Secure Computing, (2021)
- [75] Z. Wang, X. Ding, C. Pang, J. Guo, J. Zhu, B. Mao, *To detect stack buffer overflow with polymorphic canaries*, in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 243–254 (IEEE, 2018)
- [76] B. Xu, W. Wang, Q. Hao, Z. Zhang, P. Du, T. Xia, H. Li, X. Wang, *A security design for the detecting of buffer overflow attacks in IoT device*, IEEE Access, **6**, pp.72862–72869 (2018)
- [77] D.M. Shila, P. Geng, T. Lovett, *I can detect you: Using intrusion checkers to resist malicious firmware attacks*, in *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, pp. 1–6 (2016)
- [78] S. Hanna, R. Rolles, A. Molina-Markham, P. Poosankam, J. Blocki, K. Fu, D. Song, *Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices.*, in *HealthSec* (Citeseer, 2011)
- [79] A. Aviv, P. Černý, S. Clark, E. Cronin, G. Shah, M. Sherr, M. Blaze, *Security evaluation of ES&S voting machines and election management system*, in *Proceedings of the conference on Electronic voting technology*, pp. 1–13 (2008)
- [80] A. Cui, S.J. Stolfo, *A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan*, in *Proceedings of the 26th Annual Computer Security Applications Conference*, pp. 97–106 (2010)
- [81] M. Sutton, *Corporate espionage for dummies: The hidden threat of embedded web servers*, Black Hat USA, (2011)
- [82] M. Bettayeb, Q. Nasir, M.A. Talib, *Firmware update attacks and security for iot devices: Survey*, in *Proceedings of the ArabWIC 6th Annual International Conference Research Track*, pp. 1–6 (2019)
- [83] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, X. Fu, *Security vulnerabilities of internet of things: A case study of the smart plug system*, IEEE Internet of Things Journal, **4**(6), pp.1899–1909 (2017)
- [84] A. One, *Smashing the stack for fun and profit*, Phrack magazine, **7**(49), pp.14–16 (1996)
- [85] H. Shacham, *The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86)*, in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 552–561 (2007)
- [86] A. Mohanty, I. Obaidat, F. Yilmaz, M. Sridhar, *Control-hijacking vulnerabilities in IoT firmware: A brief survey*, in *The 1st International Workshop on Security and Privacy for the Internet-of-Things (IoTSec)* (2018)
- [87] N. Burow, S.A. Carr, J. Nash, P. Larsen, M. Franz, S. Brunthaler, M. Payer, *Control-flow integrity: Precision, security, and performance*, ACM Computing Surveys, **50**(1), pp.1–33 (2017)

- [88] Z. Jin, Y. Chen, T. Liu, K. Li, Z. Wang, J. Zheng, *A Novel and Fine-Grained Heap Randomization Allocation Strategy for Effectively Alleviating Heap Buffer Overflow Vulnerabilities*, in *Proceedings of the 2019 4th International Conference on Mathematics and Artificial Intelligence, ICMAI 2019*, pp. 115–122 (Association for Computing Machinery, New York, NY, USA, 2019)
- [89] H. Xia, J. Woodruff, S. Ainsworth, N.W. Filardo, M. Roe, A. Richardson, P. Rugg, P.G. Neumann, S.W. Moore, R.N.M. Watson et al., *CHERlvoke: Characterising Pointer Revocation Using CHERI Capabilities for Temporal Memory Safety*, in *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture, MICRO '52*, pp. 545–557 (Association for Computing Machinery, New York, NY, USA, 2019)
- [90] E. Karimi, Y. Fei, D. Kaeli, *Hardware/software obfuscation against timing side-channel attack on a GPU*, in *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 122–131 (IEEE, 2020)
- [91] W. Song, B. Li, Z. Xue, Z. Li, W. Wang, P. Liu, *Randomized Last-Level Caches Are Still Vulnerable to Cache Side-Channel Attacks! But We Can Fix It*, in *2021 IEEE Symposium on Security and Privacy (SP)*, pp. 955–969 (2021)
- [92] M.K. Qureshi, *New attacks and defense for encrypted-address cache*, in *2019 ACM/IEEE 46th Annual International Symposium on Computer Architecture (ISCA)*, pp. 360–371 (IEEE, 2019)
- [93] M. Werner, T. Unterluggauer, L. Giner, M. Schwarz, D. Gruss, S. Mangard, *{ScatterCache}: Thwarting Cache Attacks via Cache Set Randomization*, in *28th USENIX Security Symposium (USENIX Security 19)*, pp. 675–692 (2019)
- [94] D. Das, S. Maity, S.B. Nasir, S. Ghosh, A. Raychowdhury, S. Sen, *High efficiency power side-channel attack immunity using noise injection in attenuated signature domain*, in *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 62–67 (2017)
- [95] L. Wei, B. Luo, Y. Li, Y. Liu, Q. Xu, *I know what you see: Power side-channel attack on convolutional neural network accelerators*, in *Proceedings of the 34th Annual Computer Security Applications Conference*, pp. 393–406 (2018)
- [96] I.M. Delgado-Lozano, E. Tena-Sánchez, J. NÚÑez, A.J. Acosta, *Design and analysis of secure emerging crypto-hardware using hyperfet devices*, *IEEE Transactions on Emerging Topics in Computing*, **9**(2), pp.787–796 (2021)
- [97] W.H. Yang, L.C. Chu, S.H. Yang, Y.J. Lai, S.Q. Chen, K.H. Chen, Y.H. Lin, S.R. Lin, T.Y. Tsai, *An enhanced-security buck DC-DC converter with true-random-number-based pseudo hysteresis controller for Internet-of-Everything (IoE) devices*, in *2018 IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 126–128 (IEEE, 2018)
- [98] D. Das, M. Nath, S. Ghosh, S. Sen, *Killing EM Side-Channel Leakage at its Source*, in *2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWS-CAS)*, pp. 1108–1111 (2020)
- [99] P. Cheng, I.E. Bagci, U. Roedig, J. Yan, *Sonarsnoop: Active acoustic side-channel attacks*, *International Journal of Information Security*, **19**(2), pp.213–228 (2020)
- [100] G. de Souza Faria, H.Y. Kim, *Differential audio analysis: a new side-channel attack on PIN pads*, *International Journal of Information Security*, **18**(1), pp.73–84 (2019)
- [101] E. Carmon, J.P. Seifert, A. Wool, *Photonic side channel attacks against RSA*, in *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 74–78 (2017)

