

Medical and Healthcare

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

Nan Li¹, Minxian Xu¹, Qimeng Li^{1,2}, Jikui Liu¹, Shudi Bao³, Ye Li^{1,*},
Jianzhong Li¹, and Hairong Zheng¹

¹ Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, Shenzhen 518055, China

² University of Calabria, Rende 87036, Italy

³ Ningbo University of Technology, Ningbo 315211, China

Received: 10 June 2022 / Accepted: 2 December 2022 / Published online: 31 January 2023

Abstract Precision medicine provides a holistic perspective of an individual's health, including genetic, environmental, and lifestyle aspects to realize individualized therapy. The development of the internet of things (IoT) devices, the widespread emergence of electronic medical records (EMR), and the rapid progress of cloud computing and artificial intelligence provide an opportunity to collect 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 toward prediction and prevention, *i.e.*, precision health. To this end, various types of data such as omics, imaging, EMR, continuous physiological monitoring, lifestyle, and environmental information, need to be collected, tracked, managed and shared. Thus, internet-of-medical things (IoMT) is crucial for assimilating the health systems, applications, services, and devices that can improve the speed and accuracy of diagnosis and treatments along with real-time monitoring and modification of patient behavior as well as health status. However, security has emerged as a growing concern owing to the proliferation of IoMT devices. The increasing interconnectivity of IoMT-enabled devices with health data reception, transmission, and processing significantly increases the number of potential vulnerabilities within a system. To address the security issues of precision health in IoMT systems, this study reviews the state-of-the-art techniques and schemes from the perspective of a hierarchical system architecture. We present an IoMT system model comprising three layers: the sensing layer, network layer, and cloud infrastructure layer. In particular, we discuss the vulnerabilities and threats to security in each layer and review the existing security techniques and schemes corresponding to the system components along with their functionalities. Owing to the unique nature of biometric features in medical and health services, we highlight the biometrics-based technologies applied in IoMT systems, which contribute toward a considerable difference between the security solutions of existing IoT systems. Furthermore, we summarize the challenges and future research directions of IoMT systems to ensure an improved and more secure future of precision health.

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

Citation Li N, Xu M and Li Q et al. A review of security issues and solutions for precision health in Internet-of-Medical-Things systems. Security and Safety 2023; 2: 2022010. <https://doi.org/10.1051/sands/2022010>

* Corresponding author (email: ye.li@siat.ac.cn)

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

© The Author(s) 2023. Published by EDP Sciences and China Science Publishing & Media Ltd.

1 Introduction

In 2015, the President of the United States, Barack Obama proposed the “Precision Medicine Initiative” in his address to the State of the Union, which aims to revolutionize the approach to improving health and treating diseases [1]. Precision medicine primarily relies on the genetic, imaging, biochemical, and other data obtained in a hospital to formulate individualized diagnoses and treatment plans for patients. However, as the development of diseases and the occurrence of symptoms entail a dynamic process, an early diagnosis and comprehensive assessment of the disease cannot be achieved by relying only on the static data measured in the hospital. Therefore, disease prevention and early diagnosis require multidimensional dynamic monitoring data outside the hospital. To promote the development of precision medicine, developed countries such as the United States have successively launched precision health research programs since 2018. As such, precision health research primarily emphasizes the crucial role of prevention in maintaining health throughout the lifespan [2]. Similarly, the Chinese government has proposed the concept of prevention-oriented health management in its plan for Healthy China 2030. In this paradigm, an individual’s disease risk assessment is based on their genetic profile and family history, even including prenatal health monitoring information [3]. Precision health aims to increase the accessibility of healthcare contact by integrating monitoring and diagnostics into everyday life. This requires multiple types of sensors and devices to continuously monitor physiological signals (*e.g.*, blood pressure (BP), electrocardiogram (ECG), photoplethysmography (PPG), among others), biochemical indicators (*e.g.*, blood sugar, biomarkers), behaviors, and other health data collected outside the hospital (Figure 1). Owing to the recent development of internet of things (IoT) technology, the long-term monitoring of human health-related data can be performed using human sensor networks and medical equipment [4–8]. As such, IoT has assisted healthcare providers to develop new methods of assistance and has been integral in monitoring and curing diseases. The adoption of IoT has revolutionized the healthcare industry by enabling providers to remotely monitor patients’ health through medical and wearable devices connected via the internet of medical things (IoMT) [9].

IoMT technology is transforming the face of healthcare and promises the potential to significantly improve patient access and system efficiencies. Specifically, in the 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, including new processes to support their adoption and implementation across healthcare modalities [10–12]. The potential benefits of IoMT can be justified within a hospital setting, where monitoring COVID-19 patients is expensive in terms of time and personal protective equipment consumption [13]. IoMT technologies enable medical devices to transmit data to medical practitioners, who can monitor a patient’s condition without reading the bedside records. The same technologies can enable the safe monitoring of patients who do not require hospitalization and can be treated 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, and NB-IoT. It has revolutionized the approach to patient assessment and healthcare data management [14–16]. Existing medical devices can be modified to IoMT devices for real-time acquisition and storage of data in a centralized or distributed location. In particular, alarms and notifications can be set according to various rules and defined thresholds, which can be applied to the collected data to detect and predict deviations [17]. In addition to discovering trends in a patient’s specific disease or health condition [18], IoMT-enabled devices can facilitate health guidance by 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 acquire data on patients’ activities and related vital changes [8, 22]. Moreover, advanced sensors, convertors, and firmware at the device level enable users to analyze and correlate various vital signs with their health conditions [23]. In summary, IoMT can increase access from either the patients/caregivers or the healthcare practitioners and serve as a support manifold for medical services to enhance the quality of services. Considering that IoMT system-assisted precision health is applied in diverse scenarios, IoMT services can be classified into the following categories:

- (1) Real-time control service. In this case, a fast and accurate 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 conformed. Typical application scenarios include remote diagnosis, ambulance vehicular first-aid, remote surgery, and remote biomedical monitoring in the intensive care unit (ICU).

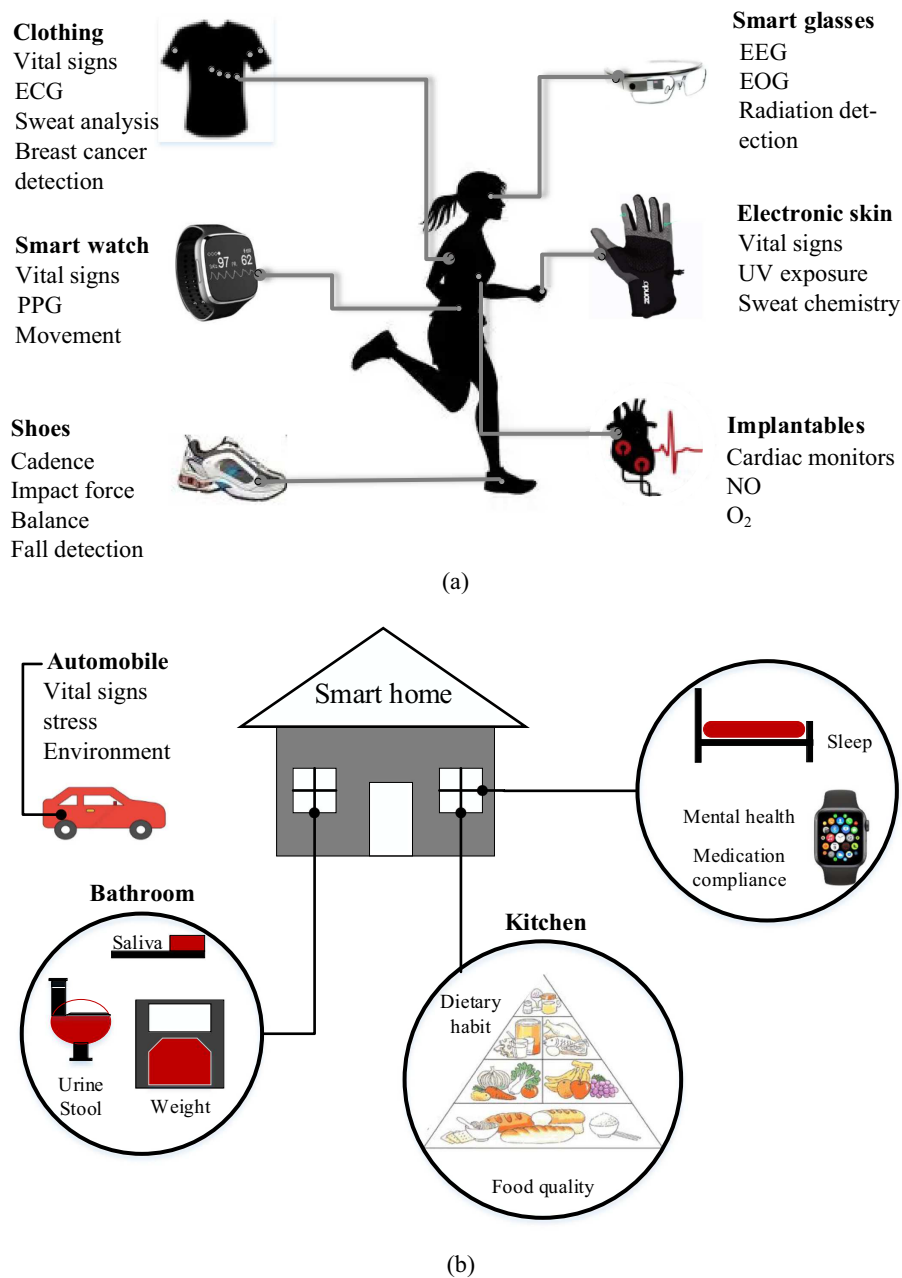


Figure 1. Multiple physiological data monitoring outside hospital. (a) Wearable devices for multi-physiological monitoring; (b) devices installed in home or automobile can passively monitor various physiological data such as biological fluids, human behavior, and physiological signals

- (2) Information exchange service. This modality involves forwarding a massive amount of medical-related data to remote data centers. Although extremely high network throughput is required in general, the demands for packet loss rate and latency are not restricted. Typical application scenarios include 24-h health data uploading and remote health education video display.
- (3) Periodic monitoring service. This is a common service modality in e-health and occupies a considerable proportion of the overall network traffic. This kind of service exhibits strong regularity and involves low requirements for minimizing delay. Typical application scenarios include remote ward rounds, in-home chronic disease management, and community rehabilitation therapy.
- (4) Event-driven service. This service is characterized by sudden, emergent, and unpredictable scenarios under the most stringent real-time constraint, such that the medical staff or caregiver can

Table 1. Comparison of this study 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 <i>et al.</i> [33]	Cryptographic techniques	○	●	●	●	○	●
Koutras <i>et al.</i> [34]	Communication protocols	●	○	●	●	●	●
Hatzivasilis <i>et al.</i> [35]	Circular economy-featured	○	○	●	●	●	●
Hathaliya <i>et al.</i> [36]	Security and privacy in Healthcare 4.0	●	●	○	○	●	●
Newaz <i>et al.</i> [37]	Attack-aspect and corresponding defense	●	●	●	●	○	●
Yaqoob <i>et al.</i> [38]	Security for medical devices	○	○	●	●	●	●
Our work	Security in hierarchical IoMT systems	●	●	●	●	●	●

● and ○ represent yes and no, respectively.

rapidly reach on-site and timely provide the necessary assistance. Typical application scenarios include health monitoring alarms, elders falling alarms, and other emergency events.

In the IoMT system, modern technologies such as 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 the patient’s safety and privacy [25, 26]. In addition to the medical devices connected to home networks, public Wi-Fi, or cellular networks, the increasing amount of valuable data from healthcare applications and platforms stored in the cloud is susceptible to hacking, which renders them prime targets [27–32]. With catastrophic consequences, any security concerns related to the healthcare system should be proactively addressed. In this case, security is one of the most critical issues in the IoMT systems as well as the healthcare industry.

Recent literature includes surveys reporting various taxonomies of potential threats and attacks, corresponding security and privacy issues, and proposed techniques and solutions across multiple research areas. As summarized in Table 1, the most recent studies review the security of IoMT systems from various aspects. Yaqoob *et al.* [38] discussed the security risks encountered by medical devices along with solutions. Koutras *et al.* [34] summarized the communication protocols applicable of IoMT systems and compared their scope of application. Specifically, from the aspect of cryptography, Ghubaish *et al.* [33] studied numerous cryptographic techniques. More recently, Newaz *et al.* [37] classified the potential attacks in various types to IoMT systems. In addition, studies have focused on an aspect of analysis, such as the application scenario in Healthcare 4.0 [36] and circular economy [35]. Compared to previously reported surveys, the present research is novel as it completely covers the entire process of health data in IoMT systems. This review discusses an integrated system incorporating medical devices, network connections, and cloud platforms. The attacks possible in the data processing stages as well as the corresponding security solutions are reviewed based on the collection, aggregation, communication, and analysis of data. In particular, this study focuses on the entire system architecture, covering the security risks and technologies in multiple functional layers. To this end, the aspects of network service and system architecture have been thoroughly reviewed in this paper.

In addition, the issue of functional safety cannot be neglected for the IoMT system. Functional safety is a component of overall safety and relies on the appropriate response of a system or device to its inputs. The safety objectives are achieved by implementing each specific safety function and satisfying the required level of performance for each safety function [39]. Although the utilization of central processing units (CPUs) and software has improved traditional functional safety, it has inevitably introduced network security issues. With the continuous development of human-machine-material integration, network security and functional safety have become an inseparably integrated security issue, and their connotation and extension will continue to expand in depth and breadth [40, 41].

With the recent advancements in security technologies that aim to address the 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 major contributions can be summarized as follows:

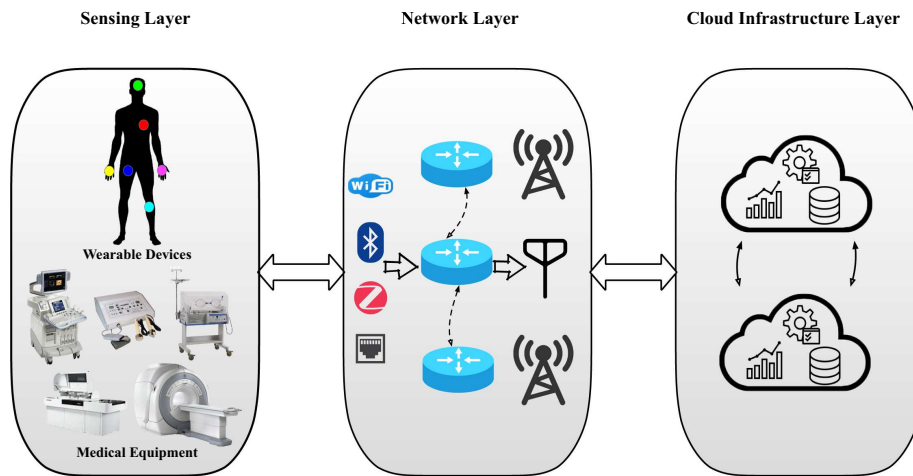


Figure 2. Hierarchical architecture of IoMT systems

- We construct a hierarchical IoMT system architecture comprising three layers: sensing layer, network layer, and cloud infrastructure layer. The connected devices, communication technologies, and the provided resources are briefly introduced in each layer. To emphasize the distinct features of the IoMT systems in comparison with the general IoT systems, the specific security requirements are summarized 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 has been provided in tabular form.
- We focus on the biometrics-based technologies applied in IoMT systems owing to the unique nature of biometric features in medical and health services. Although existing studies primarily focus on the security issues related to authentication and key management, they provide insights regarding the utilization of biometrics for security purposes, which are promising for extensive application.

A brief overview of the security issues in the IoMT system is described in the following section. Initially, we construct a three-layer IoMT system, and thereafter, introduce the fundamental components and applied technologies in each layer to perform various functions.

2 Overview of security in IoMT system

2.1 System architecture

To comprehend the communication structure followed by patients and devices to interact with the physicians, hospital management systems, and data analytics systems, the IoMT system architecture is illustrated in Figure 2, which comprises three layers: sensing layer, network layer, and cloud infrastructure layer. These layers include all stages of data acquisition and processing, starting from an individual's biometric collection stage to data storage and the subsequent processing and analysis.

2.1.1 Sensing layer

The sensing layer is composed of wireless medical devices integrating a set of intelligent, small-sized, and resource-constrained wireless on-body and in-body sensors to store, process, and monitor various psychological parameters required for diagnosis. In addition, it includes all the medical equipment in the hospital, *e.g.*, radiology and ICU equipment, ventilators, and dialysis machines, used in treatments. The devices include various types of sensors, classified into the following categories.

- *Wearables devices* are integrated into wearable objects or directly placed on the body to monitor health and/or provide clinically relevant data for care. Based on requirement and usage, these devices are further segmented into consumer wearables, clinical wearables, implantable devices, and ambient devices.

