IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 25, 2019, accepted December 13, 2019, date of publication December 18, 2019,
date of current version December 27, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2960617

Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey

YINGNAN SUN, FRANK P.-W. LO, AND BENNY LO
Hamlyn Centre, Imperial College London, London SW7 2AZ, U.K.

Corresponding author: Yingnan Sun (y.sun16@imperial.ac.uk)

This work was supported by the Bill and Melinda Gates Foundation.

ABSTRACT With the increasing demands on quality healthcare and the raising cost of care, pervasive healthcare is considered as a technological solutions to address the global health issues. In particular, the recent advances in Internet of Things have led to the development of Internet of Medical Things (IoMT). Although such low cost and pervasive sensing devices could potentially transform the current reactive care to preventative care, the security and privacy issues of such sensing system are often overlooked. As the medical devices capture and process very sensitive personal health data, the devices and their associated communications have to be very secured to protect the user's privacy. However, the miniaturized IoMT devices have very limited computation power and fairly limited security schemes can be implemented in such devices. In addition, with the widespread use of IoMT devices, managing and ensuring the security of IoMT systems are very challenging and which are the major issues hindering the adoption of IoMT for clinical applications. In this paper, the security and privacy challenges, requirements, threats, and future research directions in the domain of IoMT are reviewed providing a general overview of the state-of-the-art approaches.

INDEX TERMS Security, privacy, Internet of Medical Things, IoMT, mIoT, healthcare systems, survey.

I. INTRODUCTION

In the healthcare industry, significant improvements in efficiency and quality of care are expected from the diverse range of developments in Internet of Things (IoT), which is often referred as Internet of Healthcare Things (IoHT) or Internet of Medical Things (IoMT). In particular, smart wearable and implantable medical devices have attracted much interest in recent years due to the advances in microelectronics, materials, and biosensor designs. The rapid development of IoMT, however, has meant that the security and privacy of these IoMT-based healthcare systems often has received insufficient attention. The consequences of inadequate security in IoMT healthcare systems can be, for instance, compromised patients' privacy due to eavesdropping, and delayed detection of life threatening episodes due to the disruption of normal operations of IoMT devices caused by Denial of Service (DoS) attacks. A study conducted by HP Fortify in 2015 found that the 10 most popular smartwatches (at the time) all had security vulnerabilities from insufficient authentication or authorization, lack of data transmission encryption, insecure interfaces, insecure software/firmware, and privacy concerns [1]. Authentication, for example, is the process of confirming identity of the user. All IoMT healthcare systems should only be accessed by authorized and authenticated users or devices. Insufficient authentication protection could potentially allow attackers to enter the system and gain access to private healthcare data of the users.

User and device authentication is important to a system as it ensures that the data is correctly attributed and information in the systems is only accessible to the authorized entities. In the context of healthcare systems, the ability to authenticate the users of medical devices could be used to establish the integrity of the data, for instance, activity information form obese patients. Authentication would also be used to safeguard patients' privacy by ensuring that information, such as the patients' electronic medical records [2], is only accessible to the authorized and authenticated users (i.e. patients' general practitioners). Network and system security is a well-established field, and extensive security protection schemes and methods are available to protect computer systems and networks. For example, public-key cryptosystems, such as Rivest-Shamir-Adleman (RSA) [3] and Digital Signature Algorithm (DSA)

The associate editor coordinating the review of this manuscript and approving it for publication was Chunsheng Zhu.

[4], are commonly used algorithms in securing computer networks.

However, many of such cryptosystems cannot be applied for IoT devices due to their low power and low computational capability [5]. Compare to typical IoT devices, wearable and implantable medical and healthcare devices are often designed with even lower computational power and battery capacities as they have to be miniaturized in size. IoMT devices have to store and process personalized health data, and some devices even have actuation functions to support the users' health (i.e. insulin pump). Therefore, the level of security required for IoMT devices are expected to be much higher than typical IoT and computing devices [6]. Yet, security and threats are often overlooked in the design of IoMT healthcare systems.

Most of the IoMT devices are designed to transmit and store the data in the cloud, which can be further processed and analyzed. This advancement in healthcare systems enables the medical carer to provide faster and more accurate responses to the patients that are being monitored by the medical and healthcare devices. However, it also introduces risks of users' data stored in the cloud servers being abused or stolen [7]. The privacy of the users' data, especially users' personal data must be well protected. Yet, many examples of security breaches of cloud servers from large enterprises, such as Facebook [8] and Yahoo [9], raise the question on whether the patients' sensitive health data can really be protected. In fact, more and more malicious attackers are targeting medical servers and eHealth systems, because personal health data is very valuable in the illegal markets [10]. Therefore, medical service providers require even stronger security measures, which inevitably increases the costs of creating, running, and maintaining these medical services.

In addition to developing countermeasures to attacks, post-attack measures are also needed to be well considered. Financial information, such as credit card security codes, can be made invalid and useless quickly, but personal health data can reveal a person's current health conditions [11]. When such data is stolen in a case of security breach, the retrieval and elimination of the stolen data is both challenging and critical. To protect patients' data, strong regulations and severe penalties must be in place from governments and healthcare organizations. In the European Union, Information Commissioner's Office (ICO) could only fine a company who is responsible for a data breach up to 500,000 pounds previously, however, with the newly introduced General Data Protection Regulation (GDPR), ICO is now able to fine a company based on the company's profits. For example, British Airways is suspected to be fined up to 183 million pounds, due to a data breach of 500,000 users from its website and mobile app [12]. In the United States, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides rules and provisions for the privacy of medical and healthcare data. The law also forces healthcare service providers to ensure the security and privacy of their systems against cyber-attacks and ransomware attacks. In addition, according to the GDPR, any incidents of data breaches in the healthcare systems must be reported promptly within 72 hours [13], where as HIPAA requires companies to report data breaches no later than 60 days if the breach affected more than 500 people [14].

Medical devices in the U.S. are regulated by the Food and Drug Administration (FDA). According to a study [15], among 13.79% of all the medical devices approved or cleared by FDA that include software, only 2.13% have incorporated cybersecurity in their software designs from 2002 to 2016. Recently, the FDA had issued a warning on cybersecurity vulnerabilities referred as "URGENT/11" which exists in a third-party software called IPnet. The URGENT/11 would affect more than 200 million devices related to medical services [16]. FDA has also updated their cybersecurity guidance on medical device software in 2018, to provide up to date instructions on protecting patients' data on medical devices and services. Despite the recent efforts put in by the governments and agencies, the number of cyberattack against medical services has increased [17].

This paper provides an overview of the current the challenges, requirements, and identify potential threats for the security and privacy of the IoMT healthcare systems. Despite there are several reviews and surveys on this topic in the literature, they all have different research focuses. Sun et al. [18] published a review that focuses on the security and privacy requirements regarding to the data flow in different layers of IoMT systems. Williams and McCauley [19] reviewed the vulnerabilities of interconnected medical devices in the IoHT environment. Sahi et al. [20] presented a review that discusses the privacy preservation issues in the context of e-healthcare environments. Alsubaei *et al.* [21] published a review that provides a taxonomy of the security and privacy issues of IoMT. Hatzivasilis et al. [22] reviewed security and privacy challenges of IoMT in a business stand point. Algarni [23] surveyed and analyzed security research for smart healthcare systems by classifying and ranking top contributed research works in their applicable domains.

This paper uses a bottom-up approach, reviewing the security and privacy challenges and requirements from the data level to the medical server level of the IoMT-based healthcare systems. In addition, this paper presents the potential of biometrics and its applications for securing IoMT healthcare systems. This paper also discusses the security schemes for implantable IoMT devices, as there are increasing number of medical implantable devices and they shares unique challenges due to their hardware limitations. The rest of the paper is organized as follows: Section II provides an overview of the IoMT-based healthcare system and challenges for the IoMT network and protocol designs. A survey of the security and privacy requirements for each level of the IoMT healthcare systems is presented in Section III. Then, the state-of-the-art security research is discussed in Section IV, as well as biometric authentication and implantable security schemes. Discussions, future research directions, and conclusions are presented in the last three sections.

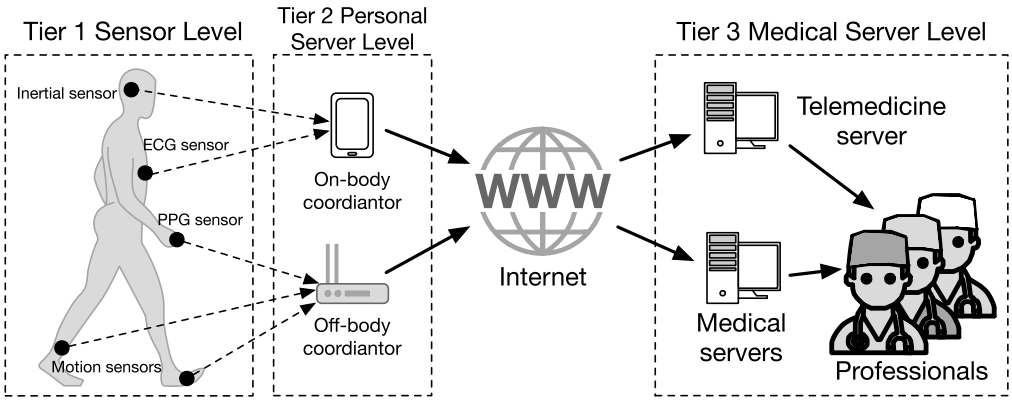


FIGURE 1. Architecture of IoMT-based healthcare systems [24].

II. INTERNET OF MEDICAL THINGS: SYSTEMS, NETWORKS, AND DESIGN CHALLENGES

A. IoMT-BASED HEALTHCARE SYSTEMS

IoMT-based healthcare systems often consist of 3 tiers, sensor level, personal server level, and medical server level, as indicated in Fig. 1. This architecture of IoMT healthcare systems have adopted in many recently proposed IoMT-based healthcare systems, such as [25]. Medical devices and sensors are located in the sensor level, which form a local network and often referred as a Body Sensor Network (BSN) [26]. Low-power wireless technology standards including Bluetooth Low Energy (BLE), Near-Field Communication (NFC), and Radio-Frequency IDentification (RFID), are often employed for wireless communications in the sensor and personal server levels. BLE supports many network topologies, such as star and mesh, whereas NFC and RFID can only support ultra-low energy, device-to-device close proximity direct communications, which are often required by implantable devices.