- [102] R.L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, **27**(2), pp.120–126 (1978)
- [103] K. Aravindhnan, R. Karthiga, *One-time password: a survey*, International Journal of Emerging Trends in Engineering and Development, **1**(3), pp.613–623 (2013)
- [104] M. Zhang, Q. Yin, *Research progress of static password authentication technology*, Journal of Cyberspace security, **9**(7), pp.11–14 (2018)
- [105] H.Y. Chien, J. Ke-Jan, Y.M. Tseng, *An efficient and practical solution to remote authentication: smart card*, Computers & Security, **21**(4), pp.372–375 (2002)
- [106] A. Shimizu, *A dynamic password authentication method using a one-way function*, Systems and computers in Japan, **22**(7), pp.32–40 (1991)
- [107] A. KumarDas, P. Sharma, S. Chatterjee, J. KantaSing, *A dynamic password-based user authentication scheme for hierarchical wireless sensor networks*, Journal of Network and Computer Applications, **35**(5), pp.1646–1656 (2012)
- [108] L. Harn, J. Ren, *Generalized digital certificate for user authentication and key establishment for secure communications*, IEEE Transactions on Wireless Communications, **10**(7), pp.2372–2379 (2011)
- [109] A. Kumari, S. Jangirala, M.Y. Abbasi, V. Kumar, M. Alam, *ESEAP: ECC-based secure and efficient mutual authentication protocol using smart card*, Journal of Information Security and Applications, **51**, pp.1–12 (2020)
- [110] C. Easttom, N. Mei, *Mitigating implanted medical device cybersecurity risks*, in *Proceeding of IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 145–148 (2019)
- [111] N. Ibtihel, S.M. Hadj, *Smart ECG monitoring through IoT* (C. ChinMay Ed., 2020)
- [112] W. Youssef, A.O. Zaid, M.S. Mourali, M.H. Kammoun, *RFID-based system for secure logistic management of implantable medical devices in Tunisian health centres*, in *Proceeding of IEEE International Smart Cities Conference (ISC2)*, pp. 83–86 (2019)
- [113] A. Jain, L. Hong, R. Bolle, *Online fingerprint verification*, IEEE Transactions on Pattern Analysis and Machine Intelligence, **19**(4), pp.302–314 (1997)
- [114] A.K. Datta, *Advances in fingerprint technology*, CRC Press, (2001)
- [115] V. Bruce, A. Young, *Understanding face recognition*, British Journal of Psychology, **77**(3), pp.305–327 (1986)
- [116] X. He, S. Yan, Y. Hu, N. P, H.J. Zhang, *Face recognition using laplacianfaces*, IEEE Transactions on Pattern Analysis and Machine Intelligence, **27**(3), pp.328–340 (2005)
- [117] M. Frank, R. Biedert, E. Ma, I. Martinovic, D. Song, *Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication*, IEEE Transactions on Information Forensics and Security, **8**(1), pp.136–148 (2013)
- [118] N. Zheng, K. Bai, H. Huang, H. Wang, *You Are How You Touch: User Verification on Smartphones via Tapping Behaviors*, in *Proceeding of the 22nd IEEE International Conference on Network Protocols*, pp. 221–232 (2014)
- [119] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, K.S. Balagani, *Hmog: New behavioral biometric features for continuous authentication of smartphone users*, IEEE Transactions on Information Forensics and Security, **11**(5), pp.877–892 (2016)
- [120] G. Zheng, W. Yang, M. Johnstone, R. Shankaran, C. Valli, *Securing the elderly in cyberspace with fingerprints* (Academic, 2020)
- [121] G. Zheng, W. Yang, C. Valli, L. Qiao, R. Shankaran, M.A. Orgun, S.C. Mukhopa, *Finger-to-heart (F2H): Authentication for wireless implantable medical devices*, IEEE Journal of Biomedical and Health Informatics, **23**(4), pp.1546–1557 (2019)