- *Consumer wearables* are generally used for real-time monitoring of physiological signals (BP, ECG, PPG) and behavioral data (gait, acceleration) from the body surface.
- *Implantable device* is a type of medical device that is placed inside a patient's body during a medical procedure such as surgery. Certain examples of state-of-the-art implantable devices include pacemakers and smart pills (also known as smart drugs or digital pills). Existing ingestible pills, *e.g.*, capsule endoscopy can record a patient's gastrointestinal information over a longer period outside the hospital, and various sensors can be incorporated to acquire additional information.
- *Ambient devices* include a series of sensors such as motion detectors, contact switches, break-beam sensors, and pressure mats used for detecting environmental information/ambient variations in a specific environment (*e.g.*, home and workplace).
- *Medical equipment* fundamentally includes medical imaging, biochemistry analyzers, and bedside monitors for disease screening in hospitals.
 - *Medical imaging equipment* refers to detection instruments that acquire information regarding the human body structure through medical imaging technology, *e.g.*, magnetic resonance imaging (MRI), computed tomography, and ultrasonography (USG). The medical image data exhibits the characteristics of large data size and low real-time requirements.
 - *Biochemistry analyzer* is mainly used to detect various biochemical markers in the human body, and the detected data exhibit characteristics of small data volumes and low real-time requirements.
 - *Bedside monitor* is used for real-time monitoring of all types of physiological parameters of the patients in the ward, and it relies strongly on real-time data transmission to timely alert the occurrence of dangerous events.

2.1.2 Network layer

The network layer transmits the data recorded by the sensing devices or medical equipment to a local gateway and a remote platform via wired or wireless communication protocols. Health providers can access the sensed patient information through the gateway. To perform health-related tasks, several gateways are distributed geographically through edge/fog computing. The gateway can bridge the internet/local switches and wireless sensor networks (WSNs) as it supports multiple protocols. Networked medical devices require both wireless short-range standards and wired technologies to efficiently perform their respective tasks. Personal area network (PAN) comprising short-distance technologies such as ZigBee, Bluetooth, and ultrawideband (UWB) or local area network, ethernet, and Wi-Fi connection. This is used to transfer the sensed information to the gateway. Wide area network (WAN) such as the global system for mobile communication (GSM) do not require connectivity but employ backend servers/applications and WSNs, which are capable of accommodating numerous sensor nodes. This feature can be utilized in certain sensors requiring low-power connectivity. The data are communicated through various technologies described below and the comparison is listed in Table 2.

- *Radio-Frequency Identification (RFID)*- is a short-range communication tag that does not require any external power source but is highly insecure.
- *Near Field Communications (NFC)*- operates in two modes: in active mode, the radio frequency and data transmission are simultaneously produced without pairing, whereas in the passive mode, the 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, tracking, and sniffing [43]. Owing to its low power consumption, BLE is appropriate for sensor-based medical devices.
- *ZigBee*- is used by most sensor-based devices for interconnected, uninterrupted connections between medical devices. Its low-power consumption renders it an ideal choice for healthcare applications, assisted by its sleep mode feature. Advanced encryption standard (AES) algorithm along with a 128-bit key is used to provide security in this standard, which is vulnerable to energy depletion attacks, replay attacks, and sniffing [44]. Moreover, AES is unsuitable for resource-constrained sensory devices.
- *Wi-Fi*- all devices, laptops, tablets, and smartphones are Wi-Fi integrated, and its high-energy consumption emerges as a considerable limitation.

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	10 cm–200 m	Varies with frequency	30 K–2.45 GHz	–	–
	NFC	20 cm	424 Kbps	13.56 MHz	Low	–
	Bluetooth/BLE	10–100 m	2.1 Mbps	2.4–2.5 GHz	Low/Very low	IEEE 802.15.1
	Zigbee	10–200 m	250 Kbps	2.4 GHz	Low	IEEE 802.15.4
	Wi-Fi	100–300 m	54 Mbps	2.4/5 GHz	High	IEEE 802.11
	6LoWPAN	10–100 m	50 Kbps	2.4 GHz	Low	IPv6 and IEEE 802.15.4
Wide Area Network (WAN)	Ethernet	Wired	400 Gbps	–	Very high	IEEE 802.3
	Cellular network	10–30 km	20 Gbps	600 M–6 GHz 24–60 GHz	Very high	–

- *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)*- is inexpensive, easily adaptable, and consumes less power, which makes it suitable for sensor-based IoMT systems.
- *Ethernet*- as one of the most widely used standards proposed by the IEEE for wired connectivity, ethernet enables the provision of connectionless user data integrity, origin authenticity, and data confidentiality.
- *Cellular Networks*- The security solutions have been adequately regulated and applied. The evolution of 5G cellular networks provides immense technical support such as software-defined networks and network slicing to ensure a more reliable communication system.

2.1.3 Cloud infrastructure layer

The cloud infrastructure layer represents the infrastructure providing physical/virtual resources to support the operation of the applications at the sensing layer [45]. The data acquired at the sensing layer can be transmitted from the network layer, and thereafter, stored in the cloud infrastructure layer. The typical resources that can be provisioned are stated as follows:

- *Processing capability*- During the cloud deployment of applications, the cloud infrastructure can provision computation resources and memory to process the data. For instance, the collected medical data are required to be analyzed by complicated data computation models. In particular, adequate computation resources should be assigned to execute the computation-intensive tasks and ensure the quality of the supported services.
- *Storage capability*- Medical data can be stored in the cloud to relieve the bottleneck in local storage. Generally, cloud storage offers efficient data storage and access methods to support the execution of applications. The hardware of the cloud storage is provided by the manufacturers and can be managed by a cloud manager to ensure data security. cloud storage should be reliable, consistent, and fault-tolerant.
- *Virtualized resources*- By leveraging virtualization technology, the physical resources can be transformed into virtualized resources and shared by multiple users more efficiently, *i.e.*, a single physical machine can be virtualized into eight virtual machines in Amazon. The virtualized resources can be instantiated using virtual machines (VMs) or microservice-based containers. In addition to directly accessing the physical resources, the users can hire VMs to implement their applications.

2.2 Security metrics based on the IoMT service demands

Compared to conventional IoT systems, the IoMT system closely caters to the service demand. According to the IoMT service categories listed in Section 1, the performance demands can be classified as follows.

- (1) *Timeliness*. Health care requires prompt delivery for the benefit of patients as well as health care providers, especially when IoMT enables remote monitoring and treatment. Nonetheless, the time required for decision-making and the feedback delay of IoMT applications varies for each case of application. For instance, a patient's condition is tracked regularly during chronic disease monitoring, and doctors are required to perform accurate and timely diagnoses in clinical decision support systems.

- (2) *Diversity*. The IoMT system incorporates medical devices with mobile applications, multisource data, processes (monitoring and care delivery), and individuals (patients, providers, professionals). Thus, the IoMT system is expected to generate and consolidate measurable information from various sources to improve the treatment speed and accuracy of an individual's service requirement.
- (3) *Accuracy*. Accuracy should be consistent for every component of IoMT, because accurate information delivery is life-critical across all stages—from data acquirement, transmission, and storage to analysis and decision-making for treatment.
- (4) *Reliability*. A reliable IoMT system must achieve its functional goals in all cases, implying that it should not be prone to unexpected failure under normal operating conditions. The potential diagnostic nature of IoMT-based systems mandates the reliability of every system component to ensure the correctness of the delivered information and services.
- (5) *Scalability*. To manage the exponential growth of various kinds of medical services, IoMT applications must be able to support an increasing number of connected devices (including the types stated in Section 2.1), users (with various service requirements), application features, and analytics capabilities, without any degradation in the quality of service. Thus, IoMT applications should be scalable to monitor, secure, and manage an increasing number of devices by proportionately increasing the resources.

However, to satisfy all the demands of the aforementioned services, the IoMT currently suffers from a major limitation of weak security. As such, any exploited vulnerability in the IoMT enables cybercriminals to enact a multitude 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 ransomware the device to yield a profit. Furthermore, IoMT demands stronger security, because, unlike other industries, a security breach in a healthcare network can practically result in loss of lives [46]. Thus, the security requirements of the IoMT systems are more rigorous than that of typical IoT-based infrastructures [47–49]. Based on these service demands, the security of IoMT systems is predominantly focused on the following metrics.

- *Confidentiality/Privacy*. This refers to the ability to maintain the privacy of the data during its acquirement, transmission, or storage. In addition, they should be accessible only to authorized users. Specifically, the collection and storage of patient health data must conform to legal and ethical privacy regulations, *e.g.*, General Data Protection Regulation and Health Insurance Portability and Accountability Act of 1996 (HIPAA) [50], states that only authorized individuals can access such data. To prevent data security breaches, adequate measures must be adopted to ensure the confidentiality of the health data associated with individual patients. The significance of such measures cannot be overemphasized, as the data stolen by cyber criminals could be traded in illegal markets, thereby causing the patients to suffer from privacy violations as well as possible financial and reputational damages.
- *Integrity*. This relates to the capability of protecting the data from any unauthorized tampering during the stages of collection, transmission, and storage. For IoMT systems, data integrity aims to ensure that the data received at the intended destination are completely uncompromised during wireless transmission [51]. Attackers could gain access to and modify the patient data by leveraging the broadcast characteristic of the wireless network, which can cause severe implications in life-threatening cases. To ensure data integrity, 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 any alteration of the transferred data by malicious attacks. Moreover, the integrity of the data stored in the medical servers needs to be ensured by validating that the data cannot be tampered with.
- *Availability*. Services and data must be accessible to the relevant users on demand. These services and data, provided by medical servers and devices, will be rendered inaccessible in case of denial of service (DoS) attacks. Any inaccessible data or services can aggravate life-threatening incidents such as with no prompt alerts in case of a heart attack. Therefore, to accommodate the possibility of availability loss, healthcare applications must be functional round-the-clock to ensure data availability to the users and emergency services [52].
- *Authenticity*. This refers to the ability to validate the identity of a user accessing the system. Overall, mutual authentication is the most secure form in which both the server and client authenticate

each other prior to any secure data/key exchange. As patients' data are often stored and aggregated at the personal server level before being forwarded to the medical servers in the IoMT systems, the data should be strongly protected during its storage on the personal servers. Generally, security and privacy the personal server level can be ensured with the deployment of two types of authentication schemes, namely, device authentication and user authentication. Personal servers (*e.g.*, smartphones) shall perform authentication before accepting the data transmitted from the medical devices and sensors. As such, device authentication must be implemented in every IoMT system, because false information on patients' physical conditions from malicious devices can pose severe negative impacts on clinical diagnosis and care decisions [53]. The data stored either temporarily or permanently on the personal servers should be accessed only by the patients and medical staff such as caregivers, which necessitates the requirement of effective user authentication schemes [54]. A popular solution to user authentication in and personal server level utilizes biometrics, which is applicable in the IoMT systems, because most biometrics data can be conveniently sourced from wearable and implanted devices.

- *Anonymity.* The capability of concealing the identities of patients/physicians from unauthorized users during their interaction with the system. Patient-sensitive data can be classified into three categories: explicit identifiers, quasi-identifiers, and privacy attributes. Explicit identifiers uniquely indicate a patient using an ID number with the patient's name and cell phone number. A combination of quasi-identifiers can uniquely indicate a patient in terms of age, birth date, and address. Privacy information refers to sensitive attributes of a patient, such as illness and income. In the data publication process, the individual attributes of the new dataset are adequately processed, considering the distribution characteristics of the original data to protect patient privacy. Presently, random perturbation technology and data anonymity technologies are employed to resolve these issues [55].

The realization of comprehensive and integrated end-to-end solutions for the IoMT systems is key for both academia and industry. Thus, we comparatively review the state-of-the-art security strategies based on the three layers of the IoMT system architecture discussed thus far. The remainder of this article is organized as follows. In Sections 3–5, we elaborate on the potential risks and the corresponding state-of-the-art security strategies in the sensing layer, network layer, and cloud infrastructure layer, respectively. Specifically, we discuss biometrics-based technologies for authentication and key management to highlight their significance and uniqueness for IoMT systems. The challenges and potential research directions on existing problems are summarized in Section 6. Finally, the conclusions of this review are presented in Section 7.

3 State-of-the-art security strategies in IoMT sensing layer

The sensing layer is responsible for acquiring and compiling data from physical devices and is closely related to the medical devices in an IoMT environment. According to an estimate reported by the World Health Organization [56], two million distinct types of medical devices are available across the global market, categorized into more than 7000 generic device groups of various forms and sizes: from home-monitoring gadgets to enormous on-site devices. This wide variety of physical devices complicates the IoMT ecosystem for prioritizing security and ensuring optimal performance throughout its lifecycle in terms of development, configuration, and updates. Therefore, the device-level threats and solutions focusing on the hardware and onboard software/system security are discussed herein. The taxonomy is displayed in Figure 3.

3.1 Hardware-based security

Hardware security ensures the vulnerability protection that is emergent in physical devices, machines, and peripherals. A hardware attack is an exploitable weakness in the hardware of the device that can be leveraged to gain physical or remote access to the device for executing malicious activities.

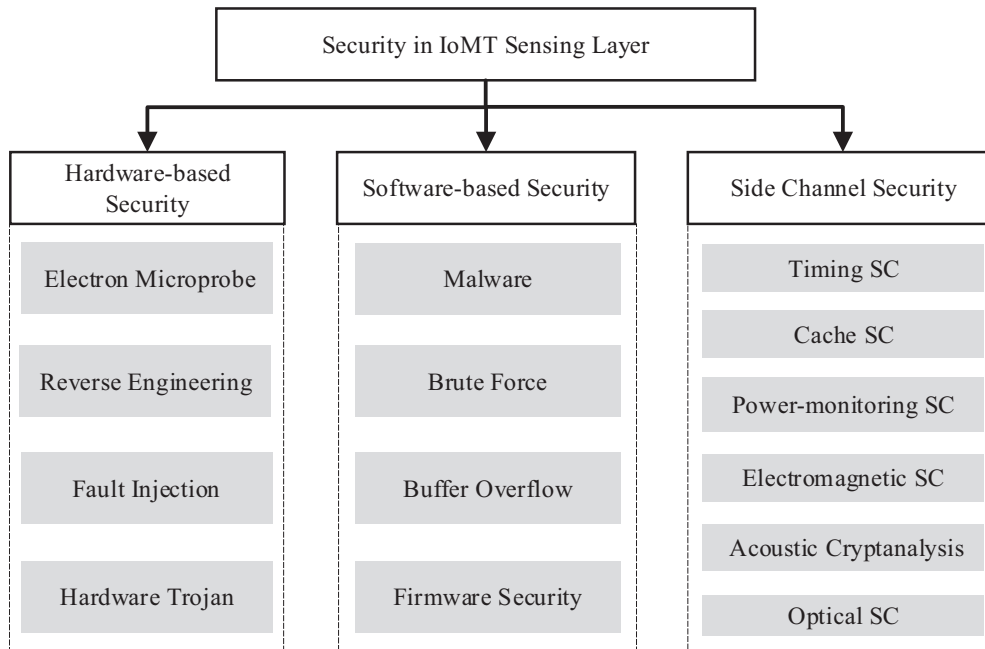


Figure 3. Classification of sensing layer security for IoMT systems

3.1.1 Electron microprobe

Electronic microprobes are used in techniques that enable an attacker to directly observe a portion or all the sensitive information such as plaintext or encryption keys. Using modern techniques of integrated-circuit (IC) editing, attackers can remove the protective layer and expose the internal chip to the air. Thereafter, using a fine-tip probe, they can analyze and extract the electrical properties, signals, and data from the interest area. ICs 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 require complete encapsulation removal as well as circuit wiring exposure. Currently, the most commonly used and powerful electron probe tool is the focused ion beam technology [60, 61], using which attackers can achieve submicron or even nano-level precision [62]. In particular, defending against such micro-probing attacks is challenging because traditional processes of IC design do not place any material under the silicon substrate. Moreover, the passive nature of both invasion methods renders them difficult to detect. However, both methods involve the detection of photon emissions, which enforces a limitation based on the wavelength of the emitted photons.

3.1.2 Reverse engineering

Invasive attacks require direct access to the inner components of the device. Reverse engineering is an analysis process that provides a complete understanding of the design of a device by extracting the information or knowledge of its inner structure [63]. The attacker can understand the internal design structure of the chip using an electron microscope and can directly analyze the data in the corresponding storage area of the chip using laser scanning. For instance, several IoT devices operate on older OS or firmware versions that are currently outdated or patched in case the vulnerabilities in the later versions are discovered or fixed. Utilizing these synergies or firmware, the attacks can directly target these unpatched vulnerabilities [64]. In this regard, a beneficial 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, wherein circuit faults can be artificially generated and introduced into the target system by establishing a specific fault model and adopting relevant strategies and methods. In addition, the data acquired through failure analysis techniques such as differential failure analysis, crash failure analysis, and invalid failure analysis can be compiled and analyzed to gain valuable information.