Physiological data collected by the medical devices will be sent to personal servers, which can be on-body devices, such as smart phones, programmers, and tablets, or off-body devices, such as routers and gateways. The purposes of personal servers are to process and store patients' data locally before sending to the centralized medical servers. A personal server is required to be able to operate normally when the network connection to the medical servers is lost. Medical personnel, such as doctors, are able to access patients' data remotely, providing prompt advice to the patients. Algorithms and computer programs for early diagnoses and rehabilitation progress assessments can also be run on the medical servers with patients' consents. Many IoMT-based healthcare systems have been proposed for continuous patient monitoring in the last decades, but many of them do not adopt any security and privacy measures in their designs or left out as future work, such as MobiCare [27]. These research have focused more on other design challenges such as power consumption and usability, rather than the security of the systems and the privacy of patients' data. Recently proposed IoMT-based healthcare systems, such as BSN-Care [28], have adopted encryption and authentication schemes into their designs.

B. NETWORK AND PROTOCOL DESIGN CHALLENGES

Protocol is a set of rules that govern the exchange or transmission of data between devices, and a routing protocol specifies how network routers exchange data with one another, disseminating information that enables them to select routes between any two nodes in the same network or in different networks. Routing protocols in wireless networks are more complex than those used in wired networks in many respects, including network topology, power conservation, and channel effectiveness. Thus, transferring data between nodes is not the only functionality required from routing protocols in wireless networks.

1) POSTURAL BODY MOVEMENTS

On-body medical devices and sensors are often in a group-based, postural body movement as the patients under diagnosis or users under monitoring are often not stationary, resulting in frequent changes in network topology and components [29]. Routing protocols in BSNs should be adaptive to both repetitive and unpredictable changes in the quality of communication links between sensor nodes, which varies as a function of time against body movements. It can be utilized in routing protocols to conserve energy. For example, a transmission power control scheme based on gait cycle for BSNs has been proposed in [30], where transmission time is optimized by matching link quality changes due to walking. On the other hand, there are also unpredictable changes of link quality due to signal blockage by clothes or bags that intensifies channel attenuation.

2) TEMPERATURE RISE

Antenna radiation absorption and power consumption of node circuitry are the two sources than cause temperature rise in sensor nodes [31]. Radio energy can also be absorbed by the tissues which could heat up the tissues, attenuate the signals,

and cause skin or tissue burns [32]. Therefore, transmission and computing power in sensor nodes should be considered in routing protocols, and extra attention should be made for implant sensor nodes, as heat can damage tissues and organs of the human body.

3) ENERGY EFFICIENCY

Routing protocols in IoMT systems should be designed to optimize the energy efficiency for both local energy consumption on sensor nodes and overall network lifetime. Energy efficiency is a crucial element of IoMT systems, as it determines the size of the devices, the lifetime of the system, and the usability of the devices. For instance, surgeries will be required for implant sensor nodes to replace batteries, and such surgeries are risky and very expensive. Typical implantable devices, such as pacemakers, should have the battery lifetime of at least 10 to 15 years to enable the user to live a normal life [33]. For wearable sensor nodes, frequently charging or replacing batteries hinder the usability of the devices.

4) TRANSMISSION RANGE

Short transmission range along with the postural body movements could lead to the problems of disconnection and re-partitioning among sensor nodes in IoMT systems [34]. The number of sensor nodes on a patient or a user should be minimized to reduce discomfort, which results in fewer routes to neighbour sensor nodes. Therefore, if the connecting sensor node is out of range, packets will have to be routed by an alternative path resulting in higher energy consumption in that path and longer time for packets to reach the destination. In BSNs, if the alternative path includes one or more implantable devices, the routing protocol must be able to decide whether to take this alternative path based on the importance of the contents in the packets.

5) HETEROGENEOUS ENVIRONMENT

In most of the IoMT applications, different types of sensor nodes from a variety of medical equipment vendors are required to measure different physiological signals of patients or users. Therefore, routing protocols have to be designed to tackle the challenges of heterogeneous environments in many BSN applications. To solve this problem, many BSN platforms and frameworks have been proposed for medical devices from different vendors to work together, such as DexterNet [35].

6) QUALITY OF SERVICE

Real time life-critical BSN applications, such as Electrocardiogram (ECG) sensing, are both data loss sensitive and time critical, and the QoS requirements of such applications must be met [36]. However, implantable sensor nodes has limited memory and computation capability, which means routing protocols have to adopt QoS measures such as retransmission and error correction strategies without increasing computational complexity on the sensor nodes.

III. SECURITY AND PRIVACY REQUIREMENTS FOR IoMT HEALTHCARE SYSTEMS

Security and privacy requirements for the IoMT healthcare systems are more rigorous than that of the typical IoT-based infrastructures. IoMT healthcare systems have many additional security requirements, such as device localization [37], which can also contribute to ensure the security and privacy of the systems. The functionalities of each level of the IoMT healthcare systems are different, which means each level has different security and privacy requirements. Therefore, the requirements for each level are analyzed and discussed individually. In addition, the security and privacy requirements in the data level is also discussed in the context of the GDPR and HIPAA.

A. DATA LEVEL

1) CONFIDENTIALITY

Collection and storage of patient health data must comply with legal and ethical privacy regulations, such as GDPR and HIPAA, in which only authorized individuals can have access to those data. To prevent breaches of data, adequate measures must be adopted to ensure the confidentiality of the health data associated with individual patients. The importance of such measures cannot be overemphasized, as the data stolen by cyber criminals could be sold in illegal markets, causing the patients to suffer from not only privacy violation but also possible financial and reputational damages. It has been stated in Article 5(e) of the GDPR that personal data should be erased once it has been processed and no longer required, with exceptions, such as archiving, scientific, historical or statistical purposes (Article 89). On the other hand, HIPAA has no restrictions on how long the patients' data can be kept. Medical service providers under HIPAA compliance may disclose protected health information (PHI) of patients to another provider without patients' consent, whereas care providers who are compliant with the GDPR must obtain explicit consent from EU patients for any PHI exchanges with other providers [38].

2) INTEGRITY

For IoMT healthcare systems, the purpose of the data integrity requirement is to ensure that the data arriving at the intended destination have not been compromised in any way during the wireless transmission [39]. Attackers could gain access to and modify patient data by taking advantage of the broadcast characteristic of the wireless network, and which could lead to severe implications in life-threatening cases. To guarantee that the data have not been compromised, the capacity to detect potential unauthorized distortions or manipulations of the data is critical. Therefore, appropriate mechanisms of data integrity must be implemented to prevent alteration of transferred data by malicious attacks. Moreover, the integrity of the data stored in the medical servers also needs to be ensured, which means the data cannot be tempered with. Article 5(d) of the GDPR states that medical

service providers have to make necessary measures to keep patients' data accurate and up to date. It also requires inaccurate personal data to be erased or rectified as soon as possible. The GDPR also emphasizes on the 'accuracy' of the data, allowing data owners request service providers for the rectification of any inaccurate data, and the service providers must respond to the requests within a calendar month. Similarly, HIPAA requires medical service providers to adopt necessary measures to ensure any PHI stored in the systems cannot be altered without authorization.

3) AVAILABILITY

Services and data must be accessible when they are required to the relevant users. Such services and data, provided by the medical servers and devices, will become inaccessible if DoS attacks occur. Any inaccessible data or services could lead to life threatening incidents, such as unable to provide prompt alert in the case of a heart attack. Therefore, to accommodate the possibility of availability loss, the healthcare applications must be always-on to ensure data availability to the users and emergency services. According to Article 32 of the GDPR, medical service providers must have the ability to restore the availability and access to personal data in a timely manner, such as adopting preventive security measures and countermeasures to DoS attacks [40]. Furthermore, according to Article 17 of the GDPR, patients in the EU have the right to request their data held by the medical service providers to be erased, which is known as 'Right to Be Forgotten', however, such right is not required by the HIPAA [38].

B. SENSOR LEVEL

The security and privacy in the sensor level faces the most challenges of the 3-tier IoMT healthcare system, due to the limited computational capability and power constraint of the medical devices and sensors [41]. The current trend in sensor level security research is to put most of the computations in the personal server level instead, and the security measures in the sensor level are required to be light-weight and less communication overheads.

1) TAMPER-PROOF HARDWARE

IoMT devices, especially ambient sensors, can be stolen physically, which leads to security information being exposed to attackers. Furthermore, the stolen devices can be reprogrammed by attackers and redeployed to the system, listening to communications without being noticed [42]. Therefore, physical theft of medical devices is a severe security threat and must be addressed in the IoMT healthcare systems. Medical devices in the systems should at least have tamper resistant integrated circuits, preventing codes loaded on the devices being read by third parties once being deployed. A example solution is to use Physically Unclonable Functions (PUFs) to secure data stored in the Integrated Circuits (ICs) of the medical devices [43].

2) LOCALIZATION

Researchers are focusing on two types of sensor localization, on-body sensor position and sensor's/patient's location in an indoor environment. The former sensor localization is typically designed to identify whether the sensors are located in the desired body positions. Such on-body sensor position identification is of vital importance for applications such as activity recognition [44]. The later sensor localization, also known as Location of Things (LoT), is designed to locate the sensor in a room or to locate the patient wearing the sensor in a building. In addition, due to the design of the IoMT healthcare systems, medical devices could move in and out of the network coverage very frequently. Therefore, a real-time intrusion detection measure is required if the network allows its sensors to leave and rejoin irregularly. An example of such measures is SVELTE [45], an intrusion detection method that reports malicious nodes joining the network to administrators.

