Security and Privacy in IoT Smart Healthcare

Sivanarayani M Karunarathne
Department of Computing and Informatics
Bournemouth University
Poole, United Kingdom
nara_cha@ymail.com

Neetesh Saxena
School of Computer Science and Informatics
Cardiff University
Cardiff, United Kingdom
nsaxena@ieee.org

Muhammad Khurram Khan
Computer & Information Assurance College
King Saud University
Kingdom of Saudi Arabia
mkhurram@ksu.edu.sa

Abstract— **Patient care is a key element of healthcare practices. The use of Healthcare IoT could enhance the lives of patients and the quality of services provided by medical practitioners, nurses, clinicians, pharmaceutical companies and government in general. Wireless healthcare monitoring systems tremendously used in hospitals and other healthcare practices and witnessed as a revolution in the medical field. Nevertheless, security and privacy for interconnected things are mostly overlooked on the Internet of Things paradigm. In the context of healthcare and remote health monitoring, it is crucial a systematic approach for security and privacy measures must be used in device manufacturing, interconnecting things, communication, data handling and storage, and destruction of such devices and data. This paper examines the current state of security and privacy of the Internet of Things in the healthcare system, the challenges encountered in implementing security frameworks and advocates security and privacy solutions.**

Keywords—Security, privacy, Healthcare IoT

I. Introduction

The integration of the Internet of Things (IoT) has influenced the quality of life in various ways by producing meaningful insights, productivity, and cost-effectiveness. Healthcare introduces IoT to improve patient monitoring, reduce cost, and foster innovation in patient care. While the integration of IoT in the manufacturing and consumer sector is referred to as industry 4.0, medicine 4.0 and Health 2.0 are boomed in the field of healthcare. This has enabled novel solutions for remote monitoring, independent assistive solutions, administering medications, devising early warning and proactive treatment plans, asset management, and maintenance of medical equipment.

Remote patient monitoring is one of the key areas in Healthcare IoT (HIoT) that saves millions of lives and money whilst other functionalities remain equally important for healthcare. In this context, it is prevalent that Wireless Body Sensor Networks (WBSN) is the core HIoT technology integrated into the healthcare sector. As discussed by Qadri *et al.* [1], HIoT is widely used in the form of fitness tracking wearables. However, the potential use of IoT in healthcare is massive and could be effectively utilized for early warning, diagnostics, and effective treatments. When it comes to IoT for medical device integration, the focus is shifted towards the consumer ends, such as Continuous Glucose Monitoring (SGM), blood pressure cuffs, ingestible sensors, connected inhalers and other devices designed to record data on patient vital signs. The recent Apple Watch with Parkinson's disease symptom detectors is another addition to the same type. Sensors and actuators in WBAN are connected to the patient's body based on the type of disease and data requirement of caregivers. It enables healthcare providers to automatically collect information and apply decision support rules to allow for earlier intervention in the treatment process.

Security and privacy measures for HIoT systems are paramount for patient's safety, effective treatment and to ensure the privacy of the patients. Conversely, the majority of security breaches and data privacy issues are reported in the medical sector [2]. Medical data is highly threatened by malware and human interventions for financial benefits and theft of personal sensitive medical data for third party use. Surprisingly, many of the current states of the art IoT solutions are not adopting adequate importance and time for employing security and privacy architectures. This results in critical security loopholes and privacy concerns of sensitive personal data. Further, a study by the Aruba research agency [2] states, IoT related security breaches exceeds 84% in 2019. Most of the devices used in IoT are designed to consume low energy, limited processing, and storage capabilities and lack of user-friendly interfaces adds complexity and leads engineers to overlook IoT security. Making security the enabler of safe and protected data transfer, exchange, and use, is fundamental to using this technology and preserving privacy [3] primarily in healthcare.