Hardware-based fault injection is a typical mainstream attack method involving 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 analyzed the influence of the capacitor size and voltage regulator phase number on the resilience of cryptographic circuits against 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

Through malicious modifications to the original circuitry, attackers exploit the hardware or use hardware mechanisms to access the data or software operating on a chip [68]. Hardware trojan (HT) can infect any IC, *e.g.*, application-specific ICs (ASICs), system on chips, field programmable grid arrays (FPGAs), and digital signal processors, cause catastrophic damage to the device at the hardware level.

For instance, an attacker proficient in internal hardware architecture can insert an HT during the chip manufacturing process to destroy data, which causes severe harm to medical devices [69]. HTs have emerged as a significant security risk for ICs, as most ICs are manufactured in outsourced manufacturing facilities. Third-party vendors can use uncertified intelligence cores such as Trojans to perform malicious activities, including information leakage from medical devices. The common hardware security issues are explained in the following subsections.

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 primarily includes malware, brute-force cracking, and buffer overflow attacks.

3.2.1 Malware

Upon deploying a piece of malicious code (*e.g.*, Mirai), attackers can intercept the data stored inside a device system and presume control over the victim's system or damage it. In general, attackers fake firmware updates, drivers, or security patches to distribute malware, which results in attacks on confidentiality, integrity, authenticity, and the availability of data and other system resources. Under such attacks, the sensitive data of IoMT may be disclosed, altered, or may not be even available to authorized users. Therefore, the IoMT environment essentially requires protection from malware attacks. Recent research has shifted interest from static or dynamic analysis-based approaches [70, 71] to malware detection for 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 behavioral patterns of various events to effectively detect new malware based on the insight that events can reflect all the operation activities possible in software applications.

3.2.2 Brute force

In this type of attack, the attacker will try to predict the authentication credentials of the intelligent device and will systematically review all possible passwords and passphrases until the correct password is derived. For instance, certain devices (*e.g.*, IP cameras and routers) are manufactured with default user credentials, which could easily gain access to the device by referring to the default password lists available on the internet. Although traditional cryptography methods are effective against this attack, it is not yet demonstrated as lightweight and rapid for IoT device authentication. Therefore, a hardware-based

security method, referred to as physically unclonable functions (PUFs) [73], has recently been developed to fulfill the security demand of IoT devices. In principle, this method is based on the characteristic that PUF leverages the randomness of the manufacturing process to create a physically unclonable unique identifier. For instance, certain authors [74] proposed a PUF-based identity-preserving protocol for IoT device authentication (PUF-IPA) to prevent an adversary from brute-forcing the PUF of the device to acquire challenge-response pairs, thereby locking out the device from generating unauthorized models.

3.2.3 Buffer overflow

By sending a crafted input, attackers can influence the application to execute an arbitrary code that causes the program or process to attempt writing more data into a fixed-length buffer block, and consequently, produces a buffer overflow. For decades, buffer overflows remain a major security threat plaguing cyberspace owing to the ubiquity of the software vulnerabilities it exploits and the low complexity of their launch. For instance, the first buffer overflow attack “Morris worm” occurred two decades ago, and it crashed more than 6000 web servers worldwide. To date, most research regarding this aspect focuses on software. Wang *et al.* [75] proposed polymorphic stack-smashing protection (P-SSP), with a core idea to re-randomize the canaries for a new process/thread or a new function call. Alternatively, hardware-based approaches are gradually starting to solve the buffer overflow issues. In [76], authors developed a security hardware design with an architecture comprising program offline behavior analysis and real-time hardware behavior monitoring (HRTBM) to detect buffer overflow attacks. Their experimental results demonstrated 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 inappropriate input validation or weak physical security vulnerabilities. Specifically, firmware attacks can be either static or dynamic [77].

- *Static Firmware Attack*- focuses on modifying the firmware code in the memory region or during runtime as part of the firmware update or patching process. Firmware update is a ubiquitous feature of modern embedded devices. However, prior research has demonstrated that the firmware update feature of numerous embedded devices is not adequately protected by proper user authentication [78–80]. Several devices involving certification to enable firmware updates are vulnerable to bypass attacks targeting simple management interfaces [81]. A firmware modification attack is one of the most dangerous attacks, as it can occur on various embedded systems such as telecommunication infrastructure, SCADA and PLC systems, laptop battery controllers, medical devices, network interface cards, and automated teller machines [82]. Ling *et al.* [83] injected a malicious code into a smart plug to preside over its control. The compromised firmware opens a reverse loop back-channel to the attacker’s server and generates a reverse shell, thereby providing remote access to the plug for further attacks.
- *Dynamic Firmware Attack*- exploits the dynamic memory regions (stack and heap) to circumvent secure boot and attestation, *e.g.*, code injection [84] and 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 for defense against such attacks include control-flow integrity [87] and methods based on randomization [88] and enforcement [89].

3.4 Side channel security

Side-channel attack (SCA) specifically refers to a nonintrusive attack on the cryptographic algorithm, which is cracked through the leakage of side-channel information during the operation of the encrypted electronic device. Owing to various attack sources, SCAs can be classified 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 SCA, the attacker attempts to compromise a cryptosystem by analyzing the time required to execute cryptographic algorithms. Therefore, defenses 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 can be exposed based on the timing information of the data, which attackers can exploit to recover the encryption keys. Therefore, they propose a hierarchical miss status handling register design and a software-based approach to permute the organization of critical data structures and address the vulnerabilities caused by GPU coalescing units.

3.4.2 Cache SCA

The cache attacks are based on the attacker's ability to monitor the cache accesses made by the victim in a shared physical system. For instance, an L1 cache-based attack learns the AES and asymmetric cryptography algorithm keys by analyzing the time variance of the cache usage. Recent research reported that CPU caches, including last-level cache, are vulnerable to attack. Cache randomization has recently been revived as a promising defense technique against conflict-based cache SCAs related to the stated issues. In [91], the authors determined experimentally that an attacker can easily detect a usable eviction set within the chosen remap period of CEASER-S [92] and increase the number of partitions without dynamic remapping such as ScatterCache [93], which cannot eliminate the threat. However, the issues can be fixed within the current performance budget, and the randomized set-associative caches can be adequately strengthened and possessed.

3.4.3 Power-monitoring SCA

Power-monitoring SCA is a common SCA in which the attacker measures the power consumption [94] of the encryption device under test, and subsequently, performs simple (SPA) or differential power analysis (DPA) of the obtained traces to decipher the secret key. For instance, attackers can target FPGA-based convolutional neural network accelerators by monitoring the power and managing the recovery of input images from the collected power traces, without knowing the detailed parameters in the neural network [95]. This type of SCA poses a devastating impact on the data security of online medical image analysis. In this regard, a feasible solution uses noise insertion in power consumption measurements to defend against power SCAs. In [94], the author demonstrated that noise injection in the AS domain achieves SCA immunity with extremely high efficiency. Others solutions involve balancing the power consumption of the fluctuating transitions and isolating the supply from the encryption engine. In [96], authors analyze the DPA resilience of the FinFET cryptocircuits and design a 4-bit substitution box (Sbox-4) of the PRIDE algorithm to use new devices in low-power applications. Moreover, in [97], the authors present a security countermeasure based on switching DC-DC regulators.

3.4.4 Electromagnetic SCA

Modern digital computer systems contain several components, especially the CPU and RAM, relying on electrical impulses 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. Electromagnetic SCAs are based on leaked electromagnetic radiation and can be employed to infer cryptographic keys using techniques equivalent to those in power analysis or noncryptographic attacks, *e.g.*, radiation monitoring attacks. To avoid such attacks, certain researchers have studied the protection of associated encrypted currents. In [98], the authors utilize signature attenuation hardware that locally encapsulates the crypto core within the lower metal layers, which significantly attenuates the critically correlated crypto-current signature before passing through the higher metal layers to connect to the external pin.

3.4.5 Acoustic cryptanalysis

Acoustic SCA exploits the sound signals produced during computation, generally segmented into active and passive types. For instance, similar to radar and sonar systems, the system speakers can emit sound

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]
Hardware-based security	Dynamic firmware attack	Availability, Integrity	Anomaly detection, Re-randomize	[77, 86–89]
	Electron microprobe	Privacy, Authenticity	Cryptography-based methods, Hardware sresedesigns	[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]

waves that are inaudible to the human ear, using which attackers can obtain access to the equipment by tracking the movements of the human body, arms, hands, and even fingers [99]. Upon exploiting the sound emanating from the pressed key, attackers can easily derive the password [100].

3.4.6 Optical SCA

Optical emissions from semiconductors can leak important information on embedded devices, which poses a major threat to their security. Attackers can extract sensitive information from a circuit by detecting the light emitted from a switching transistor in the form of several photons within a short period. 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 evaluated an optical SCA with three common implementations of Rivesta–Shamira–Adleman (RSA) [102] modular exponentiation and determined that the key length poses a marginal impact on its resilience to attack. To eliminate attacks such as laser logic-state imaging (LLSI), the authors proposed low-cost, circuit-based self-timed sensors to detect the critical steps implemented by attackers while performing LLSI attacks on two attack surfaces, *i.e.*, system clock (freezing) and supply voltage (modulation).

This section primarily focused on IoMT devices and peripherals security issues. A clear summary of the security issues in the sensing layer has been provided in Table 3, including compromised features, mitigation, and corresponding solutions. The security of IoMT devices still needs to encounter threats

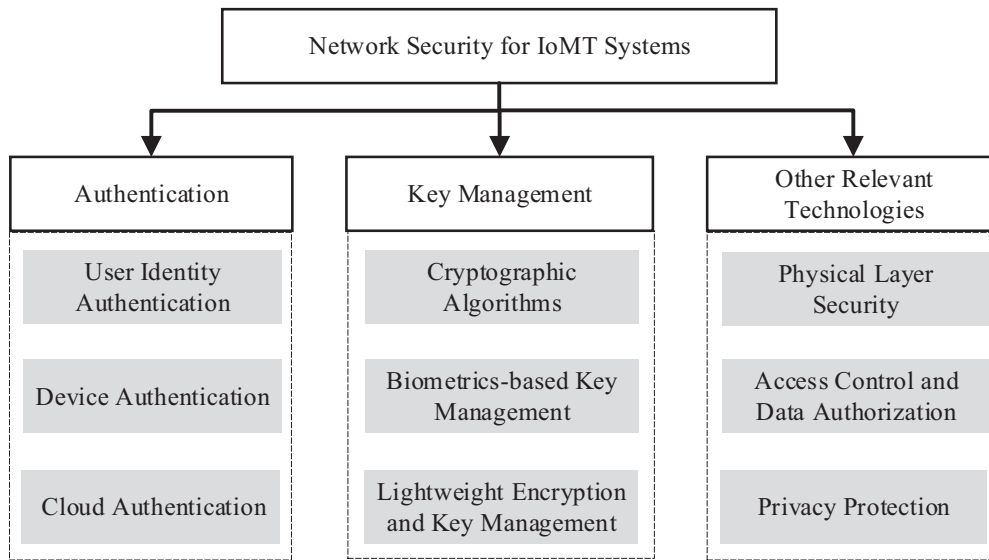


Figure 4. Classification of network security for IoMT systems

from external sources as well as the device itself. The state-of-the-art method continuously updates the hardware and software design to adapt to emerging security threats.

4 State-of-the-art security strategies in network layer

With the recent innovations in electronics including wired and wireless communications, diverse communication technologies, and network structures have been introduced in IoMT systems that may assist IoMT systems to achieve optimum performance. As discussed earlier, sensors require connectivity to the gateways and the platforms established via networks to communicate and store information either locally or centrally. The communication occurs over a wired and wireless medium and can be either short-range or long-range. Furthermore, various protocols have been employed for communications. Considering that communication fundamentally relies on backbone networks and infrastructures, the network security technologies at this level generally apply to all usage scenarios. A major component of IoMT systems is formed by WSNs, comprising numerous sensors connected via wireless communication technology that can collaborate to collect information on the covered area and enable legitimate external users to access real-time data. The sensing data are mostly transmitted over public network connections, and the sensors are often deployed in an unattended or hostile environment, which imparts vulnerability to WSNs against attacks. Therefore, for the specific application scope of IoMT systems, we discuss the major security threats and countermeasures pertaining to sensor-based networks and connections via a wireless medium. The taxonomy is presented in Figure 4.

4.1 Authentication

In IoMT systems, the security problem of data protection can be resolved by authenticating the data source through the identification of malicious users and devices. Authentication refers to the identification of the individual or group identity of users or devices by certain techniques. Generally, one-factor authentication uses an authentication technique to protect the system. In IoMT systems requiring high-level security, multifactor authentication employs a greater number of factors to protect the system. This technique promotes the resilience of the system against cyber breaks in case a factor 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 biometric signals can be of specific availability and accessibility in IoMT systems, the biometrics-based authentication methods play a unique and vital role in user authentication which will be emphatically introduced herein.

- *Password-based authentication:* Static passwords [103, 104] can remain unchanged and be reused by users for a long duration. In principle, static passwords are advantageous because of their high availability, ease of use, wide application range, and simple deployment. Nonetheless, static passwords do not contain any 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 personally carry the relevant hardware and software tokens. However, various companies manufacture their own devices, which prevented the scalability of tokens. In addition, carrying multiple tokens in all cases while ensuring their safety is highly inconvenient. Smart card relies on physical keys that are utilized as a second factor in multifactor authentication methods, with elliptic-curve cryptography (ECC) keys serving as the first factor of authentication [109]. In IoMT settings, the medical staff must enter a key and use their smart cards to access the system. Generally, the digital signature is used to verify the authenticity of the data/command following the user’s private and public keys for signature and verification, respectively. In IoMT systems, digital signatures can be integrated within the sensor’s firmware with an add-on software shim, which intercepts and validates the wireless communications of the sensors [110]. Furthermore, the x-auth-token field in the hypertext transfer protocol (HTTP) header can be used as a software token embedded in the user’s web browsers [111]. Similarly, RFID can be used as a hardware token to secure the logistic management of sensors in a hospital information system [112].
- *Biometrics-based authentication:* Biometrics-based authentication is a typical authentication technology in IoMT that utilizes the user’s unique biometric characteristics to prove their identity. Common biometrics primarily include physiological and behavioral characteristics. Physiological features are related to the user’s physical shape such as fingerprints [113, 114], facial features [115, 116], and geometric features of hands and iris. Behavioral characteristics are related to user behavior habits such as signature (handwriting), speaking mode, gait, and touch-screen habit [117–119]. The biometrics-based authentication technology does not require users to remember or store specific identity information and 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 of several kinds of biometric features used in authentication is depicted in Figure 5.

In medical care scenarios, professionals and/or patients are permitted to access medical records by using only their biometrics. The most commonly used biometric factors include fingerprint, face recognition, electrocardiogram (ECG), and electroencephalogram (EEG) which are beneficial in case of emergencies. The performance of the fingerprint-based sensors relies on the employed extraction algorithm [120]. Compared to face recognition, fingerprint authentication offers greater credibility and a substantially longer history, where systems can authenticate users by scanning their faces. Although ECG/EEG-based authentication has been developed in recent years, it increases the computational overhead during transmission compared to fingerprint-based technology [121]. ECG/EEG signals remain the primary physiological signals collected by the body sensor network [122, 123]. Although signals should be acquired from the living body, which is difficult to be simulated by other devices, time-series signals are easy to process.

Authentication depends primarily on the selection of the utilized feature(s). In past studies, numerous features such as temporal (locations and intervals among waves), amplitude (peak height of waves) and morphological variations (shapes, proportions, slopes, and angles) have been proposed to recognize individuals, which require accurate detection of fiducial markers and the results depend on the recognition procedure. In principle, fiducial-based approaches benefit from well-established normalization algorithms to compensate for the variations in ECG signal caused by heart rate variability [124, 125], but they are affected by the performance of the fiducials detection algorithms. To overcome the problem, non-fiducial-based approaches offer a promising alternative to reduce the

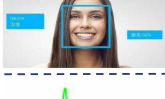
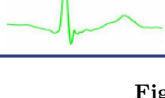
		Collectability	Security	Cost	Interference
Iris		Medium	Very High	High	Light
Voice print		High	High	Low	Cold
Finger print		High	Medium	Medium	Finger wear
Face		Very High	Medium	Medium	Age, Light, Shield
ECG		Medium	Very High	Low	Age, Cardiac disease

Figure 5. Comparison of several typical biometric features

error rate and computational effort. Accordingly, new approaches that do not require fiducial recognition include autocorrelation-based features, phase pace analysis, and frequency-based features. They do not require the identification of ECG waves and are advantageous because of considering fine features that could be lost in the case of using fiducials. To derive a deeper understanding of non-fiducial authentication, certain representative studies based on various biometric features are detailed herein. In [126], researchers proposed a multiscale power spectrum feature extraction method based on wavelet transform and artificial recognition model (Figure 6). Using a one-to-one random forest classifier combination, a more accurate identity authentication can be implemented. Moreover, a typical behavioral characteristic—gait—has been widely used for authentication. However, the gait recognition performance deteriorates dramatically if the walking speed varies. To address this issue, the speed-adaptive gait-cycle segmentation method and individualized matching threshold generation method have been proposed [127]. Moreover, as intrasubject gait fluctuation is more significant in older individuals than in young individuals owing to age-related variations, gait-based identity recognition of the aged is more challenging. In [128], a gait template synthesis method has been proposed to reduce intrasubject gait fluctuations among the elderly, and an arbitration-based score-level fusion method has been defined to improve recognition accuracy. Two matching algorithms were used to derive the preliminary decisions; in case of inconsistencies in the preliminary decisions, the third matching algorithm is applied to provide the final decision.