3) SELF-HEALING

Self-healing, introduced in Autonomic Computing [46], is of great importance for the IoMT systems, as IoMT devices shall resume operation after the network attacks. To achieve self-healing, an IoMT system should be able to detect and diagnose the attacks, and apply corresponding security mechanisms [47] with minimal human intervention. Self-healing methods deployed should also be light-weight, in terms of communication overheads to the network and computational complexity to the medical and healthcare devices. An example of self-healing architecture for IoT is proposed in [48], where dendritic cells algorithm is applied in the network to detect network attacks. However, as different types of network attacks require different detection and recovery methods, it is important for network administrators to decide which autonomic security schemes should be implemented in the network.

4) OVER-THE-AIR PROGRAMMING

Over-the-air programming or updating (OTA) has become a popular method to update an IoT system with a large number of sensor nodes, which introduces security concerns such as malicious sensor nodes listening updates and forging identities into the network. OTA can be part of the self-healing mechanism, updating security rules for the network instantly. To implement OTA properly, security measures must be made to prevent OTA updates being exploited by attackers. An example solution is SEDA [49], which is a secure OTA programming protocol designed for distributed network like IoMT systems.

5) FORWARD AND BACKWARD COMPATIBILITY

This is also a key requirement in real-time healthcare applications where faulty medical sensors are replaced promptly with new ones. Forward compatibility is characterized by the fact that future messages cannot be read by medical sensors

if their transmission occurs after the sensors have left the network. Conversely, in backward compatibility, messages that have been transmitted earlier cannot be read by a sensor which just entered the network [50]. Compatibility issues can potentially be solved by implementing OTA programming for the distribution of the newest software update promptly.

C. PERSONAL SERVER LEVEL

As patients' data is often stored and aggregated in the personal server level before being forwarded to the medical servers in the IoMT healthcare systems [51], it is essential to ensure that the data is well protected while on the personal servers. Generally, two types of authentication schemes must be deployed to ensure security and privacy in the personal server level, namely device authentication and user authentication.

1) DEVICE AUTHENTICATION

Personal server (i.e. a smart phone) shall perform authentication before accepting data sent from the medical devices and sensors. Device authentication scheme should be able to establish secured/encrypted communications for data confidentiality and integrity [52]. False information from malicious devices about patients' physical conditions could have severe negative impacts on the clinical diagnosis and care decisions, therefore, device authentication must be implemented in any IoMT healthcare systems. Device authentication is mutual between personal servers and devices, but the majority of the computation should be performed on the personal servers, as they often have more computational capability and power than the medical devices and sensors.

2) USER AUTHENTICATION

The data stored either temporarily or permanently on the personal servers should only be accessed by the patients and medical staff, such as caregivers, therefore, effective user authentication schemes are required [53]. Personal servers in the IoMT healthcare systems should also support emergency access of the data if the patients are in critical conditions, such as having a stroke or a seizure. A popular solution to user authentication in the personal server level is the use of biometrics, which is particularly applicable in the IoMT healthcare systems, as most of the biometrics can be easily collected from medical and healthcare devices worn by or implanted in the human body.

D. MEDICAL SERVER LEVEL

Two of the most important requirements on the security and privacy of patients' data in the medical server level are: only authorized devices and personnel have access to the data; and the data itself must be encrypted at all time when stored in the databases [54]. With more and more paper-based medical records have been digitized into Electronic Medical Record (EMR), security and privacy concerns with the medical servers storing EMRs are growing [55]. Therefore, proper security measures must be in place in the medical server level for IoMT healthcare systems.

1) ACCESS CONTROL

To ensure only authorized devices and personnel have access to the medical servers, effective access control schemes must be deployed. It is difficult to ask permission or consent of a patient every time a data access request is made, therefore, the service providers of the medical servers should provide selective access control for patients, i.e. to choose which data can be shared without permissions and which third parties can have access. A popular solution of selective access control is Attribute-Based Encryption (ABE) [56], which is categorized as public-key cryptography where the secret keys are generated from attributes (i.e. received signal strength, location, and channel frequency). Access trees in the ABE solutions can be selectively constructed with a set of attributes, so that only a set of attributes that satisfies the tree will be granted access to the encrypted data.

Medical servers should also be capable of updating access control policy efficiently. Policy update can be redundant for medical servers, for example, many cloud security measures require the change of encryption keys when updating access control policy [57], which leads to decrypt and re-encrypt data in the medical servers and in the personal servers. Therefore, a scalable and less redundant policy update scheme should be deployed to reduce or eliminate the computational overheads in cryptography. A popular solution is the 2-layer over-encryption [58], where policy update can be made in surface encryption layer (SEL) while a further encryption is imposed by the data owners in base encryption layer (BEL). Furthermore, emergency access control should also be supported in the medical servers, either by disabling security measures over patient's data or by granting a third-party emergency access. For example, Proxy Re-Encryption (PRE) [59] can be used to convert data encrypted by a patient's public key into encrypted data which can be decrypted by a third party, without revealing patients' data during the transmission.

2) KEY MANAGEMENT

The development of secure applications depends on key management protocols, of which the goal is to implement and distribute cryptographic keys to sensor nodes. Trusted server are key pre-distribution are the two main types of key management protocols used in the IoMT healthcare systems. Trusted server protocols achieve key agreement within the network in a trusted base station. These types of protocols are appropriate for hierarchical networks, however, in spite of this, the trusted server protocols are inadequate for critical applications like those related to healthcare because a whole network failure could paralyze a trusted server in a real-time environment [60]. Key pre-distribution protocols are often implemented in symmetric key cryptography, to share secret keys within the network prior to the network being fully functional. These types of protocols are more appropriate for

TABLE 1. DoS attacks at each routing protocol layer.

Layers	DoS attacks
Physical layer	Jamming
	Node tampering
MAC layer	Collision and unfairness
	Denial of sleep
Network layer	Spoofing, replaying, and wormhole
	Homing
	Hello floods
Transport layer	Flooding
	De-synchronization
Application layer	Overwhelming sensors
	Reprogramming attacks
	Route-based DoS

resource-limited sensor networks because their implementation is straightforward and do not require very complex computation.

3) TRUST MANAGEMENT

Trust means that there is a two-way association between two reliable nodes, such as a sensor node and a network coordinator, that share data with one another. Similarly, one study [61] explained that trust as the extent to which a node is secured and dependable when it interacts with another node. Distributed collaboration between the nodes of network must exist for wireless healthcare applications to be successful. In this regard, the level of trust of a node can be determined with trust management systems, which are important particularly as the trust assessment of a node's behaviour, such as the delivery and quality of data, is essential in healthcare applications [62].

4) RESISTANCE TO DoS ATTACKS

Table 1 lists common DoS attacks against wireless healthcare applications [63]. Attackers can use high-energy signals to stop the wireless network from operating properly, such as jamming attacks in the physical layer [64]. There are many approaches proposed in safeguarding and self-repairing the network against such attacks, such as evasion defence and competition strategies, but they are all at early stage of research [65]. Therefore, much research is required to develop strategies to protect the system against DoS attacks for real-time IoMT healthcare systems, due to the mobile and dynamic nature of the wireless networks.

IV. SECURITY SCHEMES FOR IoMT HEALTHCARE SYSTEMS

In this section, state-of-the-art security schemes for IoMT healthcare systems are discussed. A comparison of the state-of-the-art IoMT security research is presented in Table 2. A detailed discussion on the comparative study is presented, in terms of their cryptographic designs, applications and security analysis. In addition, random number generator (RNG), which is an important part of the cryptosystems is also discussed, and example RNG research applicable on IoMT devices is highlighted. Furthermore, a review on the biometric authentication and its application in the IoMT healthcare systems is provided, and a survey of security schemes for implantable IoMT devices is presented.

A. STATE-OF-THE-ART

There are generally two common types of cryptographic algorithms: symmetrical and asymmetrical (public-key). Compare to symmetric encryption, asymmetric cryptosystems provide better security protection but require significantly more computational capability. Due to the limited computational capacities of IoMT devices in the sensor level, any data encryption and decryption solutions proposed for securing IoMT devices should be light-weight and the overhead of the communication channels should be minimized. Whereas data transmission between personal server level and medical server level should be protected with much stronger security schemes, as the data is often transmitted via public channels such as the internet.

As listed in Table 2, the majority of cloud-based authentication, data storage, and access control research adopt public-key cryptography over symmetrical cryptography. Among these research ([66], [67], [69]–[73], [78], [79]), Elliptic curve cryptography (ECC) is the most popular public-key cryptographic algorithm, as it requires smaller key size over other traditional public-key cryptographic algorithms, such as Rivest-Shamir-Adleman (RSA). On the other hand, symmetric cryptographic algorithms are often used in research ([68], [75], [76]) on access control, data transmission to and from IoMT sensors, as they are light-weight on those resource constraint devices. For hybrid security schemes ([74], [77], [80], [81]), symmetric cryptographic algorithms are often used as session keys. Furthermore, the most applied attacks in the adversarial/security analysis are Chosen Plaintext Attack CPA), replay, impersonation, insider, eavesdropping, and Man-in-the-Middle (MitM) attacks. A number of research also analyze their security schemes in terms of Mutual Authentication (MA), Anonymity and Traceability (A&T), Forward Security (FS), Contextual Privacy (CP), and and unlinkability. Apart from ([68], [81]) that performed their experiments on actual hardware, the others performed their experiments using computer simulations.

Although the state-of-the-art security schemes are mainly using readily available RNGs in their simulations, on-node random number generation is an emerging research topic for IoMT applications. Random numbers are often generated by a pseudo-random number generator (PRNG) with a random seed in modern computers. PRNGs are deterministic approaches implemented in software. The PRNGs with the same seed will always generate the same sequence of random

TABLE 2. Comparison of state-of-the-art security and privacy research on IoMT healthcare systems (EHR = Electronic Health Record, Sim = Simulation, Proto = Prototype, MA = Mutual Authentication, FS = Forward Security, CP = Contextual Privacy, CPA = Chosen Plaintext Attack, A&T = Anonymity and Traceability, MitM = Man-in-the-Middle, DoS = Denial of Service).