- [122] A. Fratini, M. Sansone, P. Bifulco, M. Cesarelli, *Individual identification via electrocardiogram analysis*, Biomedical Engineering Online, **14**(78) (2015)
- [123] M. Yang, B. Liu, M. Zhao, F. Li, G. Wang, F. Zhou, *Normalizing electrocardiograms of both healthy persons and cardiovascular disease patients for biometric authentication*, PLoS ONE, **8**(8) (2013)
- [124] J.M. Irvine, S.A. Israel, *A sequential procedure for individual identity verification using ECG*, EURASIP Journal on Advances in Signal Processing, **5**, pp.42–57 (2009)
- [125] S. Pathoumvanh, S. Airphaiboon, K. Hamamoto, *Robustness study of ECG biometric identification in heart rate variability conditions*, IEEJ Transactions on Electrical and Electronic Engineering, **9**(3), pp.42–57 (2014)
- [126] J. Liu, L. Yin, C. He, B. Wen, X. Hong, Y. Li, *A multiscale autoregressive model-based electrocardiogram identification method*, IEEE Access, **6**, pp.18251–18263 (2018)
- [127] F. Sun, C. Mao, X. Fan, Y. Li, *Accelerometer-based speed-adaptive gait authentication method for wearable IoT devices*, IEEE Internet of Things Journal, **6**(1), pp.820–830 (2018)
- [128] F. Sun, W. Zang, R. Gravina, G. Fortino, Y. Li, *Gait-based identification for elderly users in wearable healthcare systems*, Information fusion, **53**, pp.134–144 (2020)
- [129] R. Amin, N. Kumar, G.P. Biswas, R. Iqbal, V. Chang, *A light weight authentication protocol for iot-enabled devices in distributed cloud computing environment*, Future Generation Computer Systems, **78**(3), pp.1005–1019 (2018)
- [130] M. Wazid, A.K. Das, N. Kumar, A.V. Vasilakos, *Design of secure key management and user authentication scheme for fog computing services*, Future Generation Computer Systems, **91**, pp.475–492 (2019)
- [131] V.H. Tutari, B. Das, D.R. Chowdhury, *A continuous role-based authentication scheme and data transmission protocol for implantable medical devices*, in *2019 2nd International Conference on Advanced Computational and Communication Paradigms*, pp. 1–6 (2019)
- [132] T.F. Yen, Y. Xie, F. Yu, R.P. Yu, M. Abadi, *Host Fingerprinting and Tracking on the Web: Privacy and Security Implications*, in *Proceedings of the 19th Annual Network and Distributed System Security Symposium* (2012)
- [133] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. van Randwyk, *Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting*, in *Proceedings of the 15th USENIX Conference on Security Symposium*, pp. 16–89 (2006)
- [134] L.C.C. Desmond, C.C. Yuan, T.C. Pheng, R.S. Lee, *Identifying Unique Devices through Wireless Fingerprinting*, in *Proceedings of the 1st ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 46–55 (2008)
- [135] S.V. Radhakrishnan, A.S. Uluagac, R. Beyah, *GTID: A technique for physical device and device type fingerprinting*, IEEE Transactions on Dependable and Secure Computing, **12**(5), pp.519–532 (2015)
- [136] J.Hall, M. Barbeau, E. Kranakis, *Radio frequency fingerprinting for intrusion detection in wireless networks*, IEEE Transactions on Dependable and Secure Computing, (2005)
- [137] V. Brik, S. Banerjee, M. Gruteser, S. Oh, *Wireless Device Identification with Radiometric Signatures*, in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, pp. 116–127 (2008)
- [138] T. van Goethem, W. Scheepers, D. Preuveneers, W. Joosen, *Accelerometerbased Device Fingerprinting for Multifactor Mobile Authentication*, in *Proceedings of the 8th International Symposium on Engineering Secure Software and Systems*, pp. 106–121

- (2016)
- [139] G. Baldini, G. Steri, F. Dimc, R. Giuliani, R. Kamnik, *Experimental identification of smartphones using fingerprints of builtin microelectro mechanical systems*, *Sensors*, **6**(16), pp.8–18 (2016)
  - [140] L. Zou, Q. He, J. Wu, *Source cellphone verification from speech recordings using sparse representation*, *Digital Signal Processing*, **62**(62), pp.125–136 (2017)
  - [141] Z. Zhou, W. Diao, X. Liu, K. Zhang, *Acoustic Fingerprinting Revisited: Generate Stable Device ID Stealthily with Inaudible Sound*, in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 429–440 (2014)
  - [142] A.E. Dirik, H.T. Sencar, N. Memon, *Digital single lens reflex camera identification from traces of sensor dust*, *IEEE Transactions on Information Forensics and Security*, **3**(3), pp.539–552 (2008)
  - [143] H. Aksu, A.S. Uluagac, E.S. Bentley, *Identification of wearable devices with bluetooth*, *IEEE Transactions on Sustainable Computing*, **6**(3), pp.221–230 (2021)
  - [144] H. Bojinov, Y. Michalevsky, G. Nakibly, D. Boneh, *Mobile device identification via sensor fingerprinting*, *Cryptography and Security*, (2014)
  - [145] T. Hupperich, H. Hosseini, T. Holz, *Leveraging sensor fingerprinting for mobile device authentication*, *Detection of Intrusions and Malware, and Vulnerability Assessment*, **9721**, pp.377–396 (2016)
  - [146] P. Gope, B. Sikdar, *Lightweight and privacy-preserving two-factor authentication scheme for iot devices*, *IEEE Internet of Things Journal*, **6**(1), pp.580–589 (2019)
  - [147] B. Chatterjee, D. Das, S. Maity, S. Sen, *RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning*, *IEEE Internet of Things Journal*, **6**(1), pp.388–398 (2019)
  - [148] D. Schürmann, S. Sigg, *Secure communication based on ambient audio*, *IEEE Transactions on Mobile Computing*, **12**(2), pp.358–370 (2013)
  - [149] Q. Quach, N. Nguyen, T. Dinh, *Secure authentication for mobile devices based on acoustic background fingerprint*, *Knowledge and Systems Engineering*, pp. 375–387 (2014)
  - [150] N. Karapanos, C. Marforio, C. Soriente, S. Capkun, *Sound-proof: Usable Twofactor Authentication Based on Ambient Sound*, in *Proceedings of the 24th USENIX Conference on Security Symposium*, pp. 483–498 (2015)
  - [151] R. Mayrhofer, H. Gellersen, *Shake well before use: Intuitive and secure pairing of mobile devices*, *IEEE Transactions on Mobile Computing*, **8**(6), pp.792–806 (2009)
  - [152] J. Han, S. Pan, M.K. Sinha, H.Y. Noh, P. Zhang, P. Tague, *Senstribute: Smart Home Occupant Identification via Fusion across on-object sensing devices*, in *Proceedings of the 4th ACM International Conference on Systems for EnergyEfficient Built Environments*, pp. 1–10 (2018)
  - [153] J. Han, A.J. Chung, M.K. Sinha, M. Harishankar, S. Pan, H.Y. Noh, P. Zhang, P. Tague, *Do You Feel What I Hear? Enabling Autonomous IoT Device Pairing Using Different Sensor Types*, in *Proceedings of the 2018 IEEE Symposium on Security and Privacy*, pp. 836–852 (2018)
  - [154] C. Shi, J. Liu, H. Liu, Y. Chen, *Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-enabled IoT*, in *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 1–10 (2017)
  - [155] H.G. Kayacik, M. Just, L. Baillie, D. Aspinall, N. Micallef, *Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors*, *arXiv preprint*, (2014)