- **Multifactor authentication:** Recently, an increasing number of enterprises and researchers [129, 130] consider the user's biometric characteristics as a factor in multifactor authentication technology. The research relevant to this area focuses on effective and rapid extraction, measurement, and comparison of unique components of the biometrics, which are treated as a special identity of the user. For instance, in the case of 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 retains the connection between the sensor and the medical controller to secure the gateway layer. This can prevent the junior medical staff from accessing the patient data in absence of a senior medical staff who has authenticated oneself but has not logged out from the system. However, owing to the limited and unmodifiable properties of biometric characteristics, the security threat caused by biometric data leakage is irreversible. Consequently, an increasing number of users are skeptical of uploading their biometric data to remote servers that could be maliciously stolen.

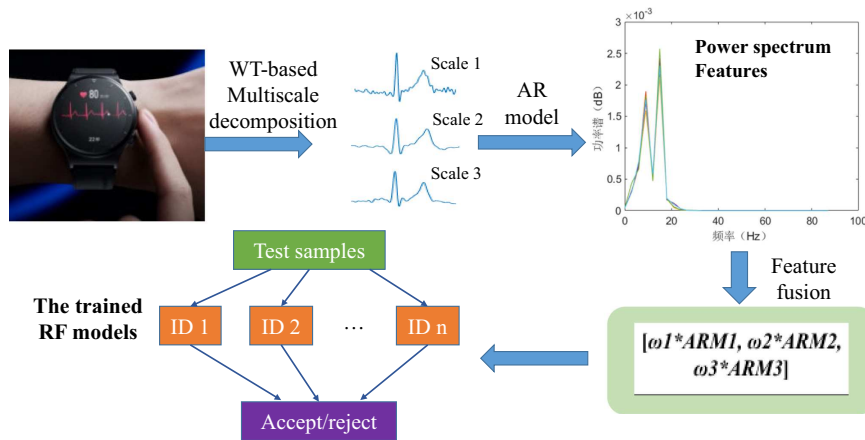


Figure 6. Flow chart of multiscale power spectrum feature extraction and identification in [126]

4.1.2 Device authentication

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

- *Digital fingerprints:* The device fingerprint is used as a label to confirm the identity in device authentication. Similar to the concept of the human fingerprint, device fingerprint refers to the device identification composed of feature information. Based on the information source, device fingerprints can be classified into software and hardware fingerprints. The feature information of the software fingerprint is sourced from the device ID, browser information, and device software environment [132–134]. Hardware fingerprint emerges 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 stated devices [144, 145]. PUF is the most common physical attribute of a device, which is a physical aspect naturally acquired from the production process and cannot be cloned. In addition, external attackers cannot easily predict the PUF of a device. Therefore, PUF is used as the “digital fingerprint” of the device and combined with cryptography technology to ensure device security. Certain studies [146, 147] consider PUFs as one of the authentication factors and propose a multifactor authentication scheme for privacy protection of IoT devices or other applications.
- *Context awareness:* Context awareness-based authentication can establish secure communication between devices as well as between devices and networks by verifying physical proximity. It can be classified into validation using the inherent properties of the device [148–150] and validation using human behavior [151–153]. Certain researchers [154, 155] proposed that certain behavioral characteristics of users can be considered for user authentication. In these studies, the authors used smart devices (e.g., Wi-Fi, smart TV, monitoring equipment) to obtain the physiological and behavioral characteristics of users in their daily use of devices and extracted 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. A strong user authentication method can firmly restrict illegal access to the cloud provider and forms the key aspect of ensuring cloud security by allowing only permitted users to access the resources and services.

- *Unauthorized User:* Cloud computing provides resources and services that are open for public use. If patients migrate their medical data to the public cloud, they will forego their restricted control over the data. Consequently, unauthorized users can deliberately access cloud data to obtain sensitive information for various reasons. For instance, the cloud service provider can predict the user’s illness by obtaining information on the medical products accessed by the user. Therefore,

access permission should be carefully provided to specific users managing the cloud [156]. To this end, Sethi *et al.* [157] proposed a 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 employ network eavesdropping in an attempt to access privileged and unauthorized access to medical data managed in the cloud. The attacker can intentionally infer users' private data without authorization. More importantly, the data can be revised with incorrect information or made entirely unavailable. Chhabra *et al.* [158] presented a security approach to prevent eavesdropping attacks on the cloud based on ECC, which can secure the services deployed in the cloud. The widely used access control approaches can be utilized to avoid this security issue in the browser [159].
- *Insecure APIs*: Cloud can allow open access to multiple APIs to enable the addition of new components that enhance their 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, wherein users can interact with the website using their login information, after which APIs authorize and fetch the account information. Moreover, poorly coded APIs may grant unnecessary access to sensitive data. To prevent this issue, the APIs for cloud resources should be carefully designed to review possible vulnerabilities and timely updates should be packed [160, 161].

4.2 Key management

Key management is the core component of system security based on cryptography, which is essential for securing IoMT systems. Symmetric cryptography includes a cryptographic algorithm based on a secret/shared key, whereas asymmetric cryptography uses both public and private keys—one for encryption/validation and another for decryption/signature, respectively. Symmetric cryptography has emerged as a focused research area of key management owing to its short key length and relatively small cost of communication and computation. However, a certain amount of resources are required to implement asymmetric cryptographic algorithms such as Diffie–Hellman algorithm. Therefore, in IoMT systems containing several resource-constrained sensors, specific schemes should be developed for exploiting the unique characteristic of medical applications. This subsection is segmented into three categories: (1) cryptographic algorithms; (2) biometrics-based key generation; (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. In particular, the exclusive OR (XOR) can be used to inspect the variations in one of its operands. After the application of XOR and hashing, the initial parameters (*i.e.*, sensor ID and shared key) are shared from the key generation server to the sensor and gateway nodes. Thereafter, these nodes can generate their keys using these parameters. The communications in IoMT systems can be secured by combining the CHF with a symmetric key and the XOR operator using the key agreement protocols proposed in [162, 163]. To resolve the problem of insecure key sharing in symmetric cryptographic algorithms, the CHF function including the ECC keys can be considered a secure certificateless channel between patients and physicians [164]. This concept enables secure key sharing between the key generation server in the cloud layer and the nodes in the IoMT sensor as well as the network layers. The ECC public key and initial parameters are hashed using CHF before transmission to the nodes generating the asymmetric keys. This technique can overcome the overhead in certificate management for data storage and share in the cloud [165]. Upon segmenting the patient's data into subsets and converting them with ECC keys and CHF, they can be securely shared among the system entities. The average energy consumption in this technique is approximately 30% less than in similar techniques. More recently, the popularity of ECC has been growing owing to its smaller key size and ability to maintain security. To satisfy the confidentiality and integrity requirements of medical applications, a novel enhanced secure sensor association and key management protocol has been designed based on ECC and hash chains [166]. In addition to satisfying the privacy demand of the patients on the medical systems, the proposed protocol can be easily implemented with higher efficiency.

4.2.2 Biometrics-based key management

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

The bio-cryptographic technique can efficiently generate cryptographic keys as it does not require a key pre-distribution mechanism or proper network setup for key generation. In addition, this approach provides an opportunity to automatically re-keying. Generally, bio-cryptographic key generation schemes are based on physiological features that are random, unique, and optimal for cryptographic keys [167]. Several researchers used this metric to generate keys, as discussed below. In [168], a bio-cryptographic key management protocol has been proposed to secure the communication of implantable and wearable medical devices. To generate secure cryptographic keys, physiological parameters such as BP, ECG, and PPG tracked by sensors have been utilized. More specifically, two recently developed approaches of physiological parameter generation include time-domain generation to derive interpulse interval (IPI) and frequency-domain generation to obtain cross-power spectral density. Both are promising candidates for generating cryptographic keys owing to their randomness and temporal variance characteristics. Similarly, heartbeat-based random binary sequences (RBSs) [169] are another approach to secure communication of sensory medical devices. This research used a finite monotonically increasing sequence generation mechanism and Hamming distance metric to excerpt entropic bits based on the IPI derived from ECG. Based on each signal, 16 random bits could be excerpted, and to authenticate users, 128-bit RBSs are generated by concatenating eight consecutive IPIs. Gait-based technique considers the human walking pattern to generate unique symmetric keys. Sun and Lo proposed a system that can generate a symmetric key within ten gait cycles using a set of IoMT sensors attached to the individual's body. They claimed 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]. By definition, the gait cycle is one cycle of movement between two repetitive events during walking. This system employs an artificial neural network model to generate 13 bits per gait cycle, which will generate a 128-bit key in ten gait cycles, which can be used to secure the communication 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 various intervals, which induces randomness to the keys without direct user interaction with the system. In addition to key generation, the bio-cryptographic technique ensures key sharing between nodes in case of 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 attached to or implanted inside 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 have explored the use of this conduit in the security mechanism of body-area sensor networks (BSNs), *i.e.*, using a biometrics-based 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 the availability of a robust and secured key distribution scheme. In this respect, random numbers produced from physiological signals are used for encrypting and decrypting 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 record its own copy of the trait and use it to decommit the key. If the selected characteristic uniquely represents an individual, the encryption key can be recovered only using the trait obtained from the same individual. Researchers developed a specific symmetric bio-cryptosystem for BSN, considering the generation of the encryption key from physiological signals and its randomness evaluation. This biometric solution is suitable for securing BSN in IoMT, because it achieves a higher level of security 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 be used as an identity for entity authentication in a BSN (*i.e.*, node-to-node authentication). Furthermore, a possible two-session communication protocol has been discussed, wherein the server initiates the communication by transmitting the biometric trait along with a nonce to the client for comparison. If the trait and nonce match, the client responds by transmitting the nonce along with

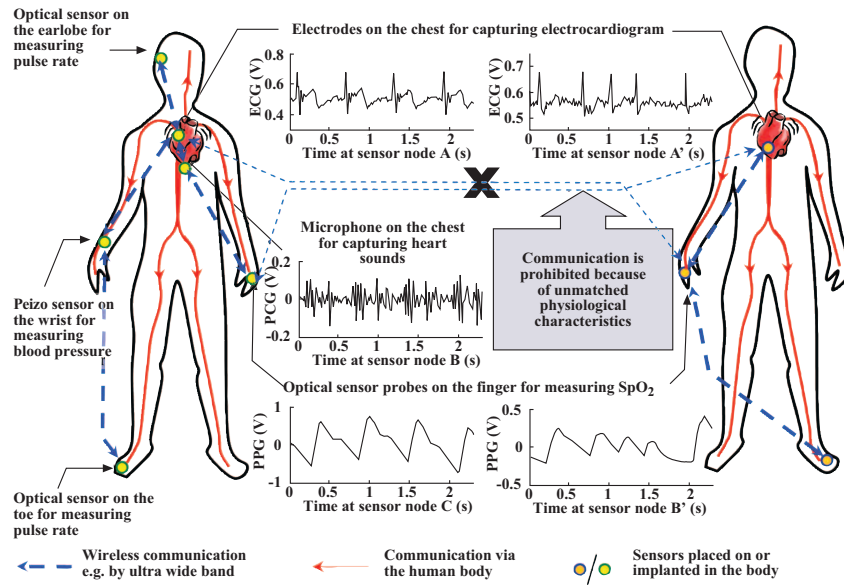


Figure 7. Application of biometrics-based approach to secure interbody area sensor network communications [171]

the variant biometric trait. A communication pathway would be established only if both the server and client verified the correspondence of the received copy with that in hand.

Another key-sharing scheme is based on fuzzy pattern recognition, primarily including a fuzzy vault for secure key distribution that is suitable for features from disordered or irregular physiological signals [172, 173]. A shared symmetric key is used to enable communication and require one entity to project the security attributes calculated from the physiological signals on a polynomial and transfer the attribute points along with the chaff points to the other side recreating the polynomial centered on certain common attributes. This scheme enhances security by minimizing the rate of data exchange during the key management process, and therefore, increases the lifespan and energy efficiency of the network [174]. However, owing to the small size of the attributes, the security of this scheme is entirely dependent on the weak vault size [175, 176], which indicates that an adversary can estimate the appropriate points in the vault.

4.2.3 Lightweight encryption and key management

In the 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 [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.

References [179] and [180] presented a vibration-based lightweight key exchange protocol and ultra-low battery resilient mechanism between external and wearable devices. The external device produces a 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 demodulation mechanism to encrypt 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

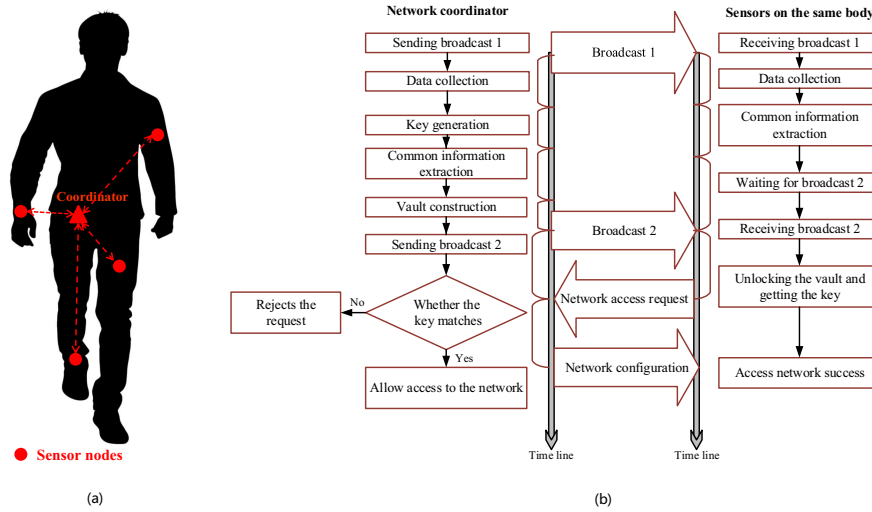


Figure 8. Overview of lightweight noise-based group key generation method using gait features in [182]. (a) Overview of proposed wearable sensor network; (b) overview of network access process

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 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 a 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 the 30s of ECG/PPG signals are required to generate 128-bit EIs in such solutions [183]. Authors in [173] proposed lightweight and resource-efficient biometrics-based security solutions, especially aiming at the energy-constrained BSNs. 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 a 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, 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 [184]. On this basis, three corresponding two-factor anonymous authentication protocols are proposed, which adopt a 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

The data transmission in an IoMT environment occurs via wireless networks, especially in WSNs. However, the wireless network is vulnerable to eavesdropping, interference, forgery, and other threats. Traditional network security mechanisms require complex interaction protocol design and additional bandwidth resources. In this case, a new mechanism to realize communication security emerges using physical layer signals of a wireless network. The physical layer security mechanism utilizes the characteristics of physical channels, such as time variability and mutuality, and offers the advantages of low energy consumption, high security, and low computational complexity.

Currently, with 5G communications, technologies such as multiple-input multiple-output and orthogonal frequency division multiplexing are conducive to constructing a physical layer security scheme [186]. The physical layer security is derived from information theory security, and this research focuses on identity authentication, channel coding, shared keys, and multiparty computation, among other related aspects. Wyner [187] first reported that secure message transmission can be realized by designing appropriate codes in insecure channels, which was the first proposal of the concept of secure coding. Against unauthorized users, a cooperative strategy is proposed in [188] with the interaction of a helper based on the wiretap channel capacity. Thereafter, Maurer [189] first proposed the use of channels to achieve key generation and distribution. In [190], the information theory method is used to generate and distribute secure keys, which were extracted and generated from communication channels. The random character of the wireless channel is used to independently generate a secure key through multipath [191, 192].

Wireless signal characteristics are utilized to secure the IoMT systems by generating keys without prior connections. Radio signal strength (RSS) is one of these characteristics that measure the received signal power, which varies with its transmission medium. Implantable medical devices can be excellent candidates for this technique, specifically, because the RSS value variation inside the human body varies from that outside the body [193]. The proposed technique utilizes the randomness in RSS values to generate a shared key that can be used to secure the communication between a headless cardiac pacemaker and a subcutaneous (under-the-skin) implant without knowing the keys. In this technique, two bits can be extracted from a single cardiac cycle (a beat) using a 128-bit key in 60s, considering the average human heart rate of 64 beats per minute (bpm).