Type	Data type	Sim	Proto	Adversarial-analysis	Purpose	Methodology
[66] Public-key	PHI/EHR	Yes	No	A&T, FS, CP, MA, Unlinkability	Data transmission	Certificateless generalized signcryption
[67] Public-key	PHI/EHR	Yes	No	Chosen keyword-CPA	Access control, data retrieval	Pairing-based cryptography
[68] Symmetric	PHI/EHR	No	Yes	Eavesdropping, CPA, Replay, Camouflage Trust Attack	Data transmission	Group send-receive model
[69] Public-key	-	Yes	No	Unlinkability, A&T, DoS, Traffic Analysis, Revocation, MA, MitM, Replay	Cloud-based authentication	Elliptic curve cryptography
[70] Public-key	PHI/EHR	Yes	No	Sinkhole, wormhole, Sybil	Access control	Elliptic curve cryptography
[71] Public-key	-	Yes	No	Key compromise impersonation, A&T, know-key attack, Replay, MA, Impersonation, Internal, MitM	Cloud-based authentication	Elliptic curve cryptography
[72] Public-key	PHI/EHR	No	No	MA, MitM, quantum computing, known ciphertext attack, CPA, data masquerading, replay	Cloud-based authentication, data encryption, access control	Lattice-based cryptography
[73] Public-key	PHI/EHR	No	No	Data leakage and destruction, collusion, insider attacks	Data storage, transmission, access control	Slepian-Wolf-coding-based secret sharing
[74] Hybrid	Medical images	Yes	No	-	Data transmission	Advanced Encryption Standard (AES), Rivest, Shamir, and Adleman (RSA)
[75] Symmetric	PHI/EHR	Yes	No	Collusion, attribute privacy	Access control	ciphertext-policy attribute-based encryption
[76] Symmetric	-	Yes	No	Impersonation, eavesdropping, FS, insider, password guessing, A&T, node capture, MitM	Wearable device authentication	bitwise XOR, one-way hash function
[77] Hybrid	-	Yes	No	Password guessing, node capture, replay, impersonation, insider, key replicating, A&T, key compromise impersonation, DoS, session key verification	Cloud-based authentication	bitwise XOR, one-way hash function, Elliptic curve cryptography
[78] Public-key	PHI/EHR	Yes	No	Identity privacy, authenticity, unforgeability	Cloud-based data storage, access control	Diffie-Hellman key exchange, identity-based cryptosystem
[79] Public-key	PHI/EHR	Yes	No	unlinkability, know-key attack, CPA, CP, A&T, replay, forging, unobservability, time correlation, mitigating, pseudonymity	Data transmission	Elliptic curve cryptography
[80] Hybrid	-	Yes	No	CPA	Cloud-based access control	Password-based break-glass key, attribute-based encryption
[81] Hybrid	-	Yes	Yes	MA, replay, MitM, false identity, key negotiation fairness, two-way identification	Device/node authentication	Elliptic curve cryptography, session key symmetric

TABLE 3. Characteristics of biometric traits and the requirements of biometric authentication schemes [82].

Characteristics	Explanations
Universal	All potential users can use the system
Unique	Each user must be differentiated
Measurable	The system must be able to collect/measure the biometrics
Acceptable	The sampling process must be user-friendly
Circumvention	The system must prevent attackers bypassing itself

numbers. If the seed is not generated from a true random source, the PRNGs can be deduced by potential attackers. Due to the size and power constraint of IoMT devices, many true random number generators based on randomness of physical phenomena are not suitable for the miniaturized sensors. An example solution to generate true random numbers is the use of inertial sensors on IoMT devices. Voris et al. [83] proposed the use of an accelerometer as the random source for generating random numbers on a RFID tag. Human's walking acceleration and gyroscope measurements collected by inertial sensors can also be used as random sources for TRNGs [84]. Furthermore, Wallace et al. [85] proposed SensoRNG, a TRNG design based on multiple internal sensors on mobile phones, including microphones, inertial sensors, and radio. Inertial sensors based TRNGs have the potentials to be used in IoMT devices for data encryption, but issues such as low entropy when idling and high power consumption for implantable devices need to be addressed first.

B. BIOMETRIC AUTHENTICATION

Different types of factors can be used to confirm identity. Facts can be knowledge factors, such as user's secrets, which are verifiable objects possessed by the user, or inherent factors, which are characteristics of the user [89]. Most commercial IoMT devices currently available for monitoring health and well-being, such as smartwatches, use numeric or alphanumeric passwords for authentication, instead of biometric authentication. For IoMT healthcare systems, researchers are exploring the use of biometric inherent factors that are unique to the user, as it is assumed that these factors are more challenging for attackers to compromise, especially in comparison to the short passwords commonly used in smartwatches. Such biometric-based security schemes in IoMT healthcare systems should meet the requirements in Table 3.

A biometric-based security systems often perform two types of actions, namely identification and verification. Identification is the matching of a sample against all the samples in the database, whereas, verification is the matching of an input sample against one person's samples in the database [90]. Fig. 2 is a block diagram illustrating a general biometric authentication system (retrieved from [86]). There are two phases, enrolment phase and matching phase, in the biometric authentication systems. In the enrolment phase, subjects register their raw biometric samples into the database, then, the recorded biometric samples will be processed into a template or a feature vector and stored into the database. In the matching phase, similar process is performed. The subject will be authenticated only if his/her sample matches the templates or the feature vectors of the claimed identity in the database. If not, the authentication attempt will be rejected by the system.

To assess the performance of biometric authentication systems, some likelihood-based performance metrics, as listed in Table 4, are commonly used [88]. A trade-off will be made between False Acceptance Rate (FAR) and False Rejection Rate (FRR) by choosing a decision threshold value t for the biometric authentication systems, as shown in Fig. 3a. If the matching score s is larger or equal than t, the authentication is considered to be successful. If s is smaller than t, the authentication is failed and the person is considered to be an impostor. The higher the decision threshold t is, the more secure the biometric authentication systems are, and t is often chosen based on the security requirements of the applications as shown in Fig. 3b.

Behavioural biometric traits, including signature, voice, gait, ECG, and keystrokes, can be used in IoMT healthcare systems. The strengths and weaknesses of those behavioural biometric traits are summarized in Table 5 [91]. Behavioural biometric traits can often be captured with low-cost hardware, requiring only adequate algorithms for feature extraction, which makes behavioural biometric-based security systems simpler and less costly. Signature and keystroke dynamics are not applicable to IoMT devices in the sensor level, due to the size of the sampling hardware, such as keypad and electronic signature pad. However, they can be used on mobile phones, which are in the personal server level of the IoMT healthcare systems.

On the other hand, a large number of physical biometric traits of humans can also be used for authentication applications. In the recent years, the majority of physical biometric traits have been exploited in biometric security systems, including fingerprint, palm print, face, retina/iris, hand geometry, ear shape, body odour, vein pattern, and DNA, as summarized in Table 6. Every physical biometric trait has its own application scenarios regarding to the security requirement and hardware availability of the systems, as no individual biometric system can perform well in all possible scenarios. In order to achieve a higher level of security, multi-biometric fusion has drawn attentions from many researchers.

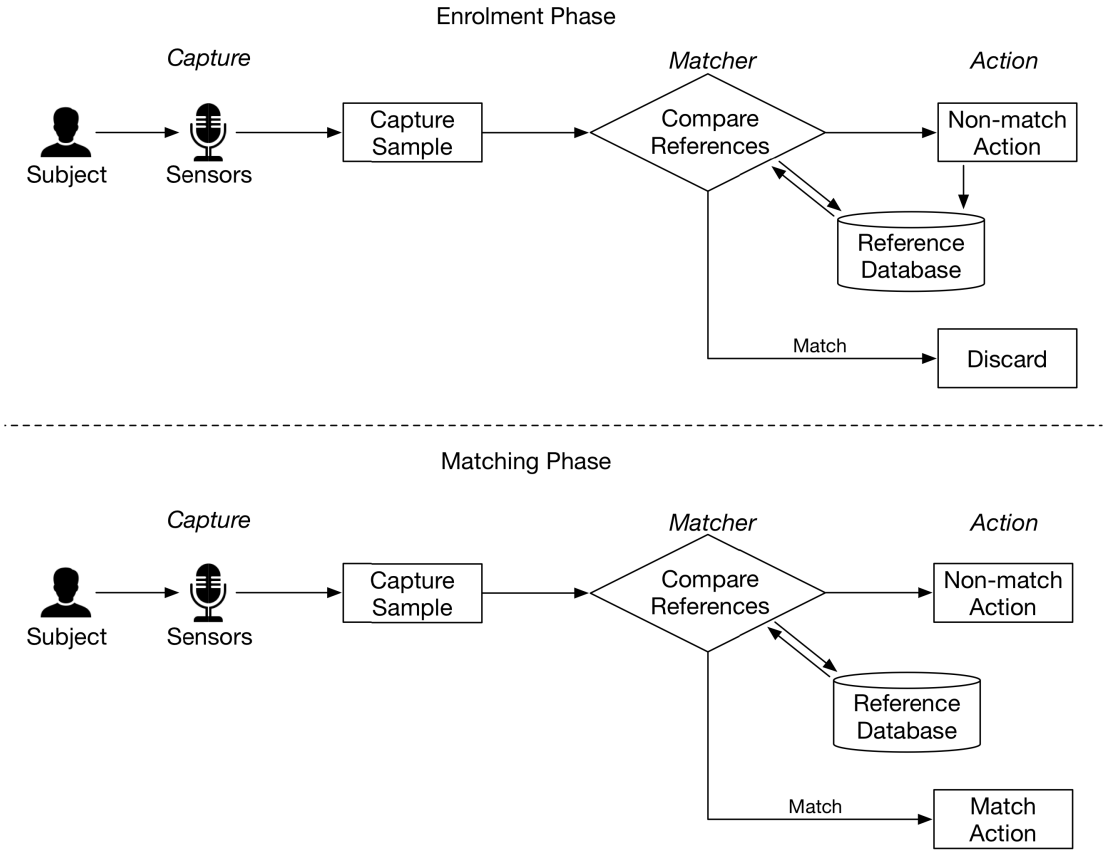


FIGURE 2. Block diagram of general biometric authentication systems [86].

TABLE 4. Common performance metrics in biometric authentication systems [88].