- [156] B. Mahalakshmi, G. Suseendran, in *Data Management, Analytics and Innovation* (Springer, 2019), pp. 467–482
- [157] K. Maitihili, V. Vinothkumar, P. Latha, *Analyzing the security mechanisms to prevent unauthorized access in cloud and network security*, Journal of Computational and Theoretical Nanoscience, **15**(6-7), pp.2059–2063 (2018)
- [158] A. Chhabra, S. Arora, *An elliptic curve cryptography based encryption scheme for securing the cloud against eavesdropping attacks*, in *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*, pp. 243–246 (IEEE, 2017)
- [159] H. Abusaimeh, *Security attacks in cloud computing and corresponding defending mechanisms*, International Journal of Advanced Trends in Computer Science and Engineering, **9**(3) (2020)
- [160] M. Mehrtak et al., *Security challenges and solutions using healthcare cloud computing*, Journal of Medicine and Life, **14**(4), pp.448 (2021)
- [161] E. Abdurachman et al., *Survey on threats and risks in the cloud computing environment*, Procedia Computer Science, **161**, pp.1325–1332 (2019)
- [162] B.A. Alzahrani, A. Irshad, A. Albeshri, K. Alsubhi, *A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks*, Wireless Personal Communications, pp. 47–69 (2021)
- [163] Z. Xu, C. Xu, W. Liang, J. Xu, H. Chen, *A lightweight mutual authentication and key agreement scheme for medical internet of things*, IEEE Access, **7** (2019)
- [164] P. Kasyoka, M. Kimwele, S.M. Angolo, *Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system*, Journal of Medical Engineering & Technology, **44**(1), pp.12–19 (2020)
- [165] T. Bhatia, A. Verma, G. Sharma, *Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing*, Concurrency Computation Practice Experience, **32**(5), pp.1–16 (2019)
- [166] J. Shen, H. Tan, S. Moh, I. Chung, Q. Liu, X. Sun, *Enhanced secure sensor association and key management in wireless body area networks*, Journal of Communications and Networks, **17**(5), pp.453–462 (2015)
- [167] H.Zhao, R.Xu, M. Shu, J. Hu, *Physiological-signal-based key negotiation protocols for body sensor networks: A survey*, in *Proceeding of IEEE 12th Int. Symp. Auton. Decentralized Syst.* (2015)
- [168] D.K. Altop, A. Levi, V. Tuzcu, *Deriving cryptographic keys from physiological signals*, Pervasive Mobile Computing, **39**, pp.65–79 (2016)
- [169] S. Pirbhulal, H. Zhang, W. Wu, S.C. Mukhopadhyay, Y. Zhang, *Heart-beats based biometric random binary sequences generation to secure wireless body sensor networks*, IEEE Transactions on Biomedical Engineering, **65**(12), pp.2751–2759 (2018)
- [170] Y. Sun, B. Lo, *An artificial neural network framework for gaitbased biometrics*, IEEE Journal of Biomedical and Health Informatics, **23**(3), pp.987–998 (2019)
- [171] C. Poon, Y.T. Zhang, S.D. Bao, *A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health*, IEEE Communications Magazine, **44**(4), pp.73–81 (2006)
- [172] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, D. Chen, *OPFKA: Secure and efficient ordered-physiological feature-based key agreement for wireless body area networks*, in *Proceeding of IEEE 12th Int. Symp. Auton. Decentralized Syst.*, pp. 14–19 (2013)
- [173] F. Miao, S. Bao, Y. Li, *Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security*, IET Information Security, **7**(2), pp.87–96 (2013)