4.3.2 Access control and data authorization

By restricting access to key resources, unauthorized users can be prevented from intruding or damaging the access to systems and data. Accordingly, network resources can be legally used. A role-based access control strategy has been proposed in which various roles are endowed with distinct access control permissions. From the perspective of the spatial-temporal relevance of data, Ray *et al.* [194] introduced the policy of location information grounding on role-based access control (RBAC). Herein, the user location determines whether it has the right to data access. The scale-based space-time RBAC model proposed by Zhang *et al.* [195] enhances the expressiveness of access control policies as well as the security of the model. In addition, 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 considers all dimensional attributes to achieve fine-grained access control. Based on ciphertext attribute encryption, researchers in [197] proposed a method that formalizes public and private keys into permissions and implements 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 stored in the cloud. Specifically, hierarchical access control has been employed to facilitate hierarchical access to privacy-sensitive data of patients. A representative approach utilizes a hierarchical role-based model to provide authorization based on the user's role [199]. For instance, all authenticated nurses can administer medicines but only personnel authenticated as a doctor can prescribe a new medication. The model supports a relatively low complex hierarchical security scheme that encrypts the patients' data and decrypts only the part of the data that are under the user's authority.

According to the system, architecture explained in Section 2, the data from sensor-based end-user networks are mostly uploaded to cloud servers through gateway nodes (*e.g.*, mobile phones, and tablets). In [200], authors reported that data security and privacy cannot be easily ensured for mobile networks

and cloud computing. Homomorphic encryption (HE) preserves data confidentiality and permits limited mathematical operations on encrypted data. This technique protects the patient's data privacy and stores them as ciphertext in the cloud layer for mathematical operations such as those for ensuring data integrity. However, it differs from other techniques that allow only the patient to review their own data but not the professionals, except in emergency scenarios. Thus, this is the application for certain IoMT sensors such as a smartwatch that allows the encryption of data at all instances and is only observed by the patient, except in case of emergency, during which the patient's data can be forwarded to professionals for diagnosis. Overall, HE can be conducted through three distinct schemes: (1) partial HE (PHE); (2) somewhat HE (SHE); (3) fully HE (FHE). In particular, PHE supports only one mathematical operation for an unlimited number of times, whereas SHE supports only a limited number of operations. In contrast, FHE supports an unlimited number of operations, and therefore, is suitable for the rapid aggregation of data without compromising data confidentiality [201]. Thus, FHE is ideal for healthcare monitoring systems in hospitals. Optimal HE is a modification of the FHE, and it differs from FHE as it is based on the step-size firefly optimization algorithm, which selects the key with the maximum breaking time [202]. This technique reduces the computation period and increases the breaking time by 2%–8% compared to other HE and non-HE techniques.

4.3.3 Privacy protection

During communications via IoMT networks, especially via wireless networks, each interaction of the users inevitably generates a considerable amount of personal data, which can be easily attacked by malicious attackers during the data-sharing process, thereby posing a severe threat to privacy. From the aspect of data communication, this technology is classified into two categories, as described below.

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

To conclude this section, a brief summary of network tier security is listed in Table 4. We predominantly focused on the connectivity between the sensing tier and the cloud infrastructure tier, where widespread technologies of authenticated visiting, encrypted data sharing, and reliable system maintenance were explained from the perspective of IoMT applications to provide a comprehensive understanding. In general, the majority of security solutions for existing network systems are applicable to IoMT systems as well. Although the application scenarios should not involve excessive alterations to the devices/servers of IoMT systems, novel technologies are required to adapt to specific IoMT applications. For authentication and key generation at the personal server level, biometrics can be applied in IoMT systems, because biometrics data can be easily sourced from medical and healthcare devices attached to or implanted in the human body. Combined with the unique strength of biometrics, these technologies can offer significant advantages to IoMT systems. Moreover, secure yet lightweight schemes should be designed to produce a diverse range of devices with restricted access. However, the limited capabilities of existing solutions compromise their security performance.

Table 4. IoMT network security taxonomy of state-of-the-art

Security issues		Compromised features	Mitigation	Representative solutions
Authentication	Unauthorized users, Eavesdropping	Authenticity, Confidentiality, Privacy	User Identity authentication	[103–131]
	Spoofing, Impersonation		Device authentication	[132–155]
	Insecure APIs		Cloud authentication	[156–161]
Key management	Information leakage, Sniffing, Eavesdropping	Confidentiality, Privacy, Integrity, Availability	Cryptographic algorithms	[162–166]
	Tampering, Relay, Replay		Biometrics-based key management	[167–176]
	Resource depletion		Lightweight encryption and key management	[173, 178–185]
Other relevant technologies	Unauthorized users, Eavesdropping	Confidentiality, Privacy, Anonymity	Physical layer security	[186–193]
	Relay, Replay		Access control and data authorization	[27, 194–201]
	Interruption		Privacy protection	[203–206]

5 State-of-the-art cloud security for IoMT applications

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

5.1 Hardware security

The hardware-related security issues that support the physical environment of the Cloud are discussed herein along with the potential solutions.

5.1.1 Natural disasters

A natural disaster occurs due to geographical location and seasonal climate. The hardware in cloud data centers can be exposed to disasters (extreme weather), *e.g.*, thunderstorms, floods, and earthquakes, all of which can influence the availability of the cloud infrastructure and the services operating on it. In 2016, Amazon's cloud data center located in Sydney experienced a power outage, rendering various bank cards of numerous users temporarily useless¹. The eHealth system that manages the medical data can encounter this problem in the occurrence of a disaster. Therefore, the locations of cloud data centers should be carefully selected to avoid the natural influence [207], and accordingly, disaster recovery solutions should be formulated [208].

5.1.2 Hardware functional safety

This kind of safety issue is associated with the functionalities of hardware, ranging from switches to physical servers in cloud data centers, which can deteriorate the functionality of the cloud services and render

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

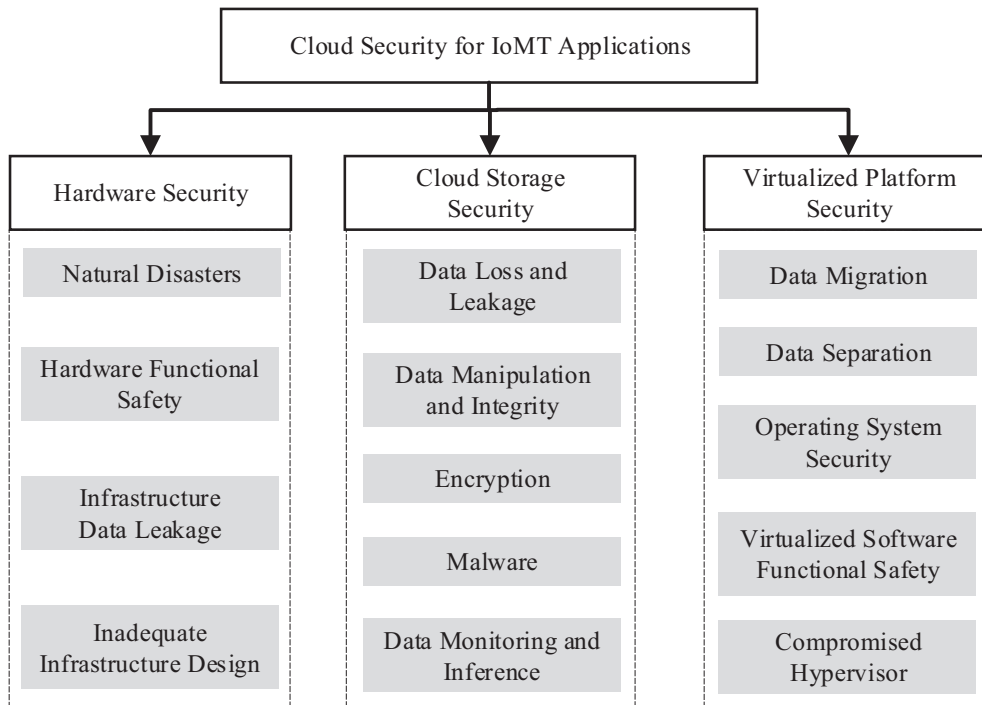


Figure 9. Classification of cloud security for IoMT applications

them inaccessible [209, 210]. The US cloud storage supplier, Swissdisk, suffered from an unplanned and unpredictable catastrophic hardware failure that disavowed users from accessing their data. Thereafter, the company decided to invest considerable resources to enhance a state-of-the-art platform. Resource replication and erasure coding are prevalent approaches that ensure hardware availability [211]. However, these approaches involve certain trade-offs in terms of durability, network bandwidth, energy consumption, and recovery performance. To avoid the issues of hardware functional safety, the hardware development process should be adapted to the requirements of certain 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 leakage of key administration information to malicious users, which can result in the misuse of cloud resources. Digital currency mining, email spam, and phishing attempts are certain representative examples. Unfavorably, cloud providers bear an immense loss if the attacker can directly access hardware resources. For instance, an attacker exploits the leaked data to obtain all privileges of the cloud resources and launches a set of power VMs to execute currency mining tasks, which consume considerable resources and electric power. Kiara *et al.* [212] proposed an 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 IoT, which includes transmission protection, storage protection, and access control based on various encryption schemes.

5.1.4 Inadequate infrastructure design

This issue is caused if the cloud provider fails to notice the potential surges in the number of users, which causes insufficient provisioning of resources for the applications. For instance, enormous traffic arrives at a single point of the critical physical node, resulting in unacceptable delays and SLA violations. The Sina Weibo application can fulfill the surge in requests caused by trending topics [214], which can occur in IoMT applications as well if numerous users are accessing the same application. To address this issue, property

resource scheduling policies should be designed, such as autoscaling 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

The security issues related to cloud storage and the promising solutions addressing the corresponding issues are discussed herein.

5.2.1 Data loss and leakage

Intrusion action or disk corruption can cause data loss and leakage in cloud storage without redundancy. This serious security issue can significantly impact privacy and trust in addition to affecting the service-level agreements 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 the data stored in the cloud. Kaur *et al.* [217] have discussed certain existing approaches to protect against data leakage, which include techniques such as local scanning of data and remote scanning. The agents installed on the devices will conduct the regular examination to avoid data loss and leakage.

5.2.2 Data manipulation and integrity

A malicious attacker with privileged access to cloud infrastructure can employ a variety of techniques to achieve their objectives. To manipulate the data in cloud storage, an attacker with complete control over the data blocks can read, insert, modify, and even corrupt the data in cloud storage. Full control over storage enables an attacker to injure the confidentiality, integrity, and availability of customer data. Consequently, this type 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. Considering the advantages of traceable and tamper-resistant features of blockchain, any entity with an illegal manipulation of data will be held accountable for the evidence. Manipulation can hurt data integrity which refers to the integrity of customer data. However, in the cloud computing environment, users can access their data stored in the cloud in a distributed manner, which can suffer from the consistency issue under the security property. Although cloud applications rely on the assurance of cloud service providers to a certain extent, the vulnerabilities can be secured by incomplete security examinations such as the errors caused by the global clock. Pandey *et al.* [219] investigated data integrity techniques in the medical domain, which can leverage blockchain-based approaches [220] and masked authenticated messaging [221].

5.2.3 Encryption

Cloud environments should ensure the secrecy of sensitive data while providing normal utilization of data. In this regard, encryption is the essential mechanism that ensures data confidentiality through protection, communication, and certain activities against malicious users aiming to disrupt the normal operation of the cloud. A significant amount of work has been investigated to achieve confidentiality while targeting other properties such as integrity, availability, authenticity, and privacy [222]. Cryptographic techniques based on attribute-based encryption aim to provide privacy and fine-grained access control, including proxy re-encryption, revocation mechanism, and hierarchical attribute-based encryption [223–226].

5.2.4 Malware

Malware refers to malicious programs injected into cloud storage, which can join the host into a zombie network and continuously add new hosts to the network. The hosts can be either physical machines or VMs in the cloud environment. As reported, half of the downloaded malware can disable local security in one minute. As such, threats combining new techniques with traditional evasive attacks can damage

security, which is referred to as malware-as-a-service. A significant amount of effort has been devoted to efficiently detecting malware [227]. For instance, Watson *et al.* [228] proposed an online anomaly detection approach based on a support vector machine with high detection accuracy. This approach can 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 data manipulation, a malicious attacker can observe and analyze the access pattern of users to predict the user data stored in the cloud, which is called data monitoring and inference. The standard encryption approach fails to appropriately conceal the access pattern. Therefore, with this kind of attack, the attackers can compromise the confidentiality of the cloud customers' data. Inference represents the data mining approach to explore the data hidden behind common users. In a cloud storage scenario, data inference indicts the database system technique to injure the databases. The attackers aim to infer sensitive data from the databases with a high-level perspective that can compromise the entire database. If inference problems are not addressed, the sensitive information may be exposed to external users. To ensure efficient and fine-grained access to electronic health records, Zhang *et al.* [230] proposed a multiphase access policy to achieve an inference attack-resistant system. Each data attribute in records is individually encrypted, and the Cloud will execute the computation-intensive data without prior knowledge of the sensitive data. Ma *et al.* [231] proposed an inference-aware mechanism in multitask learning, which can resist the inference attack through immediate results. Deznabi *et al.* [232] analyzed 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

The security issues related to the virtualized platform that provides physical or virtual resources to support the execution of IoMT applications are discussed herein, including the corresponding solutions.

5.3.1 Data migration

In a traditional cloud computing environment, VM live migration is a significant feature that shifts a VM from one place to another to optimize resource usage. The cloud-native applications that shift the monolithic applications into lightweight applications can migrate/reschedule containers developed via microservice architecture from one physical host to another. However, security problems can be triggered during the migration process. For instance, the data is not completely transferred and yields consistency problems, which can be attacked by malicious users to conduct useless migration and consume resources that diminish 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. Subsequently, they proposed an enhanced model based on the existing protocols with demonstrated security assessments.

5.3.2 Data separation

The Cloud supports multitenant scenarios by sharing resources for multiple users. To utilize the benefits of the cloud, users need to migrate their data to the cloud. However, certain users avoid migrating sensitive data to public cloud networks, which necessitates data separation [235]. In principle, data separation aims to ensure that the data are well-partitioned, *i.e.*, the user can access the data in his/her own domain but not in other domains. However, during the data separation process, sensitive information can be leaked, which poses high risks. If the data is separated in physical devices, the data can have loss or disclosure because the data is not completely formatted or used by other tenants, which can increase the costs. Moreover, the complexity of managing the security of data separation increases because of the geolocation feature of data. A significant amount of recent research has contributed to the area of mobile edge/cloud computing area, which can efficiently address this issue. For instance, Wu *et al.* [236, 237] proposed data separation approaches based on neural networks to transfer data between cloud and mobile devices. In this manner, sensitive data can be locally managed.

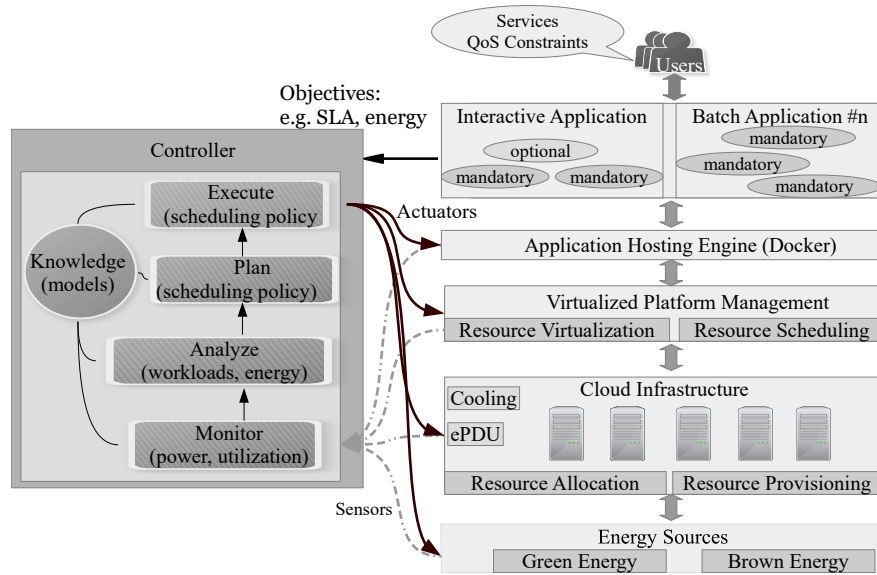


Figure 10. A prototype system that manages virtual machines and containers in [239]

5.3.3 Operating system security

Owing to the heterogeneous nature of cloud computing, various kinds of OSs working together can create a set of security issues. For instance, vulnerabilities exist widely in preventing the normal functioning of OSs such as Windows, Linux, and iOS. These operating systems need to frequently update or patched to solve security problems. In the desktop OS, the remote code execution vulnerability bug permits the unauthenticated remote attacker to execute codes by sending network packets and presuming control over the OS. In the mobile OS, the increasing popularity of smartphones can attract more attacks, and the common issues include insecure data storage and broken cryptography. In 2015, the iPhone OS reported a severity issue that allowed the attacker to execute codes in the privilege mode or cause DoS attacks². Xu *et al.* [238] proposed a virtualized education platform that provides an environment to perform private experiments. The proposed platform is based on a software-defined network to secure access via OpenVPN. In practice, most vulnerabilities are solved by commercial enterprises and open-source communities.