Performance Metrics	Acronym	Explanations
Failure-to-Enrol Rate	FTE	It is the percentage of the subjects who were not able to register their biometrics after several attempts
Failure-To-Acquire Rate	FTA	It is the probability where the system is not able to acquire data or extract template of subjects
False Acceptance Rate	FAR	It is the probability where the system matches the testing sample to non-matching templates
False Rejection Rate	FRR	It is the probability where the system fails to match the testing sample to the matching templates
Equal Error Rate	EER	It is the probability where both FFR and FAR are equal in the ROC curve
Receiver Operating Characteristic	ROC	FAR against FRR

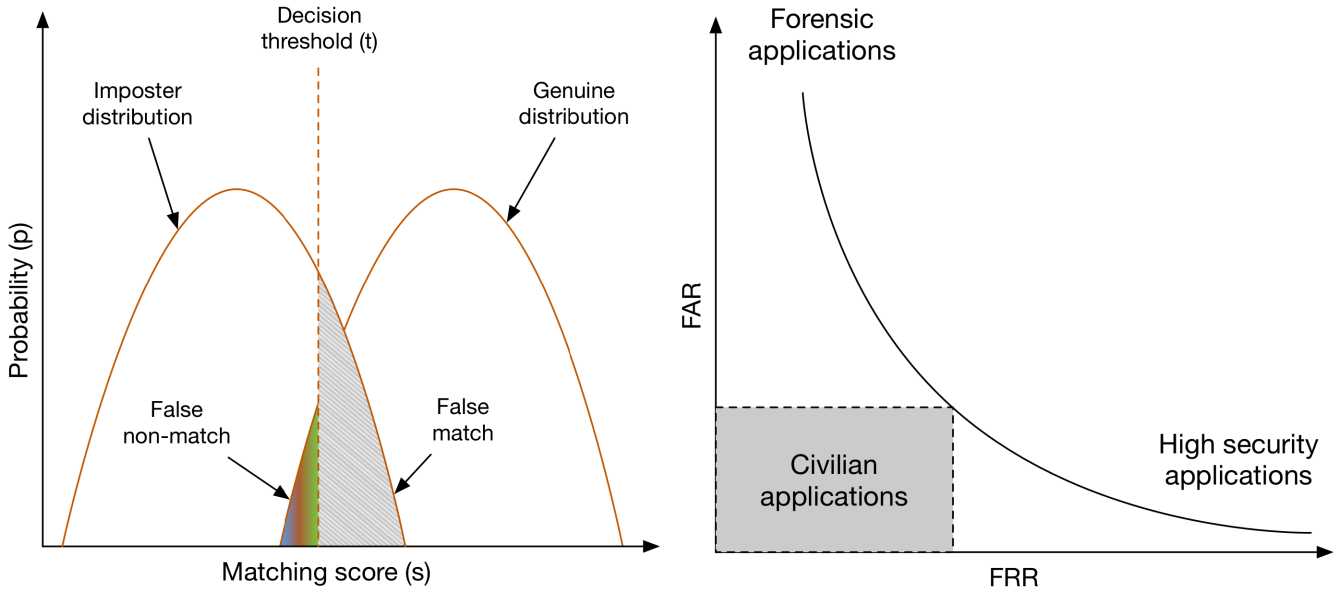
Although physical biometrics has been widely adopted in a variety of security applications, behavioural biometrics is very promising and it can be easily adapted into the current IoMT infrastructures due to its cost efficiency and less processing complexity.

1) HEART RHYTHM OR ELECTROCARDIOGRAM (ECG)

Electrocardiogram can be measured by both wearable and implantable devices, therefore it is often used as security measures for IoMT healthcare systems. Bao et al. [92] first proposed an ECG-based security scheme using grouped Inter-pulse Intervals (IPIs) of heartbeats as the source for key generation. The scheme has been further improved by the group [93] using Error-Correcting Codes (ECC). IPIs can also be accumulated to improve randomness, such as MRE-IPI [94], a new randomness extraction method which can extract Martingale Randomness from IPIs of ECG signals.

2) MOTION AND GAIT

Compare to ECG, gait is a relatively new biometric measurement. Due to the difference in bio-mechanical structure



(a) Probability against matching score

(b) ROC curve

FIGURE 3. Trade-off between FRR and FAR [87].

TABLE 5. Common behavioural biometric traits [91].

Biometric traits	Strengths	Weaknesses
Signature	Can be captured by either a touch pad or a camera	Lack of long-term reliability and accuracy; signatures can be easily imitated
Voice	Only low-cost sensors, such as a microphone, are required	Changes, due to emotion, sick, or misspoken of pass phrase, in the voice degrade the performance of the voice-based biometric systems
Gait	Easily accessible; can be captured by either wearable sensors or cameras	Changes, due to injury, ageing, or on-purpose, degrade the performance of the gait-based biometric systems; longer data collection time comparing to traditional biometrics traits, such as fingerprint, which can be collected in an instant
ECG	Easily accessible by implanted or on-body sensors	Changes, due to cardiac abnormalities, activities, and emotion, in the ECG degrade the performance of the ECG-based biometric systems
Keystroke	Can be captured without user intervention	Require keystroke recording software in either mobile devices or computers; it requires either a keyboard or a touch screen; low recognition rate

and phenotypes, everyone walks differently and by capturing the gait parameters, individual can be identified. Apart from user authentication, device-to-device authentication can also be achieved by using gait parameters, as inertial sensors, embedded in the wearable or implantable devices on the same user, can capture the similar gait parameters when the user walks [95]. A study carried out by Muaaz and Mayrhofer [96] demonstrates that a person's gait inertial signals are very difficult to be imitated, because impersonators often lose their own regularity between steps when mimicking legitimate users. Despite open problems such as gait changes due to ageing and low performance on false agreement rate, gait biometric holds great potentials in cryptographic applications due to its uniqueness, freshness, and availability.

3) VOICE

Instead of using pin numbers, banks have started to use voice recognition for user authentication in their telephone banking services. Due to the structural difference in vocal chords, trachea, nose, teeth and accentuates sounds, one's voice can be as distinctive as his/her fingerprint [97]. Unlike other biometric, voice print does not require physical contact with the scanner/reader and can be taken remotely.

TABLE 6. Common physical biometric traits.

Biometric traits	Strengths	Weaknesses
Fingerprint	Easily accessible	Wet and wrinkled fingers degrade the performance of fingerprint-based biometric systems; necessary measures must be taken to detect forgeries
Palm print	Easily accessible	Wet and wrinkled palms degrade the performance of fingerprint-based biometric systems; the size of a palm print template is much larger than a fingerprint template, requiring larger databases; larger size optical readers are required, which is not feasible to be used in mobile phones or IoT devices
Face	Easily accessible	Require high quality cameras; variation in lights and facial expressions can affect the performance of face-based biometric systems; accessories and masks can also affect the performance; multiple subjects can be authenticated at the same time
Retina/iris	Easily accessible, blood vessel pattern within a retina provides a large set of feature vectors	Require high precision retinal scanners; sunglasses and lens can degrade the performance of retina-based biometric systems; not applicable to miniaturized IoMT devices
Hand geometry	Easily accessible, an adequate amount of features available	Require specific hardware and software, which has not been widely commercialized yet; not applicable to miniaturized IoMT devices
Ear shape	Easily accessible	Ear can be easily covered by hair, hats, and glasses, affecting the performance of ear-based biometric systems
Body odour	Easily accessible; can be easily captured by on-body sensor nodes in BSNs	Deodorants can alter natural body odour, affecting the performance; only a small amount of studies on body odour recognition available
Vein pattern	Provide a large amount of features, thus, high level of security	Require infrared light based special cameras; not very reliable due to the complexity in vein patterns
DNA	Provide a high recognition rate; can be easily obtained via saliva, hair, or blood	Sample processing is complex and expensive; not applicable to miniaturized IoMT devices

Voice authentication methods have been adapted in many IoMT systems in the last decade.

4) ELECTROENCEPHALOGRAM (EEG)

Many wearable EEG sensors have been developed in recent years, and many EEG biometrics-based authentication schemes has been proposed. EEG biometrics is very rich in discriminative information and features in both time and frequency domains. Moreover, EEG biometrics has both unique/time-varying patterns, which may occur when the subject is watching an unique picture (visual stimuli), as well as permanent patterns, which occur regularly. Recently, deep learning approaches have been exploited in EEG biometrics for IoMT healthcare systems, such as [98]. As stated in [99], a person's EEG signals varies from that of another person due to different brain structures, memory, mood, stress, and mental state, mimicking an individual's EEG signals is very difficult to achieve with current technologies.

C. SECURITY SCHEMES FOR IMPLANTABLE IoMT DEVICES

Implantable IoMT devices typically requires surgeries to be implanted into patients' body. Therefore, security schemes for implantable devices have restrict requirements on power consumption, communication overhead, attack resilience, and support for emergency situations [100]. In addition to the aforementioned challenges, security schemes for implantable devices must comply with restrict regulations [101].

1) PROXY BASED PROTECTION

The concept of proxy based implant security is based on a secondary device acting as a ''proxy'' between communications of the implant and external devices. The advantage of this scheme is that it aims to enhance security of existing implanted devices. An example of this is the ''IMD-Shield'' [102]. ''shielding'' is carried out by introducing noise to intercept communication between the implant and any device that attempts to communicate with it. The decoding of implant signal at the proxy is made possible with the knowledge of the generated noise. A security scheme is implemented such that only authenticated communication is relayed to/from the implant. Another proxy based Implantable Medical Device (IMD) protection is the 'IMDGuard'' [103], which is able to share keys between the IMD and the guardian using the owner's ECG signals.

2) DISTANCE BOUNDING

Distance bounding, or proximity based access control, limits attack possibilities by restricting the wireless communication distance between an implant and an external device [104]. One example of this is inductive coupling, which often is limited to a few centimetres. While inductive links inherently operates at shorter distances and are suitable for use with device charging and programming, for data communication it lacks the bandwidth of modern devices. Implant manufacturers have adopted the higher bandwidth MICS (Medical Implant Communication System) which runs in the spectral range of 402-405MHz and signals from the implant are limited to a maximum of 2m. Practically bed-side systems streaming implant data operations at $<$ 1m. Another example of distance bounding authentication through physical layer is [105], which distinguishes legitimate external device and adversary based on the received signal power.