- [174] A. Ali, F.A. Khan, *Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art*, Journal of Medical Systems, **39**(10), pp.115 (2015)
- [175] E.K. Zaghouani, A. Jemai, A. Benzina, R. Attia, *ELPA: A new key agreement scheme based on linear prediction of ECG features for WBAN*, in *Proceeding of 23rd European Signal Processing Conference (EUSIPCO)* (2015)
- [176] B. Tams, P. Mihăilescu, A. Munk, *Security considerations in minutiae-based fuzzy vaults*, IEEE Transactions on Information Forensics and Security, **10**(5), pp.985–998 (2015)
- [177] R. Davis, *The data encryption standard in perspective*, IEEE Communications Society Magazine, **16**(6), pp.5–9 (1978)
- [178] J. Lee, S. Yu, M. Kim, Y. Park, A.K. Das, *On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks*, IEEE Access, **8** (2015)
- [179] Y. Kim, W.S. Lee, V. Raghunathan, N.K. Jha, A. Raghunathan, *Vibration-based secure side channel for medical devices*, in *Proceeding of 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (2015)
- [180] J. Kim, B. jin Lee, S.K. Yoo, *Design of real-time encryption module for secure data protection of wearable healthcare devices*, in *Proceeding of 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pp. 2283–2286 (2013)
- [181] A. Mosenia, N.K. Jha, *Opsecure: A secure unidirectional optical channel for implantable medical devices*, IEEE Transactions on Multi-Scale Computing Systems, **4**(3), pp.410–419 (2018)
- [182] F. Sun, W. Zang, H. Huang, I. Farkhatdinov, Y. Li, *Accelerometer-based key generation and distribution method for wearable IoT devices*, IEEE Internet of Things Journal, **8**(3), pp.1636–1650 (2020)
- [183] S. Bao, C. Poon, Y. Zhang, L. Shen, *Using the timing information of heartbeats as an entity identifier to secure body sensor network*, IEEE Transactions on Information Technology in Biomedicine, **12**(6), pp.772–779 (2008)
- [184] P. Gope, *LAAP: Lightweight anonymous authentication protocol for D2D-aided fog computing paradigm*, Computers & Security, **86**, pp.223–237 (2019)
- [185] S. Maji, U. Banerjee, S.H. Fuller, M.R. Abdelhamid, P.M. Nadeau, R.T. Yazicigil, A.P. Chandrakasan, *A low-power dual-factor authentication unit for secure implantable devices*, in *Proceeding of IEEE Custom Integrated Circuits Conference (CICC)* (2020)
- [186] M.N. Tehrani, M. Uysal, H. Yanikomeroglu, *Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions*, IEEE Communications Magazine, **52**(5), pp.86–92 (2014)
- [187] A.D. Wyner, *The wire-tap channel*, Bell System Technical Journal, **54**(8), pp.1355–1387 (1975)
- [188] F. Gabry, N. Li, N. Schrammar, M. Girnyk, L. Rasmussen, M. Skoglund, *On the optimization of the secondary transmitter's strategy in cognitive radio channels with secrecy*, IEEE Journal on Selected Areas in Communications, **32**(3), pp.451–463 (2014)
- [189] S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, *Radio-telepathy: extracting a secret key from an unauthenticated wireless channel*, in *Proceedings of the 14th ACM international conference on mobile computing and networking*, pp. 128–139 (2008)
- [190] R. Ahlswede, I. Csiszar, *Common randomness in information theory and cryptography. part i: secret sharing*, IEEE Transactions on Information Theory, **39**(4), pp.1121–1132 (1993)