5.3.4 Virtualized software functional safety

Cloud services enable 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 depicted in Figure 10. However, the threat is that the shared image can be used to trick victims by using malicious functions to harvest the sensitive data stored in the images (*e.g.*, default user names and passwords stored in property files) [241]. Therefore, this kind of attack can influence both 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. To ensure the security of a container image, Fotis *et al.* [243] introduced a mechanism to protect the 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 anomalous behaviors.

5.3.5 Compromised hypervisor

The compromised hypervisor represents the threat in which the attacker aims to control the hypervisor isolating the cloud users and the virtualized environment [245], such as VMs or containers. These types of security issues can significantly impact system security by stealing the visibility permission of users'

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

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	[207, 208]
	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]

data and resources and even manipulating the users' data. By controlling the hypervisor, the attacker can cause severe damage by leveraging the capability of VMs and containers. Therefore, confidentiality, integrity, and availability can be undermined after gaining partial or complete control of the hypervisor.

Lin *et al.* [246] proposed a VM protection approach for compromised hypervisors based on privilege level execution, which can create effective VM isolation and data-driven VM monitoring to reveal the user-sensitive information stored in VMs. This approach is advantageous because it is independent of platforms and can be widely applied to multiple cloud providers. Li *et al.* proposed Hypes [247] to retrofit a commodity hypervisor by leveraging the microkernel principles that protect the confidentiality and integrity of VMs, which partitions the hypervisor into an untrusted host that is only responsible to perform the functionalities without handling sensitive data. Although sensitive data can be accessed by trusted cores, this approach is limited because of the additional costs required in its implementation. 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 the hypervisor. This approach is advantageous because it does not depend on a higher privilege than the hypervisor. The container-based security of the hypervisor has garnered scholarly attention, following the trend to shift the virtualized environment based on VMs into containers. Khalimov *et al.* [249] have explored the use of container-based environments as an alternative to the hypervisor-based sandbox for security analysis.

In conclusion, the cloud security of IoMT systems has attracted scholarly attention from a wide range of perspectives. To elucidate, the Cloud security issues, compromised features, mitigation, and corresponding solutions are summarized in Table 5. Note that the security approaches for hardware, cloud storage, and virtualized platforms have been standardized across the cloud layer comprising well-known security techniques such as resource replication, masked authenticated messaging, admission control, and transmission protections applied to common scenarios. Furthermore, we determined a set of security mechanisms for new threats unique to cloud security, such as malicious VM images and cloud-side encryption for authorization, authentication, and confidentiality methods, which indicates future research directions. In addition, we highlight the emerging problems unresolved by current solutions, such as identification and management of malicious container images for IoMT services in a cloud-native environment.

6 Challenges and research directions

Although this review explored the security issues in IoMT applications, supported networks, and cloud infrastructure from a diverse perspective, the research gaps and challenges have only been partially addressed. These challenges are summarized below.

- *Identification of Malicious Container Images.* The cloud-native environment has been regarded as the new generation of cloud computing and has shifted monolithic applications into lightweight 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 regarding the security issues in the container-based environment, and the identification of malicious container images is still a challenge for the cloud-based scenario that supports IoMT services.

- *Regulations and Licensing.* With the integration of IoMT devices into comprehensive medical facilities, adherence to compliance regulations, and security of licensing approvals are mandatory. The majority of devices aimed at acquiring, transmitting, or analyzing information are subjected to compliance regulations and licensing approvals. Although manufacturing these devices is a time-consuming process, it is not the only challenge experienced by healthcare service providers employing IoMT. Regulatory compliance is a considerable hurdle that must be successfully addressed, and in the future, neglecting this challenge can increase the overall risks and legal costs.
- *Tradeoff between Interoperability and Data Security.* A crucial challenge is caused by the dearth of systems that collate and utilize the massive amounts of data collected from medical devices. In healthcare, various departments often operate in silos and may not efficiently communicate with each other. To garner critical insights from the generated data, the installed systems should interact with each other. The integration of IoMT systems can yield extensive medical interoperability among crucial devices in the systems. However, the data related to patient health and information contain inpatient databases such as credit card details, addresses, and email IDs, which are highly demanded by hackers. Thus, IoMT devices are fundamentally designed from a utilitarian perspective and frequently employ legacy software that is not equipped with in-built data security features. Consequently, with the extension of data interoperability, certain vulnerabilities prevail in the devices and across various healthcare departments in the hospital.
- *Long-term and System-wide Comprehensive Security.* From the system perspective, integrated security involves multiple elements, agents, levels, and links, with significant complexity (including high dimensionality, multiscale, nonlinear, openness, integrity, interaction, coupling, interactivity, and dynamics). Integrated security has emerged as one of the key research directions and tasks in the field of safety science, which constitutes one of the major challenges of safety science in the 21st century. To mitigate the security challenges caused by integrated security problems, security researchers should update their research concepts, develop research ideas, focus on strengthening the scientific research on complex security, and conduct long-term and system-wide comprehensive security research on complex giant systems (including human beings and human activities).

The opportunities and future directions of research are presented as follows:

- *Firmware Upgrades.* IoMT devices must be regularly monitored and patched with critical firmware upgrades that optimize the performance of the firmware or device drivers to potentially improve the performance of processors and related device hardware. These updates eliminate 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. The integration of 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 impacted. The real-time health checks of device software, correlation, and forensic analysis of all security data and event feed aid in preventing attacks and automating incident response playbooks.
- *Segmenting Security.* The vast majority of device-to-device communications are superfluous. Overall, security through segmentation forms one of the best practices. Upon creating a separation between patient data and the remainder of the IT network, cyber security experts can understand network traffic and improve anomaly detection. Consequently, deeper insights can be obtained into atypical traffic patterns or movements implying the presence of an intruder or a cyber infection.
- *Blockchain-based Techniques.* The current approaches to security assurance preventing the data manipulation of cloud services and cloud storage (e.g., medical data) are 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. Moreover, the data in the IoMT scenarios can be secured with further developments in blockchain technology.
- *Microservice-based Applications.* Although a significant amount of effort has been devoted to ensuring the security of traditional applications, an increasing number of applications have been shifted from monolithic applications into microservice-based applications. The security issues in the virtualized environment of the microservice platform, such as container image security and data

isolation between containers, have not been comprehensively investigated, and thus, require focused attention.

- *Data Management with Federated Learning.* The data management between the user's local device and remote cloud servers is a challenging task because partitioning the data to ensure user privacy and data processing efficiency is difficult. Federated learning is regarded as a promising paradigm that locally retains the sensitive data and outsources the insensitive data to the cloud, *e.g.*, the personal data of patients can be processed using local devices and general information can be trained by the AI models in the cloud. The distributed data can coordinate to fulfill the requirements of medical-oriented tasks.
- *Research Direction of Integrated Security.* The integration security problem can be resolved by performing certain 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 modifications of the system; (5) prevention and resolution of systemic security risks; (6) emergence of system security risks.

7 Conclusion

IoMT is essential for precision health as it improves the timeliness and quality of care while reducing the complexities and costs of patient care, especially in the management of a pandemic crisis. As data security and prediction accuracy have been the primary concerns in this area, the related security issues should be treated with concern, thereby highlighting their significance to develop and implement successful security strategies in IoMT systems. This paper presents a comprehensive review of research on IoMT systems, focusing on the corresponding security and privacy problems. This paper projects an overview of IoMT systems from the aspect of hierarchical system architecture and details the assessment of the security metrics conducted based on the performance demands of network services. The state-of-the-art security techniques relevant to this research domain have been discussed with respect to the potential security risks. The security issues and solutions for the sensing layer, network layer, and cloud infrastructure layer in IoMT systems were explained and analyzed to ensure their compliance with the system architecture and performance demands of various network services. Specifically, the significance and uniqueness of biometrics-based technologies are potentially the most beneficial approach for the authentication and key management of IoMT systems, which were detailed including the future research directions for further improvement. The current challenges and future research directions revealed the immense potential of 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 the network layer; Minxian Xu carried out the review of the cloud infrastructure layer, and participated in manuscript preparation; Qimeng Li carried out the review of the 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] Gambhir SS, Ge TJ and Vermesh O et al. Toward achieving precision health. *Sci Transl Med* 2018; **10**: eaao3612.
- [3] Vermeesch JR, Voet T and Devriendt K. Prenatal and pre-implantation genetic diagnosis. *Nat Rev Genet* 2016; **17**: 643–56.
- [4] Pathinarupothi RK, Durga P and Rangan ES, IoT-based smart edge for global health: remote monitoring with severity detection and alerts transmission. *IEEE Internet Things J* 2019; **6**: 2449–462.
- [5] Satija U, Ramkumar B and Manikandan MS. Real-time signal quality-aware ECG telemetry system for IoT-based health care monitoring. *IEEE Internet Things J* 2017; **4**: 815–23.
- [6] Yang Z, Zhou Q and Lei L et al. An IoT-cloud based wearable ECG monitoring system for smart healthcare. *J Med Syst* 2016; **40**: 1–11.
- [7] Catarinucci L, de Donno D and Mainetti L et al. An IoT-aware architecture for smart healthcare systems. *IEEE Internet Things J* 2015; **2**: 515–26.
- [8] Castillejo P, Martinez JF and Rodriguez-Molina J et al. Integration of wearable devices in a wireless sensor network for an E-health application. *IEEE Wireless Commun* 2013; **20**: 38–49.
- [9] Qadri YA, Nauman A and Zikria YB et al. The future of healthcare Internet of Things: a survey of emerging technologies. *IEEE Commun Surv Tutor* 2020; **22**: 1121–67.
- [10] Masud M, Gaba GS and Alqahtani S et al. A lightweight and robust secure key establishment protocol for Internet of Medical Things in covid-19 patients care. *IEEE Internet Things J* 2021; **8**: 15694–703.
- [11] Lin H, Garg S and Hu J et al. Privacy-enhanced data fusion for covid-19 applications in intelligent Internet of Medical Things. *IEEE Internet Things J* 2021; **8**: 15683–693.
- [12] Yang T, Gentile M and Shen CF et al. Combining point-of-care diagnostics and Internet of Medical Things (IoMT) to combat the covid-19 pandemic. *Diagnostics* 2020; **10**: 224–6.
- [13] Liu J, Miao F and Yin L et al. A noncontact ballistocardiography-based iomt system for cardiopulmonary health monitoring of discharged covid-19 patients. *IEEE Internet Things J* 2021; **8**: 15807–17.
- [14] Firouzi F, Rahmani AM and Mankodiya K et al. Internet-of-Things and big data for smarter healthcare: from device to architecture applications and analytics. *Future Gener Comput Syst* 2018; **78**: 583–86.
- [15] Joyia J, Liaqat RM and Farooq A et al. Internet of medical things (IoMT): applications benefits and future challenges in healthcare domain. *J Commun* 2017; **12**: 240–47.
- [16] Jara AJ, Zamora-Izquierdo MA and Skarmeta AF. Interconnection framework for mHealth and remote monitoring based on the Internet of Things. *IEEE J Sel Areas Commun* 2013; **31**: 47–65.
- [17] Verma P and Sood SK. Fog assisted-IoT enabled patient health monitoring in smart homes. *IEEE Internet Things J* 2018; **5**: 1789–96.
- [18] Redondi A, Chirico M and Borsani L et al. An integrated system based on wireless sensor networks for patient monitoring localization and tracking. *Ad Hoc Netw* 2013; **11**: 39–53.
- [19] Fan Y, Yin Y and Xu L et al. IoT-based smart rehabilitation system. *IEEE Trans Ind Inform* 2014; **10**: 1568–77.
- [20] Occhiuzzi C, Vallese C and Amendola S et al. NIGHT-care: a passive RFID system for remote monitoring and control of overnight living environment. *Proc Comput Sci* 2014; **32**: 190–7.
- [21] Liu L, Stroulia E and Nikolaidis I et al. Smart homes and home health monitoring technologies for older adults: a systematic review. *Int J Med Inform* 2016; **91**: 44–59.
- [22] Pasluosta CF, Gassner H and Winkler J et al. An emerging era in the management of Parkinson's disease: wearable technologies and the Internet of Things. *IEEE J Biomed Health Inform* 2015; **19**: 1873–81.
- [23] Yang G, Xie L and Mäntysalo M et al. A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. *IEEE Trans Ind Inform* 2014; **10**: 2180–91.
- [24] Cynerio. Health it security, 2022. <https://healthitsecurity.com/news/53-of-connected-medical-devices-contain-critical-vulnerabilities>.
- [25] He D, Ye R and Chan S et al. Privacy in the Internet of Things for smart healthcare. *IEEE Commun Mag* 2018; **56**: 38–44.
- [26] Masud M, Gaba GS and Choudhary K et al. Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. *IEEE Internet Things J* 2022; **9**: 2649–56.
- [27] Kumar M and Chand S. A secure and efficient cloud-centric Internet-of-medical-things-enabled smart healthcare system with public verifiability. *IEEE Internet Things J* 2020; **17**: 10650–59.
- [28] Stergiou CL and Gupta KEPBB. IoT-based big data secure management in the fog over a 6G wireless network. *IEEE Internet Things J* 2021; **8**: 5164–71.
- [29] Lopes APG and Gondim PRL. Mutual authentication protocol for D2D communications in a cloud-based E-health system. *Sensors* 2020; **20**: 2072–95.
- [30] Deebak BD and Al-Turjman F. Smart mutual authentication protocol for cloud based medical healthcare systems using Internet of medical things. *IEEE J Sel Areas Commun* 2021; **39**: 346–60.
- [31] Cao R, Tang Z and Liu C et al. A scalable multicloud storage architecture for cloud-supported medical Internet of Things. *IEEE Internet Things J* 2020; **7**: 1641–54.
- [32] Ning Z, Dong P and Wang X et al. Mobile edge computing enabled 5G health monitoring for Internet of medical things: a decentralized game theoretic approach. *IEEE J Sel Areas Commun* 2021; **39**: 463–78.
- [33] Ghubaish A, Salman T and Zolanvari M et al. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet Things J* 2020; **8**: 8707–18.
- [34] Koutras D, Stergiopoulos G and Dasaklis T et al. Security in IoMT communications: a survey. *Sensors* 2020; **20**: 4828.
- [35] Hatzivasilis G, Soultatos O and Ioannidis S et al. Review of security and privacy for the Internet of Medical Things (IoMT). In: 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS). IEEE, 2019, 457–64.