Machine learning, blockchain, big data analytics, edge computing, biometric, and nanotechnologies are no longer restricted to the application of a particular domain or a specific application. Instead, these technologies could be integrated into an array of solutions, including security and privacy solutions for IoT. Hence, the authors in this study are investigating the existing security solutions, privacy-preserving frameworks, and mechanisms for HIoT. As the functionalities of the HIoT is vast, authors primarily focus on remote patient monitoring solutions and discuss the applications of the above listed emerging technologies in the same context. Besides, the authors also discuss future directions towards achieving secured and privacy-preserving novel solutions for HIoT.

This work has our three-fold contribution as follows. (1) We examined the current state of security and privacy in terms of technical and unique challenges encountered in implementing healthcare IoT frameworks. (2) We evaluated existing security and privacy solutions inline with the HIoT technical requirements and identified key gaps. (3) We proposed an architecture and reflected on lessons learned and future research directions.

II. Motivating Scenario and Scope

IoT is redefining experiences between people and machines. A new generation of innovations in technology and IoT are integrated into the healthcare sector that plays a significant role in helping save millions of pounds each year. Remote patient monitoring, independent living, clinical trials, and supply chain are a few of the areas IoT is integrated into the healthcare sector. The IoT integration benefits doctors, patients, and healthcare workers in smart hospitals, smart home care, and robot surgeons. Big data collected from millions of IoT devices provide a powerful impact on all levels associated with medical care for data analytics and predictive care using machine learning solutions. However, the majority of security breaches and data privacy issues are reported in the medical sector [2]. Therefore, it is imperative to adopt sufficient security measures to secure the medical systems, infrastructure, and protect the privacy of patient's sensitive personal data. Table I illustrates a few scenarios related to privacy issues faced in healthcare IoT.

TABLE I. SECURITY VULNERABILITIES AND ATTACKS IN HIOT SYSTEMS

Scenario 1	It is reported infusion pumps manufactured by Hospira had security vulnerabilities and allowed an unauthorized user to alter the dose the devices deliver [4]. The security vulnerability came to light when the late hacker Barnaby Jack hacked into his insulin pump potentially to drip a lethal dose of insulin [5].
Scenario 2	Two Austrians meddled with the pain management infusion pumps and the overdose caused respiratory problems but could be fatal [4].
Scenario 3	FDA also warned that two pacemaker programmer models are at risk as outsiders can adjust the pacemaker setting in a patient via internet connection [4].

In this paper, the authors examine the current state of security and privacy of the IoT systems in healthcare, the challenges encountered, and advocate security and privacy solutions using emerging technologies.

III. OUR APPROACH TO THE WORK

Our approach to this study is fundamentally surveying the existing literature (used qualitative research methods with secondary data sources) on security solutions and privacy-preserving mechanisms for HIoT. Thereafter, the authors plot to investigate how complementing novel technologies such as edge computing, machine learning, and Artificial Intelligence (AI), blockchain, biometric technologies, and nanotechnologies contribute to enhance security and privacy measures of HIoT applications. Authors thereafter discuss the future directions for highly secured sophisticated security architecture, privacy-preserving solutions, challenges encountered when implementing such solutions in healthcare.

Section IV of this paper discusses the system model, technical requirements, and challenges encountered in HIoT. Section V discusses the present literature on security and privacy solutions, technologies, and challenges for HIoT. Further, Section VI examines the novel technologies that could complement an enhanced security and privacy framework for HIoT. This section also discusses the challenges of implementing such solutions in the real world. Section VII discusses the proposed security and privacy solutions for HIoT. Finally, Section VIII of this work discusses the future research directions and conclusion.

This study provides real-world scenarios, incidents, security breaches, and challenges encountered. The authors' contributions in this work are summarised as follows.

1. Examined the current state of the security and privacy of the IoT-based healthcare systems and identified current issues and challenges.
2. Identified key functional requirements along with security and privacy requirements for an IoT-based healthcare system.
3. Identified the pros and cons of the existing solutions and proposed an architecture adhering the best practice solutions.