3) ECG BASED ENCRYPTION

Theoretically, ECG signals can be captured by IMDs, therefore, ECG based data encryption schemes have the potentials to be applied for implantable devices. The advantage of using ECG signals as entropy sources for data encryption is that patients are not required to remember passwords, which remove the risks of being stolen. For example, an One-Time-Pad (OTP) encryption scheme proposed in [106], which uses the Inter-pulse Intervals of the ECG signals to encrypt messages between the IMD and the external device. The disadvantages of using ECG signals as entropy sources are as follows: firstly, ECG based security schemes typically require signal collection time, which is not feasible in emergency situations; secondly, distortion and attenuation can be easily introduced to ECG signals due to patients' movement or poor contact between skin and the electrodes of ECG sensors; thirdly, although error collection coding is often used to reduce bit errors, it is not sufficient to eliminate false rejection rate. Although ECG signals can be measured very accurately by an external device, the ECG signals captured by the external device are still different from that of the ECG signals captured by the IMD at a different location.

4) ANALOGUE SHIELDING

Researchers have shown that implants without adequately robust sensor architectures are susceptible to ''analogue attacks'' [107]. Typically, sensors play a pivotal role in a closed loop system such as implanted insulin pumps. The sensor signal is inherently analogue in nature and can be interfered, resulting in incorrect sensor readings and erroneous implant operation [108]. The disturbance of analogue signals, often of small amplitude, from intentional noise injection can be mitigated by following good design practices, such as use shielded cables for data transmission.

5) ZERO POWER COMMUNICATION

This security measure is devised to counter ''power drawing'' attacks where deliberate continuous requests to communicate with the implant are used with the intention to deplete the implant battery. Zero power communication requires all communication from the implant to be initialized by non-battery sources such as piezoelectric RF harvesters [109], also improving patient security awareness by signalling during communication initialization. Zero power communication can also be achieved by radio frequency energy harvesting. For example, a powerless mutual authentication protocol proposed in [110] utilizes Ultra High Frequency (UHF) energy harvester and dynamic encryption keys extracted from ECG signals for securing IMDs. zero power communication can only work when the two devices are in very close proximity, which inevitably limits its applications.

6) ANOMALY DETECTION

Resource depletion attacks, which could sufficiently reduce the battery power of an IMD, can be detected by anomaly detection, by investigating the patterns of communications between a IMD and legitimate external devices. An example of anomaly detection is MedMon [111], in which a smart phone examining physical layer characteristics, such as Received Signal Strength Indication (RSSI) and Time of Arrival (TOA), as well as behavioural characteristics, such as value range and frequency, of the signals to and from IMDs to identify potential malicious communications. A limitation of MedMon is that it only provides IMD integrity protection, therefore, additional security schemes should be used to protect the confidentiality and availability of the implantable devices.

V. DISCUSSIONS

With the internet and wireless connectivity of IoMT technologies, the new generation of medical devices are facing security and privacy challenges aforementioned in this survey. Instead of medical equipment securely installed in hospital wards or laboratories, the new generation of IoMT devices will be worn by or implanted in patients such that they can be monitored continuously. As the majority of the IoMT devices have to handle personal and physiological data of the users, the impact of security attacks on the users could be more direct and severe compare to other IoT systems. For example, wireless connected implantable devices are designed to manage cardiac functions, insulin functions, nerve stimulation, etc. and equipped with electrodes, pumps and other actuators. Malicious attacks on such devices could have life threatening effects on the patients. If only minimal security protection is applied to these medical devices, they can easily be hacked. For example, Radcliffe demonstrated that he can hack into an insulin pump 150 feet away and disable the device or instruct the device to inject excessive amount of insulin [112].

There are always new approaches and methods to attack a network, and administrators have to be constantly updated with patches and anti-virus libraries to protect the systems against malicious attacks. However, unlike computer networks where patches or virus update can easily be injected into the systems, wearable and implantable medical devices

often do not have sufficient network bandwidth and resources to update their firmware regularly [113]. Majority of these health devices cannot be shut down and wait until security experts to find the anti-virus or patches to recover the devices after the attacks. The state-of-the-art security research in IoMT systems are often analyzed in computer simulations, how the security schemes handle the over-the-air updates in real-world scenarios have not been researched thoroughly.

Biometric authentication is another emerging research topic in the field of IoMT security and privacy. However, it has yet to be widely adopted due to the limitations, such as costs of the sensors and low authentication performance. Given the fact that most medical devices capture physiological measurements of the users, there are advantages of applying biometric authentication schemes over other methods. For example, a real-time biometric key authentication can be carried out by comparing physiological measurements of the patient captured by wearable devices with the signals obtained by implanted sensors. Such scenarios occur in many IoMT applications, giving advantages to biometric authentication over other security schemes.

VI. FUTURE RESEARCH DIRECTIONS

With other emerging technologies, such as cloud computing, become popular, there are some interesting future research directions that have not been fully exploited by the IoMT security and privacy research community. The followings are a few example research directions that could potentially be applied for the security and privacy of IoMT healthcare systems.

A. BLOCKCHAIN

Blockchain was developed for securely keeping financial ledger records in a decentralized fashion, so that the ''blocks'' in the blockchain depend on one another. It would also be applied to medical data stored distributively in the medical servers, providing extensively strong security and privacy protection to the IoMT healthcare systems. However, blockchain requires a significant amount of computational resources on the devices to generate blocks, which is infeasible on the resource constraint IoMT devices. On the other hand, blockchain can be used for securing electronic health records stored in the medical servers. An example is MedRec [114], a pioneer research on using blockchain for medical data access and permission management.

B. ARTIFICIAL INTELLIGENCE

Machine learning and deep learning has become the most popular research topics in nearly every industry, including network security. Many machine learning based network intrusion detection methods, such as [115], have been proposed in recent years, and they can also be applied to IoMT healthcare systems. As there is a trend of using deep learning approaches for disease diagnosis in the medical servers, the use of such approaches for security and privacy of the systems should also be taken into consideration. An example research is [116], where PHI in different levels of the IoMT systems are examined by deep learning networks for intermediate attack detection.

C. SECURITY ASSESSMENT

Security research is often carried out by different research groups individually, and there is not a standard on how to measure the security strength of the proposed IoMT security strength. Adversarial analysis is one of the tools for researchers to measure the security level of their research, and yet, these adversarial analysis is not based on the same assumptions and principles, thus cannot be compared together. Therefore, developing a framework for assessing the security and privacy level of security research is of necessity for the IoMT security and privacy community. An example research is IoMT-SAF [117], a web-based IoMT security assessment framework where recommendations can be made based on the input of the users. However this work does not assess the security strength of the existing research and does not provide crypto-analysis for the cryptographic algorithms. Further research is required regarding to assessing security strength of the IoMT healthcare systems.

VII. CONCLUSION

In the last few years, the number of IoMT devices deployed in healthcare systems have grown and expanded rapidly, as a myriad of new wearable and implantable medical devices have been introduced in recent years for healthcare applications, ranging from glucose sensors, insulin pumps, to ingestible core body temperature sensors and drug-eluting stents. These smart devices have facilitated the transformation of healthcare services, enabling personalized and preventative patient care. Although the network connectivity of these IoMT devices greatly eases the control and monitoring functions of the devices, it inevitably causes vulnerabilities of the devices and the network. Similar to other IoT devices and systems, IoMT devices could suffer from same security threats and attacks. Given the fact that the IoMT devices handle highly personal health data and some of the devices have life supporting actuation functions, security attacks on connected health devices could have direct and life-threatening impacts on the users.

Many security schemes developed for IoMT devices could potentially be applied for protecting medical devices, however, due to the size and power constraints, wearable and implantable devices are tended to be built with very limited resources and they may not have sufficient resources to implement those schemes. Ensuring the safety and security of such devices requires new solutions that span across the design space of human, cyber and physical elements. Apart from increasing research efforts in the security and privacy of IoMT devices, close collaboration is needed between the academic, industries and standard agencies to develop new methods, regulations, and standards to ensure the security of this new generation of medical technologies.

ACKNOWLEDGMENT

The authors would like to thank Dr. C. Wong for his contributions to this project.

REFERENCES

[1] K. Rawlinson. (2015). *HP Study Reveals Smartwatches Vulnerable to Attack*. [Online]. Available: https://www8.hp.com/us/en/hp-news/press-release.html?id=2037386

[2] J. A. Evans, "Electronic medical records system," U.S. Patent 5 924 074, Jul. 13, 1999.

[3] D. W. Kravitz, "Digital signature algorithm," U.S. Patent 5 231 668, Jul. 27, 1993.

[4] P. Barrett, "Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1986, pp. 311–323.

[5] F. Jonsson and M. Tornkvist, "RSA authentication in Internet of Things: Technical limitations and industry expectations," KTH Roy. Inst. Technol., Stockholm, Sweden, Tech. Rep. urn:nbn:se:kth:diva-209426, 2017, p. 57.

[6] J. Turner. (2018). *Security for Connected Medical Devices*. [Online]. Available: https://www.medtechintelligence.com/feature_article/security-for-connected-medical-devices/

[7] R. Scammell. (2019). *PCM Data Breach Highlights Risks of Third-Party Cloud Providers*. [Online]. Available: https://www.verdict.co.uk/pcm-data-breach-cloud-providers/

[8] B. Hutchinson. (2018). *87 Million Facebook Users to Find Out if Their Personal Data was Breached*. [Online]. Available: https://abcnews.go.com/US/87-million-facebook-users-find-personal-data-breached/story?id=54334187

[9] N. Garun. (2017). *Yahoo Says all 3 Billion User Accounts Were Impacted by 2013 Security Breach*. [Online]. Available: https://www.theverge.com/2017/10/3/16414306/yahoo-security-data-breach-3-billion-verizon

[10] M. Yao. (2017). *Your Electronic Medical Records Could Be Worth $1000 to Hackers*. [Online]. Available: https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#61a0d42850cf

[11] S. Brooks. (2019). *Can You Trust Healthcare Organisations With Your Digital Wellbeing?* [Online]. Available: https://www.enterprisetimes.co.uk/2019/06/27/can-you-trust-healthcare-organisations-with-your-digital-wellbeing/

[12] N. Pratley. (2019). *British Airways Fine Shows GDPR has Given Watchdogs Teeth*. [Online]. Available: https://www.theguardian.com/business/nils-pratley-on-finance/2019/jul/08/british-airways-fine-shows-gdpr-has-given-watchdogs-teeth

[13] ICO. (2019). *Health and Social Care*. [Online]. Available: https://ico.org.uk/for-organisations/in-your-sector/health/

[14] HHS. (Jul. 2013). *Breach Notification Rule*. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

[15] A. D. Stern, W. J. Gordon, A. B. Landman, and D. B. Kramer, "Cybersecurity features of digital medical devices: An analysis of FDA product summaries," *BMJ Open*, vol. 9, no. 6, 2019, Art. no. e025374.