- [36] Hathaliya JJ and Tanwar S. An exhaustive survey on security and privacy issues in healthcare 4.0. *Comput Commun* 2020; **153**: 311–35.
- [37] Newaz AI, Sikder AK and Rahman MA et al. A survey on security and privacy issues in modern healthcare systems: attacks and defenses. *ACM Trans Comput Healthcare* 2021; **2**: 1–44.
- [38] Yaqoob T, Abbas H and Atiquzzaman M. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices – a review. *IEEE Commun Surv Tutor* 2019; **21**: 3723–768.
- [39] Smith D and Simpson K. *Functional Safety*, Routledge, 2004.
- [40] Wu J. Development paradigms of cyberspace endogenous safety and security. *Sci China Inform Sci* 2022; **65**: 1–3.
- [41] Wu J. *Cyberspace endogenous safety and security*. Engineering 2021.
- [42] Fatema N and Brad R. Security requirements, counterattacks and projects in healthcare applications using WSNs – a review. *Int J Comput Netw Commun* 2014; **2**: 1–9.
- [43] Clausen E, Schiefer M and Lösche U. Tech. rep., Independent IT-Security Institute 2015.
- [44] Cao X, Shila DM and Cheng Y et al. Ghost-in-ZigBee: Energy depletion attack on zigbee-based wireless networks. *IEEE Internet Things J* 2016; **3**: 816–29.
- [45] Gill SS, Xu M and Ottaviani C et al. AI for next generation computing: emerging trends and future directions. *Internet Things* 2022; **19**: 100514.
- [46] Sun W, Cai Z and Li Y et al. Security and privacy in the medical internet of things: a review. *Secur Commun Netw* 2018; **2018**: 1–9.
- [47] Kasyoka P, Kimwele M and Angolo SM. Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. *J Med Eng Technol* 2020; **44**: 12–9.
- [48] Bromwich M and Bromwich R. Privacy risks when using mobile devices in health care, *Can Med Assoc J* 2016; **188**: 855–56.
- [49] Raposo VL. Electronic health records: is it a risk worth taking in healthcare delivery?. *GMS Health Technol Assess* 2015; **11**: 1–9.
- [50] Mooney G. Is HIPAA compliant with the GDPR?, 2018. <https://blog.ipswitch.com/is-hipaa-compliant-with-the-gdpr>.
- [51] Pearlman S. What is data integrity and why is it important?, 2019. <https://www.talend.com/resources/what-is-data-integrity/>.
- [52] Bienkowski T. GDPR is explicit about protecting availability, 2018. <https://www.netscout.com/blog/gdpr-availability-protection>.
- [53] Crilly P and Muthukkumarasamy V, 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*, 2010, 291–296.
- [54] Kogetsu A, Ogishima S and Kato K et al. 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. *Front Genet* 2018; **9**: 1–6.
- [55] Kambourakis G, Anonymity and closely related terms in the cyberspace: an analysis by example. *J Inform Secur Appl* 2014; **19**: 2–17.
- [56] Medical devices, 2022. <https://www.who.int/health-topics/medical-devices#tab=tab.1>.
- [57] Ray V, Freud applications of fib: invasive fib attacks and countermeasures in hardware security devices. In: *East-Coast Focused Ion Beam User Group Meeting*, 2009.
- [58] Tarnovsky C, Security failures in secure devices. *Black Hat DC Presentation* 2008; **74**.
- [59] Shi Q, Asadizanjani N and Forte D et al. A layout-driven framework to assess vulnerability of ICs to microprobing attacks. In: *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2016, 155–60.
- [60] Quadir SE, Chen J and Forte D et al. A survey on chip to system reverse engineering. *ACM J Emerging Technol Comput Syst (JETC)* 2016; **13**: 1–34.
- [61] Botero UJ, Wilson R and Lu H et al. 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] Sidorkin V, van Veldhoven E and van der Drift et al. Sub-10-nm nanolithography with a scanning helium beam. *J Vacuum Sci Technol B: Microelectron Nanometer Struct Process Meas Phenom* 2009; **27**: L18–20.
- [63] Fyrbiak M, Wallat S and Swierczynski P et al. HALthe missing piece of the puzzle for hardware reverse engineering, trojan detection and insertion. *IEEE Trans Dependable Secure Comput* 2018; **16**: 498–510.
- [64] Costin A, Zaddach J and Francillon A et al. A {Large-scale} analysis of the security of embedded firmwares. In: *23rd USENIX Security Symposium (USENIX Security 14)*, 2014, 95–110.
- [65] Ben Yehuda R and Zaidenberg NJ. Protection against reverse engineering in ARM. *Int J Inform Secur* 2020; **19**: 39–51.
- [66] Vosoughi A and Köse S. Leveraging On-Chip Voltage Regulators Against Fault Injection Attacks. In: *Proceedings of the 2019 on Great Lakes Symposium on VLSI, GLSVLSI '19*. New York, NY, USA: Association for Computing Machinery, 2019, 15–20. <https://doi.org/10.1145/3299874.3317978>.
- [67] Nechvatal J, Barker E and Bassham L et al. Report on the development of the advanced encryption standard (AES). *J Res Nat Inst Stand Technol* 2001; **106**: 511–77.
- [68] Tehranipoor M and Koushanfar F. A survey of hardware trojan taxonomy and detection. *IEEE Des Test Comput* 2010; **27**: 10–25.
- [69] Wehbe T, Mooney VJ and Javaid AQ et al. 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)*. IEEE, 2017, 106–09.

- [70] Jordaney R, Sharad K and Dash SK et al. Transcend: Detecting concept drift in malware classification models. In: 26th USENIX Security Symposium (USENIX Security 17), 2017, 625–642.
- [71] Cai H, Meng N and Ryder B et al. Droidcat: Effective android malware detection and categorization via app-level profiling. *IEEE Trans Inform Forensics Secur* 2019; **14**: 1455–70.
- [72] Lei T, Qin Z and Wang Z et al. Evedroid: Event-aware android malware detection against model degrading for IoT devices. *IEEE Internet Things J* 2019; **6**: 6668–80.
- [73] Aman MN, Chua KC and Sikdar B. In: *Cryptographic Security Solutions for the Internet of Things*, IGI Global, 2019, 117–41.
- [74] Qureshi MA and Munir A. PUF-RAKE: a PUF-based robust and lightweight authentication and key establishment protocol. *IEEE Trans Dependable Secure Comput* 2021; **19**: 2457–75.
- [75] Wang Z, Ding X and Pang C et al. To detect stack buffer overflow with polymorphic canaries. In: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). IEEE, 2018, 243–54.
- [76] Xu B, Wang W and Hao Q et al. A security design for the detecting of buffer overflow attacks in IoT device. *IEEE Access* 2018; **6**: 72862–869.
- [77] Shila DM, Geng P and Lovett T et al. I can detect you: Using intrusion checkers to resist malicious firmware attacks. In: 2016 IEEE Symposium on Technologies for Homeland Security (HST), 2016, 1–6.
- [78] Hanna S, Rolles R and Molina-Markham A et al. Take Two Software Updates and See Me in the Morning: the Case for Software Security Evaluations of Medical Devices. In: *HealthSec*, Citeseer, 2011.
- [79] Aviv A, Černý P and Clark S et al. Security Evaluation of ES&S Voting Machines and Election Management System. In: *Proceedings of 2008 USENIX/ACCURATE Electronic Voting Workshop (EVT 2008)*, 2008, 1–13.
- [80] Cui A and Stolfo SJ. 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*, 2010, 97–106.
- [81] Sutton M. *Corporate Espionage for Dummies: The Hidden Threat of Embedded Web Servers*, Black Hat USA, 2011.
- [82] Bettayeb M, Nasir Q and Talib MA. Firmware update attacks and security for IoT devices: survey. In: *Proceedings of the ArabWIC 6th Annual International Conference Research Track*, 2019, 1–6.
- [83] Ling Z, Luo J and Xu Y et al. Security vulnerabilities of internet of things: a case study of the smart plug system. *IEEE Internet Things J* 2017; **4**: 1899–909.
- [84] One A. Smashing the stack for fun and profit. *Phrack Mag* 1996; **7**: 14–6.
- [85] Shacham H. 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*, 2007, 552–61.
- [86] Mohanty A, Obaidat I and Yilmaz F et al. 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] Burow N, Carr SA and Nash J et al. Control-flow integrity: Precision, security, and performance. *ACM Comput Surv* 2017; **50**: 1–33.
- [88] Jin Z, Chen Y and Liu T et al. 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, ICAI 2019*. New York, NY, USA: Association for Computing Machinery, 2019, 115–22.
- [89] Xia H, Woodruff J and Ainsworth S et al. CHERIvoke: characterising pointer revocation using CHERI capabilities for temporal memory safety. In: *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture, MICRO '52*. New York, NY, USA: Association for Computing Machinery, 2019, 545–557.
- [90] Karimi E, Fei Y and Kaeli D et al. Hardware/software obfuscation against timing side-channel attack on a GPU. In: 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2020, 122–31.
- [91] Song W, Li B and Xue Z et al. 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), 2021, 955–69.
- [92] Qureshi MK. New attacks and defense for encrypted-address cache. In: 2019 ACM/IEEE 46th Annual International Symposium on Computer Architecture (ISCA). IEEE, 2019, 360–71.
- [93] Werner M, Unterluggauer T and Giner L et al. {ScatterCache}: thwarting cache attacks via cache set randomization. In: 28th USENIX Security Symposium (USENIX Security 19), 2019, 675–92.
- [94] Das D, Maity S and Nasir SB et al. 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), 2017, 62–7.
- [95] Wei L, Luo B and Li Y et al. I know what you see: Power side-channel attack on convolutional neural network accelerators. In: *Proceedings of the 34th Annual Computer Security Applications Conference*, 2018, 393–406.
- [96] Delgado-Lozano IM, Tena-Sánchez E and Núñez J et al. Design and analysis of secure emerging crypto-hardware using hyperfet devices. *IEEE Trans Emerging Top Comput* 2021; **9**: 787–96.
- [97] Yang WH, Chu LC and Yang SH et al. 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). IEEE, 2018, 126–28.
- [98] Das D, Nath M and Ghosh S et al. Killing EM side-channel leakage at its source. In: 2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS), 2020, 1108–11.
- [99] Cheng P, Bagci IE and Roedig U et al. Sonarsnoop: active acoustic side-channel attacks. *Int J Inform Secur* 2020; **19**: 213–28.
- [100] de Souza Faria G and Kim HY. Differential audio analysis: a new side-channel attack on PIN pads. *Int J Inform Secur* 2019; **18**: 73–84.
- [101] Carmon E, Seifert JP and Wool A et al. Photonic side channel attacks against RSA. In: 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2017, 74–8.
- [102] Rivest RL, Shamir A and Adleman L et al. A method for obtaining digital signatures and public-key cryptosystems. *Commun ACM* 1978; **27**: 120–26.

- [103] Aravindhan K and Karthiga R. One-time password: a survey. *Int J Emerging Trends Eng Dev* 2013; **1**: 613–23.
- [104] Zhang M and Yin Q. Research progress of static password authentication technology. *J Cyberspace Secur* 2018; **9**: 11–4.
- [105] Chien HY, Ke-Jan J and Tseng YM. An efficient and practical solution to remote authentication: smart card. *Comput Secur* 2002; **21**: 372–75.
- [106] Shimizu A. A dynamic password authentication method using a one-way function. *Syst Comput Jpn* 1991; **22**: 32–40.
- [107] KumarDas A, Sharma P and Chatterjee S et al. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *J Netw Comput Appl* 2012; **35**: 1646–56.
- [108] Harn L and Ren J. Generalized digital certificate for user authentication and key establishment for secure communications. *IEEE Trans Wireless Commun* 2011; **10**: 2372–79.
- [109] Kumari A, Jangirala S and Abbasi MY et al. ESEAP: ECC-based secure and efficient mutual authentication protocol using smart card. *J Inform Secur Appl* 2020; **51**: 1–12.
- [110] Easttom C and Mei N. Mitigating implanted medical device cybersecurity risks. In: *Proceeding of IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2019, 145–48.
- [111] Ibtihel N and Hadj SM. Smart ECG monitoring through IoT In: ChinMay C (ed.), 2020.
- [112] Youssef W, Zaid AO and Mourali MS et al. RFID-based system for secure logistic management of implantable medical devices in Tunisian health centres. In: *Proceeding of IEEE International Smart Cities Conference (ISC2)*, 2019, 83–6.
- [113] Jain A, Hong L and Bolle R et al. Online fingerprint verification. *IEEE Trans Pattern Anal Mach Intell* 1997; **19**: 302–14.
- [114] Datta AK. *Advances in Fingerprint Technology*, CRC Press, 2001.
- [115] Bruce V and Young A. Understanding face recognition, *Br J Psychol* 1986; **77**: 305–27.
- [116] He X, Yan S and Hu Y et al. Face recognition using laplacianfaces. *IEEE Trans Pattern Anal Mach Intell* 2005; **27**: 328–40.
- [117] Frank M, Biedert R and Ma E et al. Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Trans Inform Forensics Secur* 2013; **8**: 136–48.
- [118] Zheng N, Bai K and Huang H et al. You are how you touch: user verification on smartphones via tapping behaviors. In: *Proceeding of the 22nd IEEE International Conference on Network Protocols*, 2014, 221–32.
- [119] Sitová Z, Šedenka J and Yang Q et al. Hmog: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Trans Inform Forensics Secur* 2016; **11**: 877–92.
- [120] Zheng G, Yang W and Johnstone M et al. Securing the elderly in cyberspace with fingerprints, *Academic*, 2020.
- [121] Zheng G, Yang W and Valli C et al. Finger-to-heart (F2H): Authentication for wireless implantable medical devices. *IEEE J Biomed Health Inform* 2019; **23**: 1546–57.
- [122] Fratini A, Sansone M and Bifulco P et al. Individual identification via electrocardiogram analysis. *Biomed Eng Online* 2015; **14**: 1–23.
- [123] Yang M, Liu B and Zhao M et al. Normalizing electrocardiograms of both healthy persons and cardiovascular disease patients for biometric authentication. *PLoS ONE* 2013; **8**: e71523.
- [124] Irvine JM and Israel SA. A sequential procedure for individual identity verification using ECG. *EURASIP J Adv Signal Process* 2009; **5**: 42–57.
- [125] Pathoumvanh S, Airphaiboon S and Hamamoto K. Robustness study of ECG biometric identification in heart rate variability conditions. *IEEE Trans Electr Electr Eng* 2014; **9**: 42–57.
- [126] Liu J, Yin L and He C et al. A multiscale autoregressive model-based electrocardiogram identification method. *IEEE Access* 2018; **6**: 18251–263.
- [127] Sun F, Mao C and Fan X et al. Accelerometer-based speed-adaptive gait authentication method for wearable IoT devices. *IEEE Internet Things J* 2018; **6**: 820–30.
- [128] Sun F, Zang W and Gravina R et al. Gait-based identification for elderly users in wearable healthcare systems. *Inform Fusion* 2020; **53**: 134–44.
- [129] Amin R, Kumar N and Biswas GP et al. A light weight authentication protocol for iot-enabled devices in distributed cloud computing environment. *Future Gener Comput Syst* 2018; **78**: 1005–19.
- [130] Wazid M, Das AK and Kumar N et al. Design of secure key management and user authentication scheme for fog computing services. *Future Gener Comput Syst* 2019; **91**: 475–92.
- [131] Tutari VH, Das B and Chowdhury DR. 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 (ICACCP)*, 2019, 1–6.
- [132] Yen TF, Xie Y and Yu F et al. 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] Franklin J, McCoy D and Tabriz P et al. Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting. In: *Proceedings of the 15th USENIX Conference on Security Symposium*, 2006, 16–89.
- [134] Desmond LCC, Yuan CC and Pheng TC et al. Identifying unique devices through wireless fingerprinting. In: *Proceedings of the 1st ACM Conference on Wireless Network Security*, 2008, 46–55.
- [135] Radhakrishnan SV, Uluagac AS and Beyah R. GTID: a technique for physical device and device type fingerprinting. *IEEE Trans Dependable Secure Comput* 2015; **12**: 519–32.
- [136] Hall J, Barbeau M and Kranakis E. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In: *Proceedings of Communications, Internet, and Information Technology*, 2004, 201–06.
- [137] Brik V, Banerjee S and Gruteser M et al. Wireless device identification with radiometric signatures. In: *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, 2006, 116–27.
- [138] van Goethem T, Scheepers W and Preuveneers D et al. Accelerometerbased Device Fingerprinting for Multifactor Mobile Authentication. In: *Proceedings of the 8th International Symposium on Engineering Secure Software and Systems*, 2016, 106–21.