- [191] A.M. Sayeed, A. Perrig, *Secure wireless communications: Secret keys through multipath*, in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 3013–3016 (2008)
- [192] T.H. Chou, S.C. Draper, A.M. Sayeed, *Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness*, in *Proceedings of IEEE International Symposium on Information Theory*, pp. 2518–2522 (2010)
- [193] M.F. Awan, K. Kansanen, S.P. Simbor, C. Garcia-Pardo, S. Castello-Palacios, N. Cardona, *RSS-based secret key generation in wireless in-body networks*, in *2019 13th International Symposium on Medical Information and Communication Technology*, pp. 1–6 (2019)
- [194] I. Ray, M. Kumar, L. Yu, *LRBAC: a location-aware role-based access control model*, in *the 2nd international conference on information systems security*, pp. 147–161 (2006)
- [195] Y. Zhang, D. Feng, *A role-based access control model based on space, time and scale*, *Journal of Computer Research and Development*, **7**(47), pp.1252–1260 (2010)
- [196] T. Macaulay, *RIoT Control: Understanding and Managing Risks and the Internet of Things* (Elsevier, 2016)
- [197] G. Sun, Y. Dong, Y. Li, *CP-ABE based data access control for cloud storage*, *Journal on Communications*, **7**(32), pp.146–152 (2011)
- [198] S. Ruj, M. Stojmenovic, A. Nayak, *Decentralized access control with anonymous authentication of data stored in clouds*, *IEEE Transactions on Parallel and Distributed Systems*, **25**(2), pp.384–394 (2014)
- [199] T. Belkhouja, S. Sorour, M.S. Hefeida, *Role-based hierarchical medical data encryption for implantable medical devices*, in *Proceedings of IEEE Global Communications Conference (GLOBECOM)* (2019)
- [200] D. He, N. Kumar, M.K. Khan, L. Wang, J. Shen, *Efficient privacy-aware authentication scheme for mobile cloud computing services*, *IEEE Systems Journal*, **12**(2), pp.1621–1631 (2018)
- [201] V.J. Jariwala, D.C. Jinwala, *Chapter 4 - Adaptable SDA: Secure data aggregation framework in wireless body area networks* (Academic, 2020)
- [202] G. Kalyani, S. Chaudhari, *An efficient approach for enhancing security in internet of things using the optimum authentication key*, *International Journal of Computers and Applications*, **42**(3), pp.306–314 (2019)
- [203] I. Moskowitz, L. Chang, *A decision theoretical based system for information downgrading*, in *Proceedings of the 5th conference on information sciences*, pp. 82–89 (2000)
- [204] R. Cramer, I. Damgård, J.B. Nielsen, *Multiparty computation from threshold homomorphic encryption*, in *International conference on the theory and applications of cryptographic techniques*, pp. 280–300 (Springer, 2001)
- [205] X. Liu, K.K.R. Choo, R.H. Deng, R. Lu, J. Weng, *Efficient and privacy-preserving outsourced calculation of rational numbers*, *IEEE Transactions on Dependable Secure Computing*, **15**(1), pp.27–39 (2016)
- [206] W. Song, B. Wang, Q. Wang, C. Shi, W. Lou, Z. Peng, *Publicly verifiable computation of polynomials over outsourced data with multiple sources*, *IEEE Transactions on Information Forensics Security*, **12**(10), pp.2334–2347 (2017)
- [207] K. Baudry, *Data center site search and selection*, *Data Center Handbook: Plan, Design, Build, and Operations of a Smart Data Center*, pp. 367–380 (2021)

- [208] J. Mendonca, E. Andrade, P.T. Endo, R. Lima, *Disaster recovery solutions for IT systems: A systematic mapping study*, Journal of Systems and Software, **149**, pp.511–530 (2019)
- [209] R. Ko, S.G. Lee, V. Rajan, *Cloud computing vulnerability incidents: A statistical overview* (2013)
- [210] P. Garraghan, R. Yang, Z. Wen, A. Romanovsky, J. Xu, R. Buyya, R. Ranjan, *Emergent failures: Rethinking cloud reliability at scale*, IEEE Cloud Computing, **5**(5), pp.12–21 (2018)
- [211] R. Nachiappan, B. Javadi, R. Calheiros, K. Matawie, *Cloud storage reliability for big data applications: A state of the art survey*, Journal of Network and Computer Applications, **97**, pp.35–47 (2017)
- [212] A. Kirar, A.K. Yadav, S. Maheswari, *An efficient architecture and algorithm to prevent data leakage in Cloud Computing using multi-tier security approach*, in *2016 International Conference System Modeling & Advancement in Research Trends (SMART)*, pp. 271–279 (IEEE, 2016)
- [213] F. Chen, Y. Luo, J. Zhang, J. Zhu, Z. Zhang, C. Zhao, T. Wang, *An infrastructure framework for privacy protection of community medical internet of things*, World Wide Web, **21**(1), pp.33–57 (2018)
- [214] M. Xu, R. Buyya, *Brownout approach for adaptive management of resources and applications in cloud computing systems: A taxonomy and future directions*, ACM Computing Surveys, **52**(1), pp.1–27 (2019)
- [215] Z. Zhong, M. Xu, M.A. Rodriguez, C. Xu, R. Buyya, *Machine learning-based orchestration of containers: A taxonomy and future directions*, ACM Computing Surveys, (2021)
- [216] M. Xu, C. Song, H. Wu, S.S. Gill, K. Ye, C. Xu, *EsDNN: Deep neural network based multivariate workload prediction in cloud computing environments*, ACM Transactions on Internet Technology, (2022), to appear
- [217] K. Kaur, I. Gupta, A.K. Singh et al., *A comparative evaluation of data leakage/loss prevention systems (DLPS)*, in *Proceedings of 4th International Conference on Computer Science & Information Technology (CS & IT-CSCP)*, pp. 87–95 (2017)
- [218] H. Huang, X. Sun, F. Xiao, P. Zhu, W. Wang, *Blockchain-based ehealth system for auditable EHRs manipulation in cloud environments*, Journal of Parallel and Distributed Computing, **148**, pp.46–57 (2021)
- [219] A.K. Pandey, A.I. Khan, Y.B. Abushark, M.M. Alam, A. Agrawal, R. Kumar, R.A. Khan, *Key issues in healthcare data integrity: Analysis and recommendations*, IEEE Access, **8**, pp.40612–40628 (2020)
- [220] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, D. Tzovaras, *On the design of a blockchain-based system to facilitate healthcare data sharing*, 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)*, pp. 1374–1379 (IEEE, 2018)
- [221] G. Manogaran, C. Thota, D. Lopez, R. Sundarasekar, in *Cybersecurity for industry 4.0* (Springer, 2017), pp. 103–126
- [222] Y. Zhang, R.H. Deng, S. Xu, J. Sun, Q. Li, D. Zheng, *Attribute-based encryption for cloud computing access control: A survey*, ACM Computing Surveys, **53**(4), pp.1–41 (2020)
- [223] P. Kumar, P. Alphonse et al., *Attribute based encryption in cloud computing: A survey, gap analysis, and future directions*, Journal of Network and Computer Applications,