[16] J. E. Tomasco. (Oct. 2019). *Urgent/11 Cybersecurity Vulnerabilities Could Affect Medical Devices and Hospital Networks*. [Online]. Available: https://www.natlawreview.com/article/urgent11-cybersecurity-vulnerabilities-could-affect-medical-devices-and-hospital

[17] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: how safe are we?" *Brit. Med. J.*, vol. 358, p. j3179, Jul. 2017.

[18] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical Internet of Things: A review," *Secur. Commun. Netw.*, vol. 2018, Mar. 2018, Art. no. 5978636.

[19] P. A. Williams and V. McCauley, "Always connected: The security challenges of the healthcare Internet of Things," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, Dec. 2016, pp. 30–35.

[20] M. A. Sahi, H. Abbas, K. Saleem, X. Yang, A. Derhab, M. A. Orgun, W. Iqbal, I. Rashid, and A. Yaseen, "Privacy preservation in e-healthcare environments: State of the art and future directions," *IEEE Access*, vol. 6, pp. 464–478, 2017.

[21] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of medical things: Taxonomy and risk assessment," in *Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops (LCN Workshops)*, Oct. 2017, pp. 112–120.

[22] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the Internet of Medical Things (IoMT)," in *Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2019, pp. 457–464.

[23] A. Algarni, "A survey and classification of security and privacy research in smart healthcare systems," *IEEE Access*, vol. 7, pp. 101879–101894, 2019.

[24] Y. Sun and B. Lo, "An artificial neural network framework for gait-based biometrics," *IEEE J. Biomed. Health Inform.*, vol. 23, no. 3, pp. 987–998, Aug. 2018.

[25] K.-H. Yeh, "A secure IoT-based healthcare system with body sensor networks," *IEEE Access*, vol. 4, pp. 10288–10299, 2016.

[26] G.-Z. Yang, *Body Sensor Networks*. Springer, 2006.

[27] R. Chakravorty, "A programmable service architecture for mobile medical care," in *Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2006, pp. 1–5.

[28] P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors J.*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[29] M. Shin and I. Joe, "An indoor localization system considering channel interference and the reliability of the RSSI measurement to enhance location accuracy," in *Proc. 17th Int. Conf. Adv. Commun. Technol. (ICACT)*, Jul. 2015, pp. 583–592.

[30] W. Zang and Y. Li, "Gait-cycle-driven transmission power control scheme for a wireless body area network," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 3, pp. 697–706, May 2018.

[31] Q. Tang, N. Tummala, S. K. S. Gupta, and L. Schwiebert, "Communication scheduling to minimize thermal effects of implanted biosensor networks in homogeneous tissue," *IEEE Trans. Biomed. Eng.*, vol. 52, no. 7, pp. 1285–1294, Jul. 2005.

[32] Q. Tang, N. Tummala, S. K. S. Gupta, and L. Schwiebert, "TARA: Thermal-aware routing algorithm for implanted sensor networks," in *Proc. 1st IEEE Int. Conf. Distrib. Comput. Sensor Syst.* Berlin, Germany: Springer, 2005, pp. 206–217.

[33] D. Z. Uslan, M. J. Gleva, D. K. Warren, T. Mela, M. K. Chung, V. Gottipaty, R. Borge, D. Dan, T. Shinn, K. Mitchell, R. G. Holcomb, and J. E. Poole, "Cardiovascular implantable electronic device replacement infections and prevention: Results from the REPLACE registry," *Pacing Clin. Electrophysiol.*, vol. 35, no. 1, pp. 81–87, 2012.

[34] M. Quwaider and S. Biswas, "On-body packet routing algorithms for body sensor networks," in *Proc. 1st Int. Conf. Netw. Commun.*, Dec. 2009, pp. 171–177.

[35] P. Kuryloski, A. Giani, R. Giannantonio, K. Gilani, R. Gravina, V.-P. Seppa, E. Seto, V. Shia, C. Wang, and P. Yan, "DexterNet: An open platform for heterogeneous body sensor networks and its applications," in *Proc. 6th Int. Workshop Wearable Implantable Body Sensor Netw.*, Jun. 2009, pp. 92–97.

[36] X. Liang and I. Balasingham, "Performance analysis of the IEEE 802.15.4 based ECG monitoring network," in *Proc. 7th IASTED Int. Conf. Wireless Opt. Commun.*, 2007, pp. 99–104.

[37] H. Huang, J. Zhou, W. Li, J. Zhang, X. Zhang, and G. Hou, "Wearable indoor localisation approach in Internet of Things," *IET Netw.*, vol. 5, no. 5, pp. 122–126, 2016.

[38] G. Mooney. (2018). *Is HIPAA Compliant With the GDPR?* [Online]. Available: https://blog.ipswitch.com/is-hipaa-compliant-with-the-gdpr

[39] S. Pearlman. (2019). *What is Data Integrity and Why Is It Important?* [Online]. Available: https://www.talend.com/resources/what-is-data-integrity/

[40] T. Bienkowski. (Feb. 2018). *GDPR is Explicit About Protecting Availability*. [Online]. Available: https://www.netscout.com/blog/gdpr-availability-protection

[41] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Med. Syst.*, vol. 36, no. 1, pp. 93–101, Feb. 2012.

[42] T. Nilges, "The cryptographic strength of tamper-proof hardware," Karlsruhe Inst. Technol., Karlsruhe, Germany, Tech. Rep. urn:nbn:de:swb:90-518099, 2015.

[43] B. Halak, M. Zwolinski, and M. S. Mispan, "Overview of PUF-based hardware security solutions for the Internet of Things," in *Proc. IEEE 59th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Oct. 2016, pp. 1–4.

[44] R. Saeedi, J. Purath, K. Venkatasubramanian, and H. Ghasemzadeh, "Toward seamless wearable sensing: Automatic on-body sensor localization for physical activity monitoring," in *Proc. 36th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Aug. 2014, pp. 5385–5388.