IV. SYSTEM MODEL AND HIOT TECHNICAL REQUIREMENTS

A. System Model

HIoT significantly contributes to the quality of healthcare products, services, and patient-focused personalized treatments. Most of the patient-focused devices are sensors or microchips enabled. A three-tier architecture of a smart healthcare system is depicted in Figure 1.

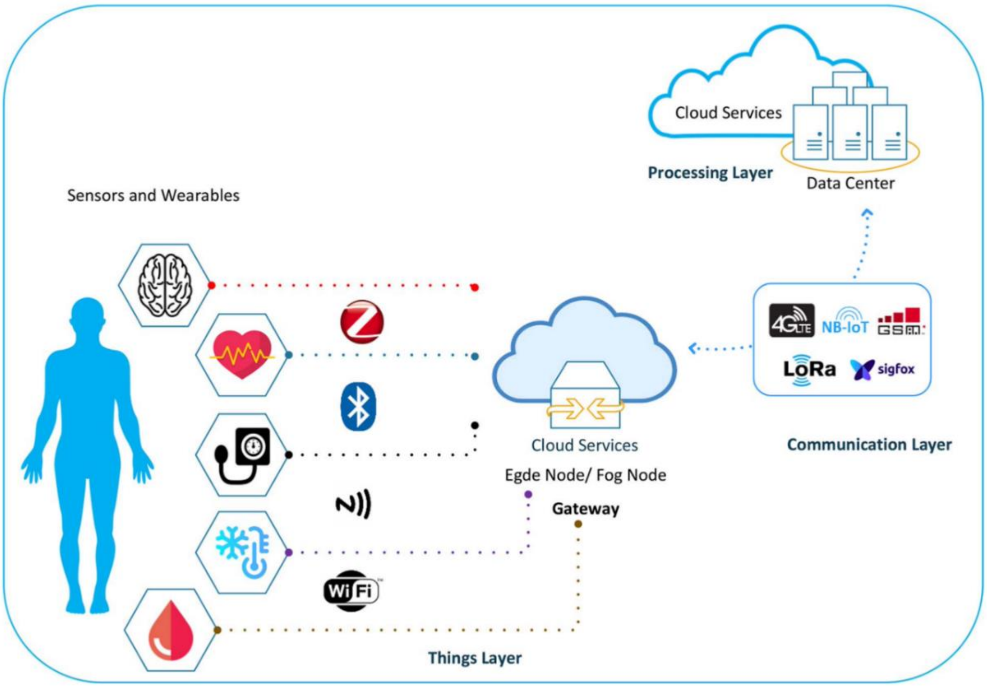

Fig. 1. The three-tier architecture of the IoT healthcare system [1].

TABLE II. HEALTHCARE IoT (HIoT) FUNCTIONALITIES

Remote health monitoring	Help the doctors and healthcare workers remotely monitor the patient's health. Data collected from remote monitoring devices help medical workers respond to emergencies, analyze patient health, prescribe context-based personalized medication, and update suppliers about patient needs. Examples include respiratory and asthma monitors, heart rate monitors, and insulin monitors.
Body wearables devices for self-assistance and monitoring	Assist patients and the medical team constantly comprehend the health condition, monitor health remotely, individuals take precautions based on wearable gadget readings, and medical team and care workers respond to emergencies. Examples include fitness trackers, heart rate trackers other health monitoring devices.
Personalized patient medicine infusing	The demand and supply of medication can be automated using patient-focused medicines. This is implemented using wearable IoT devices. An example includes IoT enabled insulin infusers and IoT based asthma inhalers.
Maintenance of medical equipment	The efficient maintenance of medical equipment saves lives and money. The data collected, faults reported, and track of usage help the maintenance team provide support in advance effectively.
Medical asset management	Beds, medical equipment and other assets must be easily trackable to respond to emergencies, reduce cost on asset management, and to provide a better medical care experience to patients.