108, pp.37–52 (2018)

- [224] Q. Huang, Y. Yang, M. Shen, *Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing*, Future Generation Computer Systems, **72**, pp.239–249 (2017)
- [225] Y. Yang, X. Chen, H. Chen, X. Du, *Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing*, IEEE Access, **6**, pp.18009–18021 (2018)
- [226] J. LI, N. CHEN, Y. ZHANG, *Extended file hierarchy access control scheme with attribute-based encryption in cloud computing*, IEEE Transactions on Emerging Topics in Computing, **9**(2), pp.983–993 (2021)
- [227] A. Marnerides, M. Watson, N. Shirazi, A. Mauthe, D. Hutchison, *Malware analysis in cloud computing: Network and system characteristics*, in *2013 IEEE Globecom workshops*, pp. 482–487 (IEEE, 2013)
- [228] M. Watson, A. Marnerides, A. Mauthe, D. Hutchison et al., *Malware detection in cloud computing infrastructures*, IEEE Transactions on Dependable and Secure Computing, **13**(2), pp.192–205 (2015)
- [229] R.M. Yadav, *Effective analysis of malware detection in cloud computing*, Computers & Security, **83**, pp.14–21 (2019)
- [230] W. Zhang, Y. Lin, J. Wu, T. Zhou, *Inference attack-resistant e-healthcare cloud system with fine-grained access control*, IEEE Transactions on Services Computing, **14**(1), pp.167–178 (2018)
- [231] X. Ma, J. Ma, S. Kumari, F. Wei, M. Shojafar, M. Alazab, *Privacy-preserving distributed multi-task learning against inference attack in cloud computing*, ACM Transactions on Internet Technology, **22**(2), pp.1–24 (2021)
- [232] I. Deznabi, M. Mobayen, N. Jafari, O. Tastan, E. Ayday, *An inference attack on genomic data using kinship, complex correlations, and phenotype information*, IEEE/ACM transactions on computational biology and bioinformatics, **15**(4), pp.1333–1343 (2017)
- [233] S. Shakya et al., *An efficient security framework for data migration in a cloud computing environment*, Journal of Artificial Intelligence, **1**(1), pp.45–53 (2019)
- [234] J.R. Ngnie Sighom, P. Zhang, L. You, *Security enhancement for data migration in the cloud*, Future Internet, **9**(3), pp.23 (2017)
- [235] S. Singh, Y.S. Jeong, J.H. Park, *A survey on cloud computing security: Issues, threats, and solutions*, Journal of Network and Computer Applications, **75**, pp.200–222 (2016)
- [236] H. Wu, K. Wolter, P. Jiao, Y. Deng, Y. Zhao, M. Xu, *Eedto: an energy-efficient dynamic task offloading algorithm for blockchain-enabled iot-edge-cloud orchestrated computing*, IEEE Internet of Things Journal, **8**(4), pp.2163–2176 (2020)
- [237] H. Wu, Z. Zhang, C. Guan, K. Wolter, M. Xu, *Collaborate edge and cloud computing with distributed deep learning for smart city internet of things*, IEEE Internet of Things Journal, **7**(9), pp.8099–8110 (2020)
- [238] L. Xu, D. Huang, W.T. Tsai, *Cloud-based virtual laboratory for network security education*, IEEE Transactions on Education, **57**(3), pp.145–150 (2013)
- [239] M. Xu, A.N. Toosi, R. Buyya, *A self-adaptive approach for managing applications and harnessing renewable energy for sustainable cloud computing*, IEEE Transactions on Sustainable Computing, **6**(4), pp.544–558 (2021)
- [240] M. Souppaya, J. Morello, K. Scarfone, Tech. rep., National Institute of Standards and Technology (2017)

- [241] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, R. Buyya, *Ensuring security and privacy preservation for cloud data services*, ACM Computing Surveys, **49**(1), pp.1–39 (2016)
- [242] J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning, *Managing security of virtual machine images in a cloud environment*, in *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 91–96 (2009)
- [243] F. Loukidis-Andreou, I. Giannakopoulos, K. Doka, N. Koziris, *Docker-Sec: A Fully Automated Container Security Enhancement Mechanism*, in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, pp. 1561–1564 (2018)
- [244] S. Kwon, J.H. Lee, *Divds: Docker image vulnerability diagnostic system*, IEEE Access, **8**, pp.42666–42673 (2020)
- [245] W. Huang, A. Ganjali, B.H. Kim, S. Oh, D. Lie, *The state of public infrastructure-as-a-service cloud security*, ACM Computing Surveys, **47**(4), pp.1–31 (2015)
- [246] K. Lin, W. Liu, K. Zhang, B. Tu, *HyperMI: A privilege-level VM protection approach against compromised hypervisor*, in *2019 18th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference On Big Data Science and Engineering (TrustCom/BigDataSE)*, pp. 58–65 (IEEE, 2019)
- [247] S.W. Li, J.S. Koh, J. Nieh, *Protecting cloud virtual machines from hypervisor and host operating system exploits*, in *28th USENIX Security Symposium (USENIX Security 19)*, pp. 1357–1374 (2019)
- [248] W. Liu, K. Zhang, B. Tu, K. Lin, *HyperPS: A Hypervisor Monitoring Approach Based on Privilege Separation*, in *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 981–988 (IEEE, 2019)
- [249] A. Khalimov, S. Benahmed, R. Hussain, S.A. Kazmi, A. Oracevic, F. Hussain, F. Ahmad, C.A. Kerrache, *Container-based sandboxes for malware analysis: A compromise worth considering*, in *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing*, pp. 219–227 (2019)



**Nan Li** received the B.Sc. degree from Xidian University (Xi’an, China) in 2007, the M.Sc. degree from University of Electronic Science and Technology of China (Chengdu, China) in 2010 and her Ph.D. degree from KTH Royal Institute of Technology (Stockholm, Sweden) in March 2018, all in Electrical Engineering. She is now an Associate Professor at Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences (Shenzhen, China). Her research interests include wireless communication theory, information theory, Internet of Things, network and information security and recently she has been probing into relevant

areas including covert communications and quantum communications.