[45] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 8, pp. 2661–2674, May 2013.
[46] J. O. Kephart and D. M. Chess, "The vision of autonomic computing," *Computer*, vol. 36, no. 1, pp. 41–50, Jan. 2003.
[47] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.
[48] F. M. de Almeida, A. de Ribamar Lima Ribeiro, and E. D. Moreno, "An architecture for self-healing in Internet of Things," in *Proc. UBICOMM*, 2015, p. 89.
[49] J. Y. Kim, W. Hu, H. Shafagh, and S. Jha, "SEDA: Secure over-the-air code dissemination protocol for the Internet of Things," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 6, pp. 1041–1054, Nov./Dec. 2016.
[50] J. Spacey. (2016). *Backward Compatibility vs Forward Compatibility*. [Online]. Available: https://simplicable.com/new/backward-compatibility-vs-forward-compatibility
[51] M. Bromwich and R. Bromwich, "Privacy risks when using mobile devices in health care," *Can. Med. Assoc. J.*, vol. 188, no. 12, p. 855, 2016.
[52] P. Crilly and V. Muthukkumarasamy, "Using smart phones and body sensors to deliver pervasive mobile personal healthcare," in *Proc. 6th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process.*, Dec. 2010, pp. 291–296.
[53] A. Kogetsu, S. Ogishima, and K. Kato, "Authentication of patients and participants in health information exchange and consent for medical research: A key step for privacy protection, respect for autonomy, and trustworthiness," *Frontiers Genet.*, vol. 9, p. 167, Jun. 2018.
[54] N. A. Azeez and C. Van der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egyptian Inform. J.*, vol. 20, no. 2, pp. 97–108, 2018.
[55] V. L. Raposo, "Electronic health records: Is it a risk worth taking in healthcare delivery?" *GMS Health Technol. Assessment*, vol. 11, pp. 1–9, Dec. 2015.
[56] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, 2006, pp. 89–98.
[57] S. Murugesan and I. Bojanova, *Encyclopedia of Cloud Computing*. Hoboken, NJ, USA: Wiley, 2016.
[58] S. de Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in *Proc. 33rd Int. Conf. Very Large Data Bases*, 2007, pp. 123–134.
[59] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1998, pp. 127–144.
[60] R. Kumar and R. Mukesh, "State of the art: Security in wireless body area networks," *Int. J. Comput. Sci. Eng. Technol.*, vol. 4, no. 5, pp. 622–630, 2013.
[61] A. Boukerche and Y. Ren, "A secure mobile healthcare system using trust-based multicast scheme," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 387–399, May 2009.
[62] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.
[63] G. Kumar, "Understanding denial of service (DoS) attacks using OSI reference model," *Int. J. Educ. Sci. Res.*, vol. 1, no. 5, pp. 1–8, 2014.
[64] N. Sufyan, N. A. Saqib, and M. Zia, "Detection of jamming attacks in 802.11b wireless networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 1, p. 208, 2013.
[65] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.
[66] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 662–675, Mar. 2017.
[67] Y. Yang, X. Zheng, and C. Tang, "Lightweight distributed secure data management system for health Internet of Things," *J. Netw. Comput. Appl.*, vol. 89, pp. 26–37, Jul. 2017.
[68] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and secured medical data transmission and analysis for wireless sensing healthcare system," *IEEE Trans. Ind. Informat.*, vol. 13, no. 3, pp. 1227–1237, Jun. 2017.
[69] A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston, and Y. Zhang, "Anonymous authentication scheme for smart cloud based healthcare applications," *IEEE access*, vol. 6, pp. 33552–33567, 2018.
[70] A. Vaniprabha and P. Poongodi, "Augmented lightweight security scheme with access control model for wireless medical sensor networks," *Cluster Comput.*, vol. 22, no. 5, pp. 12495–12505, 2019.
[71] X. Liu and W. Ma, "ETAP: Energy-efficient and traceable authentication protocol in mobile medical cloud architecture," *IEEE Access*, vol. 6, pp. 33513–33528, 2018.
[72] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena, "LSCSH: Lattice-based secure cryptosystem for smart healthcare in smart cities environment," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 24–32, Apr. 2018.
[73] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "Privacyprotector: Privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 163–168, Feb. 2018.
[74] M. Elhoseny, G. Ramirez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for iot-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.
[75] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145, Jun. 2018.
[76] A. Gupta, M. Tripathi, T. J. Shaikh, and A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wearable devices," *Comput. Netw.*, vol. 149, pp. 29–42, Feb. 2019.
[77] A. Ostad-Sharif, D. Abbasinezhad-Mood, and M. Nikooghadam, "A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications," *J. Med. Syst.*, vol. 43, p. 10, Jan. 2019.
[78] R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, "Lightweight privacy-preserving identity-based verifiable IoT-based health storage system," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8393–8405, Oct. 2019.
[79] R. Boussada, B. Hamdane, M. E. Elhdhili, and L. A. Saidane, "Privacy-preserving aware data transmission for IoT-based e-health," *Comput. Netw.*, vol. 162, Oct. 2019, Art. no. 106866.
[80] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Inf. Sci.*, vol. 479, pp. 567–592, Apr. 2019.
[81] X. Cheng, Z. Zhang, F. Chen, C. Zhao, T. Wang, H. Sun, and C. Huang, "Secure identity authentication of community medical Internet of Things," *IEEE Access*, vol. 7, pp. 115966–115977, 2019.
[82] S. Guennouni, A. Mansouri, and A. Ahaitouf. (2019). *Biometric Systems and Their Applications*. [Online]. Available: https://www.intechopen.com/online-first/biometric-systems-and-their-applications
[83] J. Voris, N. Saxena, and T. Halevi, "Accelerometers and randomness: Perfect together," in *Proc. 4th ACM Conf. Wireless Netw. Secur. (WiSec)*, 2011, pp. 115–126.
[84] Y. Sun and B. Lo, "Random number generation using inertial measurement unit signals for on-body IoT devices," in *Proc. Living Internet Things, Cybersecur. IoT*, 2018, pp. 1–9.
[85] K. Wallace, K. Moran, E. Novak, G. Zhou, and K. Sun, "Toward sensor-based random number generation for mobile and IoT devices," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1189–1201, Dec. 2016.
[86] K. Dharavath, F. A. Talukdar, and R. H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res.*, Dec. 2013, pp. 1–7.
[87] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Secur. Privacy*, vol. 1, no. 2, pp. 33–42, Mar. 2003.
[88] D. Thakkar. (2017). *Biometric Performance Metrics Can Help You Select the Right Biometric Solution*. [Online]. Available: https://www.bayometric.com/biometric-performance-metrics-select-right-solution/
[89] D. Turner. (2016). *Digital Authentication—The Basics*. [Online]. Available: https://www.cryptomathic.com/news-events/blog/digital-authentication-the-basics
[90] A. Goode. (2018). *Biometric Identification or Biometric Authentication?* [Online]. Available: https://www.veridiumid.com/blog/biometric-identification-and-biometric-authentication/
[91] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: A survey and classification," *Int. J. Biometrics*, vol. 1, no. 1, pp. 81–113, 2008.

[92] S. D. Bao, C. C. Y. Poon, Y. T. Zhang, and L. F. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *IEEE Trans. Inf. Technol. Biomed.*, vol. 12, no. 6, pp. 772–779, Nov. 2008.
[93] S. D. Bao, Z. K. He, R. Jin, and P. An, "A compensation method to improve the performance of IPI-based entity recognition system in body sensor networks," in *Proc. 35th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2013, pp. 1250–1253.
[94] H. Chizari and E. C. Lupu, "Extracting randomness from the trend of IPI for cryptographic operators in implantable medical devices," *IEEE Trans. Dependable Secure Comput.*, to be published.
[95] Y. Sun, C. Wong, G.-Z. Yang, and B. Lo, "Secure key generation using gait features for body sensor networks," in *Proc. IEEE 14th Int. Conf. Wearable Implantable Body Sensor Netw. (BSN)*, May 2017, pp. 206–210.
[96] M. Muaaz and R. Mayrhofer, "Smartphone-based gait recognition: From authentication to imitation," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3209–3221, Nov. 2017.
[97] M. Khitrov, "Talking passwords: Voice biometrics for data access and security," *Biometric Technol. Today*, vol. 2013, no. 2, pp. 9–11, 2013.
[98] Y. Sun, F. P.-W. Lo, and B. Lo, "EEG-based user identification system using 1D-convolutional long short-term memory neural networks," *Expert Syst. Appl.*, vol. 125, pp. 259–267, Jul. 2019.
[99] Q. Gui, Z. Jin, W. Xu, M. V. Ruiz-Blondet, and S. Laszlo, "Multichannel EEG-based biometric using improved RBF neural networks," in *Proc. IEEE Signal Process. Med. Biol. Symp. (SPMB)*, Dec. 2015, pp. 1–6.
[100] N. Ellouze, M. Allouche, H. B. Ahmed, S. Rekhis, and N. Boudriga, "Security of implantable medical devices: Limits, requirements, and proposals," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2475–2491, 2014.
[101] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao, and K. Saleem, "Ideas and challenges for securing wireless implantable medical devices: A review," *IEEE Sensors J.*, vol. 17, no. 3, pp. 562–576, Feb. 2017.
[102] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 2–13, Aug. 2011.
[103] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862–1870.
[104] H. Kilinc and S. Vaudenay, "Contactless access control based on distance bounding," in *Proc. Int. Conf. Inf. Secur.* Cham, Switzerland: Springer, 2017, pp. 195–213.
[105] Z. E. Ankaral, A. F. Demir, M. Qaraqe, Q. H. Abbasi, E. Serpedin, H. Arslan, and R. D. Gitlin, "Physical layer security for wireless implantable medical devices," in *Proc. IEEE 20th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Sep. 2015, pp. 144–147.
[106] G. Zheng, G. Fang, R. Shankaran, and M. A. Orgun, "Encryption for implantable medical devices using modified one-time pads," *IEEE Access*, vol. 3, pp. 825–836, Jun. 2015.
[107] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2013, pp. 145–159.
[108] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 524–539.
[109] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2008, pp. 129–142.
[110] N. Ellouze, M. Allouche, H. Ben Ahmed, S. Rekhis, and N. Boudriga, "Securing implantable cardiac medical devices: Use of radio frequency energy harvesting," in *Proc. 3rd Int. Workshop Trustworthy Embedded Devices*, 2013, pp. 35–42.
[111] M. Zhang, A. Raghunathan, and N. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Trans. Biomed. Circuits Syst.*, vol. 7, no. 6, pp. 871–881, Dec. 2013.
[112] D. Kaplan. (2011). *Black Hat: Insulin Pumps can be Hacked.* [Online]. Available: https://www.scmagazine.com/black-hat-insulin-pumps-can-be-hacked/article/559187/
[113] T. Olavsrud. (2016). *Connected Medical Device Makers Need to Step Up Security*. [Online]. Available: https://www.cio.com/article/3102918/connected-medical-device-makers-need-to-step-up-security.html
[114] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.
[115] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proc. 9th EAI Int. Conf. Bio-Inspired Inf. Commun. Technol. (BIONETICS)*, 2016, pp. 21–26.
[116] P. M. Shakeel, S. Baskar, V. R. S. Dhulipala, S. Mishra, and M. M. Jaber, "Maintaining security and privacy in health care system using learning based deep-Q-networks," *J. Med. Syst.*, vol. 42, no. 10, p. 186, 2018.
[117] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, "IoMT-SAF: Internet of medical things security assessment framework," *Internet Things*, vol. 8, Dec. 2019, Art. no. 100123.

YINGNAN SUN received the B.Eng. degree (Hons.) in electronics from the University of Liverpool, U.K., in 2015, and the M.Sc. degree in Internet engineering from the Department of Electronic Engineering, University College London, U.K., in 2016. He is currently pursuing the Ph.D. degree with the Department of Computing, Imperial College London, U.K. His current research interests include deep learning, wearable security, the Internet of Things, big data, and biometrics.

FRANK P.-W. LO received the B.Eng. degree (Hons.) in biomedical engineering from The Chinese University of Hong Kong, Hong Kong, in 2015, and the M.Phil. degree in biomedical engineering from the Department of Electronic Engineering, The Chinese University of Hong Kong, Hong Kong, in 2017. He is currently pursuing the Ph.D. degree with the Department of Surgery and Cancer, Imperial College London, London. His current research interests include deep learning, image classification and segmentation, depth estimation, 3D reconstruction, signal processing, blind source separation, and volume estimation.

BENNY LO received the B.A.Sc. degree in electrical engineering from The University of British Columbia, Canada, the M.Sc. degree (Hons.) in electronics from King's College London, and the Ph.D. degree in computing from Imperial College London. He is currently a Senior Lecturer with the Hamlyn Centre and the Department of Surgery and Cancer, Imperial College London. His researches mainly focus on body sensor networks (BSN) and wearable technologies for healthcare and wellbeing. As one of the pioneers in BSN, he has introduced numerous new platform technologies, novel approaches for wellbeing, and healthcare applications. He has published over 150 peer-reviewed publications in the field of BSN. His work has led to numerous awards, such as the Medical Futures Award. He is an Associate Editor of the IEEE JOURNAL OF BIOMEDICAL HEALTH INFORMATICS, the Chair of the IEEE EMBS Wearable Biomedical Sensors and Systems Technical Committee, and a member of the IEEE EMBS Standards Committee.