- [139] Baldini G, Steri G and Dimc F et al. Experimental identification of smartphones using fingerprints of builtin microelectro mechanical systems. *Sensors* 2016; **6**: 8–18.
- [140] Zou L, He Q and Wu J. Source cellphone verification from speech recordings using sparse representation. *Digital Signal Process* 2017; **62**: 125–36.
- [141] Zhou Z, Diao W and Liu X et al. Acoustic fingerprinting revisited: generate stable device ID stealthily with inaudible sound. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, 429–40.
- [142] Dirik AE, Sencar HT and Memon N. Digital single lens reflex camera identification from traces of sensor dust. *IEEE Trans Inform Forensics Secur* 2008; **3**: 539–52.
- [143] Aksu H, Uluagac AS and Bentley ES. Identification of wearable devices with bluetooth. *IEEE Trans Sustainable Comput* 2021; **6**: 221–30.
- [144] Bojinov H, Michalevsky Y and Nakibly G et al. Mobile device identification via sensor fingerprinting. *ArXiv preprint [arXiv:1408.1416]*, 2014.
- [145] Hupperich T, Hosseini H and Holz T. Leveraging sensor fingerprinting for mobile device authentication. *Detection Intrusions Malware Vulnerability Assess* 2016; **9721**: 377–96.
- [146] Gope P and Sikdar B. Lightweight and privacy-preserving two-factor authentication scheme for iot devices. *IEEE Internet Things J* 2019; **6**: 580–89.
- [147] Chatterjee B, Das D and Maity S et al. RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning. *IEEE Internet Things J* 2019; **6**: 388–98.
- [148] Schrmann D and Sigg S. Secure communication based on ambient audio. *IEEE Trans Mob Comput* 2013; **12**: 358–70.
- [149] Quach Q, Nguyen N and Dinh T. Secure authentication for mobile devices based on acoustic background fingerprint. *Knowl Syst Eng* 2014; **244**: 375–87.
- [150] Karapanos N, Marforio C and Soriente C et al. Sound-proof: usable twofactor authentication based on ambient sound. In: *Proceedings of the 24th USENIX Conference on Security Symposium*, 2015, 483–98.
- [151] Mayrhofer R and Gellersen H. Shake well before use: intuitive and secure pairing of mobile devices. *IEEE Transac Mob Comput* 2009; **8**: 792–806.
- [152] Han J, Pan S and Sinha MK et al. Smart home occupant identification via sensor fusion across on-object devices. *ACM Trans Sensor Networks* 2018; **14**: 1–22.
- [153] Han J, Chung AJ and Sinha MK et al. 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*, 2018, 836–52.
- [154] Shi C, Liu J and Liu H et al. 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*, 2017, 1–10.
- [155] Kayacik HG, Just M and Baillie L. et al. Data driven authentication: on the effectiveness of user behaviour modelling with mobile device sensors, 2014. <https://doi.org/10.48550/ARXIV.1410.7743>.
- [156] Mahalakshmi B and Suseendran G. *Data Management, Analytics and Innovation*, Springer, 2019, 467–82.
- [157] Maithili K, Vinothkumar V and Latha P. Analyzing the security mechanisms to prevent unauthorized access in cloud and network security. *J Comput Theor Nanosci* 2018; **15**: 2059–63.
- [158] Chhabra A and Arora S. 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)*. IEEE, 2017, 243–46.
- [159] Abusaimh H. Security attacks in cloud computing and corresponding defending mechanisms. *Int J Adv Trends Comput Sci Eng* 2020; **9**: 4141–8.
- [160] Mehrtak M, SeyedAlinaghi S and MohsseniPour M. et al. Security challenges and solutions using healthcare cloud computing. *J Med Life* 2021; **14**: 448–61.
- [161] Maniah, Abdurachman E, Gaol FL and Soewito B. Survey on threats and risks in the cloud computing environment. *Proc Comput Sci* 2019; **161**: 1325–32.
- [162] Alzahrani BA, Irshad A and Albeshri A et al. A provably secure and lightweight patient-healthcare authentication protocol in wireless body area networks. *Wireless Personal Commun* 2021; **117**: 47–69.
- [163] Xu Z, Xu C and Liang W et al. A lightweight mutual authentication and key agreement scheme for medical internet of things. *IEEE Access* 2019; **7**: 53922–31.
- [164] Kasyoka P, Kimwele M and Angolo SM. Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. *J Med Eng Technol* 2020; **44**: 12–9.
- [165] Bhatia T, Verma A and Sharma G. Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing. *Concurrency Comput Pract Experience* 2019; **32**: 1–16.
- [166] Shen J, Tan H and Moh S et al. Enhanced secure sensor association and key management in wireless body area networks. *J Commun Netw* 2015; **17**: 453–62.
- [167] Zhao H, Xu R and Shu M et al. Physiological-signal-based key negotiation protocols for body sensor networks: a survey. In: *Proceeding of IEEE 12th International Symposium on Autonomous Decentralized Systems*, 2015.
- [168] Altop DK, Levi A and Tuzcu V. Deriving cryptographic keys from physiological signals. *Pervasive Mob Comput* 2016; **39**: 65–79.
- [169] Pirbhulal S, Zhang H and Wu W et al. Heart-beats based biometric random binary sequences generation to secure wireless body sensor networks. *IEEE Trans Biomed Eng* 2018; **65**: 2751–59.
- [170] Sun Y and Lo B. An artificial neural network framework for gaitbased biometrics. *IEEE J Biomed Health Inform* 2019; **23**: 987–98.
- [171] Poon C, Zhang YT and Bao SD. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Commun Mag* 2006; **44**: 73–81.

- [172] Hu C, Cheng X and Zhang F et al. 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., 2013, 14–19.
- [173] Miao F, Bao S and Li Y. Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security. *IET Inform Secur* 2013; **7**: 87–96.
- [174] Ali A and Khan FA. Key agreement schemes in wireless body area networks: taxonomy and state-of-the-art. *J Med Syst* 2015; **39**: 115.
- [175] Zaghoulani EK, Jemai A and Benzina A et al. 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] Tams B, Mihailescu P and Munk A. Security considerations in minutiae-based fuzzy vaults. *IEEE Trans Inform Forensics Secur* 2015; **10**: 985–98.
- [177] Davis R. The data encryption standard in perspective. *IEEE Commun Soc Mag* 1978; **16**: 5–9.
- [178] Lee J, Yu S and Kim M et al. On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks. *IEEE Access* 2015; **8**: 107046–62.
- [179] Kim Y, Lee WS and Raghunathan V et al. Vibration-based secure side channel for medical devices. In: Proceedings of the 52nd Annual Design Automation Conference, 2015.
- [180] Kim J, Jin Lee B and Yoo SK. 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), 2013, 2283–86.
- [181] Mosenia A and Jha NK. Opsecure: A secure unidirectional optical channel for implantable medical devices. *IEEE Trans Multi-Scale Comput Syst* 2018; **4**: 410–19.
- [182] Sun F, Zang W and Huang H. Accelerometer-based key generation and distribution method for wearable IoT devices. *IEEE Internet Things J* 2020; **8**: 1636–50.
- [183] Bao S, Poon C and Zhang Y et al. Using the timing information of heartbeats as an entity identifier to secure body sensor network. *IEEE Trans Inform Technol Biomed* 2008; **12**: 772–9.
- [184] Gope P. LAAP: Lightweight anonymous authentication protocol for D2D-aided fog computing paradigm. *Comput Secur* 2019; **86**: 223–37.
- [185] Maji S, Banerjee U and Fuller SH et al. A low-power dual-factor authentication unit for secure implantable devices. In: Proceeding of IEEE Custom Integrated Circuits Conference (CICC), 2020.
- [186] Tehrani MN, Uysal M and Yanikomeroglu H. Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions. *IEEE Commun Mag* 2014; **52**: 86–92.
- [187] Wyner AD. The wire-tap channel. *Bell Syst Tech J* 1975; **54**: 1355–87.
- [188] Gabry F, Li N and Schrammar N et al. On the optimization of the secondary transmitters strategy in cognitive radio channels with secrecy. *IEEE J Sel Areas Commun* 2014; **32**: 451–63.
- [189] Mathur S, Trappe W and Mandayam N et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, 2008, 128–39.
- [190] Ahlswede R and Csiszar I. Common randomness in information theory and cryptography. Part I: secret sharing. *IEEE Trans Inform Theory* 1993; **39**: 1121–32.
- [191] Sayeed AM and Perrig A. Secure wireless communications: secret keys through multipath. In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, 2008, 3013–16.
- [192] Chou TH, Draper SC and Sayeed AM. Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness. In: Proceedings of IEEE International Symposium on Information Theory, 2010, 2518–22.
- [193] Awan MF, Kansanen K and Simbor SP et al. RSS-based secret key generation in wireless in-body networks. In: 2019 13th International Symposium on Medical Information and Communication Technology, 2019, 1–6.
- [194] Ray I, Kumar M and Yu L. LRBAC: a location-aware role-based access control model. In: the 2nd international conference on information systems security, 2006, 147–61.
- [195] Zhang Y and Feng D. A role-based access control model based on space, time and scale. *J Comput Res Dev* 2010; **7**: 1252–60.
- [196] Macaulay T. *RIoT Control: Understanding and Managing Risks and the Internet of Things*. Elsevier, 2016.
- [197] Sun G, Dong Y and Li Y. CP-ABE based data access control for cloud storage. *J Commun* 2011; **7**: 146–52.
- [198] Ruj S, Stojmenovic M and Nayak A. Decentralized access control with anonymous authentication of data stored in clouds. *IEEE Trans Parallel Distrib Syst* 2014; **25**: 384–94.
- [199] Belkhouja T, Sorour S and Hefaida MS. Role-based hierarchical medical data encryption for implantable medical devices. In: Proceedings of IEEE Global Communications Conference (GLOBECOM), 2019.
- [200] He D, Kumar N and Khan MK et al. Efficient privacy-aware authentication scheme for mobile cloud computing services. *IEEE Syst J* 2018; **12**: 1621–31.
- [201] Jariwala VJ and Jinwala DC. Chapter 4 – Adaptable SDA: Secure data aggregation framework in wireless body area networks, Academic, 2020.
- [202] Kalyani G and Chaudhari S. An efficient approach for enhancing security in internet of things using the optimum authentication key. *Int J Comput Appl* 2019; **42**: 306–14.
- [203] Chang L and Moskowitz IS. A decision theoretical based system for information downgrading. In: Proceedings of the 5th Conference on Information Sciences, 2000, 82–9.
- [204] Cramer R, Damgrd I and Nielsen JB. Multiparty computation from threshold homomorphic encryption. In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2001, 280–300.
- [205] Liu X, Choo KKR and Deng RH et al. Efficient and privacy-preserving outsourced calculation of rational numbers. *IEEE Trans Dependable Secure Comput* 2016; **15**: 27–39.

- [206] Song W, Wang B and Wang Q et al. Publicly verifiable computation of polynomials over outsourced data with multiple sources. *IEEE Trans Inform Forensics Secur* 2017; **12**: 2334–47.
- [207] Baudry K. Data center site search and selection, *Data Center Handbook: Plan, Design, Build, and Operations of a Smart Data Center*, 2021, 367–80.
- [208] Mendonca J, Andrade E and Endo PT et al. Disaster recovery solutions for IT systems: a systematic mapping study. *J Syst Software* 2019; **149**: 511–30.
- [209] Ko R, Lee SG and Rajan V. Cloud computing vulnerability incidents: A statistical overview, 2013.
- [210] Garraghan P, Yang R and Wen Z et al. Emergent failures: rethinking cloud reliability at scale. *IEEE Cloud Comput* 2018; **5**: 12–21.
- [211] Nachiappan R, Javadi B and Calheiros R. et al. Cloud storage reliability for big data applications: a state of the art survey *J Netw Comput Appl* 2017; **97**: 35–47.
- [212] Kirar A, Yadav AK and Maheswari S. 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). IEEE, 2016, 271–79.
- [213] Chen F, Luo Y and Zhang J et al. An infrastructure framework for privacy protection of community medical internet of things. *World Wide Web* 2018; **21**: 33–57.
- [214] Xu M and Buyya R. Brownout approach for adaptive management of resources and applications in cloud computing systems: a taxonomy and future directions. *ACM Comput Surv* 2019; **52**: 1–27.
- [215] Zhong Z, Xu M and Rodriguez MA et al. Machine learning-based orchestration of containers: a taxonomy and future directions. *ACM Comput Surv* 2022; **54**: 1–35.
- [216] Xu M, Song C and Wu H et al. EsDNN: Deep neural network based multivariate workload prediction in cloud computing environments. *ACM Trans Internet Technol* 2022; to appear.
- [217] Kaur K, Gupta I and Singh AK 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), 2017, 87–95.
- [218] Huang H, Sun X and Xiao F et al. Blockchain-based ehealth system for auditable EHRs manipulation in cloud environments. *J Parallel Distrib Comput* 2021; **148**: 46–57.
- [219] Pandey AK, Khan AI and Abushark YB et al. Key issues in healthcare data integrity: analysis and recommendations. *IEEE Access* 2020; **8**: 40612–628.
- [220] Theodouli A, Arakliotis S and Moschou K et al. 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). IEEE, 2018, 1374–79.
- [221] Manogaran G, Thota C and Lopez D et al. *Cybersecurity for Industry 4.0*, Springer, 2017, 103–26.
- [222] Zhang Y, Deng RH and Xu S et al. Attribute-based encryption for cloud computing access control: a survey. *ACM Comput Surv* 2020; **53**: 1–41.
- [223] Praveen Kumar P, Syam Kumar P and Alphonse PJA. Attribute based encryption in cloud computing: a survey, gap analysis, and future directions. *J Netw Comput Appl* 2018; **108**: 37–52.
- [224] Huang Q, Yang Y and Shen M. Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing. *Future Gener Comput Syst* 2017; **72**: 239–49.
- [225] Yang Y, Chen X and Chen H et al. Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing. *IEEE Access* 2018; **6**: 18009–21.
- [226] Li J, Chen N and Zhang Y. Extended file hierarchy access control scheme with attribute-based encryption in cloud computing. *IEEE Trans Emerging Top Comput* 2021; **9**: 983–93.
- [227] Marnerides A, Watson M and Shirazi N et al. Malware analysis in cloud computing: network and system characteristics. In: 2013 IEEE Globecom workshops. IEEE, 2013, 482–87.
- [228] Watson M, Marnerides A and Mauthe A et al. Malware detection in cloud computing infrastructures. *IEEE Trans Dependable Secure Comput* 2015; **13**: 192–205.
- [229] Yadav RM. Effective analysis of malware detection in cloud computing. *Comput Secur* 2019; **83**: 14–21.
- [230] Zhang W, Lin Y and Wu J et al. Inference attack-resistant e-healthcare cloud system with fine-grained access control. *IEEE Trans Serv Comput* 2018; **14**: 167–78.
- [231] Ma X, Ma J and Kumari S et al. Privacy-preserving distributed multi-task learning against inference attack in cloud computing. *ACM Trans Internet Technol* 2021; **22**: 1–24.
- [232] Deznabi I, Mobayen M and Jafari N et al. An inference attack on genomic data using kinship, complex correlations, and phenotype information. *IEEE/ACM Trans Comput Biol Bioinform* 2017; **15**: 1333–43.
- [233] Shakya S. An efficient security framework for data migration in a cloud computing environment. *J Artif Intell* 2019; **1**: 45–53.
- [234] Ngnie Sighom JR, Zhang P and You L. Security enhancement for data migration in the cloud. *Future Internet* 2017; **9**: 23.
- [235] Singh S, Jeong YS and Park JH. A survey on cloud computing security: issues, threats, and solutions. *J Netw Comput Appl* 2016; **75**: 200–22.
- [236] Wu H, Wolter K and Jiao P et al. Eedto: an energy-efficient dynamic task offloading algorithm for blockchain-enabled iot-edge-cloud orchestrated computing. *IEEE Internet Things J* 2020; **8**: 2163–76.
- [237] Wu H, Zhang Z and Guan C et al. Collaborate edge and cloud computing with distributed deep learning for smart city internet of things. *IEEE Internet Things J* 2020; **7**: 8099–110.
- [238] Xu L, Huang D and Tsai WT. Cloud-based virtual laboratory for network security education. *IEEE Trans Educ* 2013; **57**: 145–50.

- [239] Xu M, Toosi AN and Buyya R. A self-adaptive approach for managing applications and harnessing renewable energy for sustainable cloud computing. *IEEE Trans Sustainable Comput* 2021; **6**: 544–58.
- [240] Souppaya M, Morello J and Scarfone K. Tech. rep., National Institute of Standards and Technology, 2017.
- [241] Tang J, Cui Y and Li Q et al. Ensuring security and privacy preservation for cloud data services. *ACM Comput Surv* 2016; **49**: 1–39.
- [242] Wei J, Zhang X and Ammons G et al. Managing security of virtual machine images in a cloud environment. In: *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, 2006, 91–6.
- [243] Loukidis-Andreou F, Giannakopoulos I and Doka K et al. Docker-Sec: a Fully Automated Container Security Enhancement Mechanism. In: *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, 2018, 1561–64.
- [244] Kwon S and Lee JH. Divds: Docker image vulnerability diagnostic system. *IEEE Access* 2020; **8**: 42666–673.
- [245] Huang W, Ganjali A and Kim BH et al. The state of public infrastructure-as-a-service cloud security. *ACM Comput Surv* 2015; **47**: 1–31.
- [246] Lin K, Liu W and Zhang K et al. 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)*. IEEE, 2019, 58–65.
- [247] Li SW, Koh JS and Nieh J. Protecting cloud virtual machines from hypervisor and host operating system exploits. In: *28th USENIX Security Symposium (USENIX Security 19)*, 2019, 1357–74.
- [248] Liu W, Zhang K and Tu B et al. 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)*. IEEE, 2019, 981–88.
- [249] Khalimov A, Benahmed S and Hussain R et al. Container-based sandboxes for malware analysis: a compromise worth considering. In: *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing*, 2019, 219–27.



Nan Li received a B.Sc. degree from Xidian University (Xi'an, China) in 2007, her M.Sc. degree from the 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 convert 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 an MSc degree in 2015, both in software engineering from the University of Electronic Science and Technology of China. He obtained his Ph.D. 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. The thesis was awarded the 2019 IEEE TCSC Outstanding Ph.D. Dissertation Award.



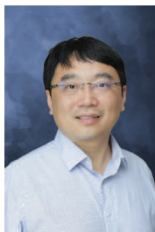
Qimeng Li graduated from the University of Calabria (UNICAL) with a master's degree in electrical engineering in 2017. And he received his Ph.D. in Information and Communication Technologies at UNICAL in 2022. His main research interests lie mainly in the field of multi-user activity recognition, wearable 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 a 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 a Ph.D. degree in computer applications technology from the University of Chinese Academy of Sciences, Shenzhen, China. His research interests include biomedical signal processing, medical image processing, biometrics, machine learning, the 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 a 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 College London. She is currently a Professor at Ningbo University of Technology and also the dean of the 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 the 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 than 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 the Chinese Society of Biomedical Engineering and the Executive member of the International Federation of Medical and Bioengineering (IFMBE). His current research interests include medical imaging technology and systems, information technology, and theoretical methods in medical imaging applications. 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 the non-linear acoustic radiation force theory, invented the ultrasonic shear wave quantitative elastography instrument, and the original non-invasive ultrasonic neuromodulation technology.