**Minxian Xu** is currently an Associate Professor at Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences. He received the BSc degree in 2012 and the MSc degree in 2015, both in software engineering from University of Electronic Science and Technology of China. He obtained his PhD degree from the University of Melbourne in 2019. His research interests include resource scheduling and optimization in cloud computing. He has co-authored 40+ peer-reviewed papers published in prominent international journals and conferences, such as ACM CSUR, ACM TOIT, IEEE TSUSC, IEEE TCC, IEEE TASE, IEEE TGCN, JPDC and JSS. His Ph.D. Thesis was awarded the 2019 IEEE TCSC Outstanding Ph.D. Dissertation Award.



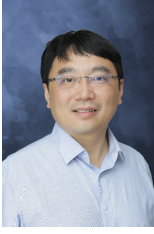
**Qimeng Li** graduated from the University of Calabria (UNICAL) with a master's degree in electrical engineering in 2017. And he received his Ph.D. in Information and Communication Technologies at UNICAL in 2022. His main research interests lie mainly in the field of multi-user activity recognition, wearable computing, e-health system, and the Internet of Things. In particular, the main research directions focus on the definition, methods, architecture, and system verification of multi-user activity recognition. He has authored and co-authored 20+ conference and journal papers, some of which have been published in top journals, including Information Fusion.



**Jikui Liu** received the B.S. degree in biomedical engineering from the Shandong First Medical University, Taian, China, in 2010, the M.S. degrees from Changchun University of Science and Technology, Changchun, China, in 2013, and the Ph.D. degree in computer applications technology from University of Chinese Academy of Sciences, Shenzhen, China. His research interests include biomedical signal processing, medical image processing, biometrics, machine learning, internet of medical things (IoMT) and wearable intelligent monitoring of cardiovascular disease. He has co-authored 15+ peer-reviewed papers published in international journals and conferences, such as IEEE IoT, IEEE JBHI, Information Fusion.



**Shudi Bao** received the B.S. degree from Ningbo University, Ningbo, China, in 1999, and the M.S. and Ph.D. degrees from Southeast University, Nanjing, China, in 2003 and 2007, respectively, all in communications and information systems. She was a Research Assistant at the Joint Research Centre for Biomedical Engineering, Chinese University of Hong Kong, a Research Associate at Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, and a visiting scholar at Imperial Collage London. She is currently a Professor at Ningbo University of Technology and also the dean of School of Computer Science and Technology. Her research interests included information security, private computing, and Internet-of-Things in healthcare.



**Ye Li** received the B.S. and M.S. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 1999 and 2002, respectively, and the Ph.D. degree from Arizona State University, AZ, U.S. in 2006, all in electrical engineering. Since 2008, he has been the Director of the Research Center for Biomedical Information Technology, Shenzhen Institute of Advanced Technology, where he is currently a full Professor with the Chinese Academy of Sciences. His current research interests include wireless body sensor networks, wearable sensors, mobile health, and medical signal processing and analysis using artificial intelligence.



**Jianzhong Li** is a chair professor at Shenzhen Institute of Advanced Technology and a professor at Harbin Institute of Technology, China. His current research interests include big data computation and wireless sensor networks. He has published more than 400 papers in refereed journals and conference proceedings, such as VLDB Journal, IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Parallel and Distributed Systems, SIGMOD, VLDB, ICDE and INFOCOM. His papers have been cited more 20000 times and His H-index is 65. He has been involved in the program committees of major computer science and technology conferences, including SIGMOD, VLDB, ICDE, and INFOCOM. He has also served on the editorial boards for distinguished journals, such as IEEE Transactions on Knowledge and Data Engineering, and refereed papers for varied journals and proceedings.



**Hairong Zheng** is presently the deputy director and professor of Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, and the director of the National Innovation Center for High-Performance Medical Devices. He is also the vice President of Chinese Society of Biomedical Engineering and the Executive member of the International Federation of Medical and Bioengineering (IFMBE). He is committed to the research and development of medical imaging technology and instruments, including ultrasound and magnetic resonance imaging. He proposed the fast imaging theory of physical and mathematical prior information fusion, systematically solved the problem of high-field fast MR imaging technology and realized clinical applications. He developed non-linear acoustic radiation force theory, invented ultrasonic shear wave quantitative elastography instrument and the original non-invasive ultrasonic neuromodulation technology. He is the National 973 chief scientist, the winner of the National Outstanding Youth Fund, and successively won the China Youth Science and Technology Award, the Ho Leung Ho Lee Science and Technology Innovation Award, and the National Innovation Award. He has also won the first prize of the National Science and Technology Progress Award.