Sensors and wearables healthcare devices send medical data to gateway using cloud services with edge or node computing via communication technologies such as Bluetooth, Zigbee and WiFi. This is then further transferred to the data center through the processing layer via wide-area communication technologies such as 4G LTE, LoRaWAN and NB-IoT. This large amount of data is processed and analyzed at the data center and then individual data is shared with the respective patient. Further, the key functionalities of an HIoT are listed in Table II. As specified in the scope of the study, the authors primarily focus on a remote patient monitoring system for the study. The security of IoT infrastructure and the privacy of patient data collected in healthcare is paramount. However, due to the processing capabilities, low power, and other limitations in the IoT devices, the security infrastructure of smart healthcare systems is overlooked and resulted in numerous security breaches.

B. Technical Requirements and Challenges

Medical IoT devices and Wireless Medical Sensor Networks (WMSN) have become of great importance in healthcare systems in the recent past. The static and dynamic sensitive personal data collected from devices must be safeguarded and unauthorized access to such data must be prevented by implementing strong authentication, authorization mechanisms, configuration controls, encryption, and use of standard protocols [3]. Nevertheless, data security and privacy have been an issue that is being overlooked in IoT.

The major challenge in implementing security measures for Healthcare IoT (HIoT) is the devices that enter through various channels to the HIoT network systems. For example, Bring Your Own Device (BYOD) is one of such devices in HIoT. Unlike other systems, IoT devices run on different operating systems and their capabilities vary. These devices may not have common security controls including strong passwords, authentication mechanisms, encryption, hardware, updated firmware, and software. Integrating such devices to smart hospital systems and IoT networks poses security threats to the whole network. Cyber and IoT network security researchers [5] have identified security vulnerabilities in medicine infusion devices that could harm patient health and safety, and also pose threats to medical records and hospital networks. A vast number of heterogeneous devices are connected to the internet via hospital networks without passwords or encryption. Hackers could target individuals to disable their device and remove life-saving care, launch a widespread attack across a particular kind of device, or steal data.

1) Security Requirements: The WMSN aims to protect the sensor nodes and the network from malicious attacks from internal or external environments promptly. Hence, the core security requirements of MWSN in a healthcare system are the counter-measures related to the top 10 security vulnerabilities listed by the Open Web Application Security Project (OWASP) [7]. The formidable requirement is the shift of mindset about security in a smart system. The research proposes a three-step process to adopt security measures as described: 1) assess security impact, 2) apply a multifaceted approach, and 3) define life cycle control across device and data lifecycle. Michael Gareth et al. [8], list the critical security requirement of a HIoT system in Table III.

2) Privacy Requirements: According to the Information Commissioners Office (ICO), UK, there is an alarming number of privacy violations that happened in the healthcare sector. ICO illustrates the number of data security incidents reported in healthcare. Healthcare sector deals with sensitive personal data that are not limited to static information, but also dynamic behavioral information collected via sensors that reveals the personal life of an individual. Exposing such information pertains to high risk and considered a severe breach of data protection. Table IV lists how privacy measures can be implemented across all horizontal layers in an HIoT framework. Presumably, the things layer or sensor devices have challenges implementing security and privacy due to power and processing capabilities.

Healthcare sensitive data is generally sensitive in nature that falls under three categories: explicit identifiers, quasi-identifiers, and privacy attributes. Explicit identifiers represent any personally identifiable information in health records, such as any ID, serial number, patient name, and contact details. Quasi-identifiers are a set of attributes that can derive unique personal information, such as ZIP code, age, and birth records. Privacy attributes represent any specific identifiable information about a person such as any health sickness, disability, and salary. Random perturbation and data anonymous methods such as k-anonymity, l-diversity, and confidence bounding, are usually used to resolve these issues. However, traditional-anonymity does not apply constraints on classified data, hence it can lead to privacy leakage as attackers can perform background knowledge attacks to identify data with these.

C. Associated and Unique Provisioned Challenges of HIoT

The nature of challenges in HIoT is associated with multiple and interconnected devices [3]. They are related to power sources and scalability, interoperability, reliability and security, biocompatibility, vulnerability, the regulatory environment of healthcare, integration, privacy, and security.

1) Power sources and scalability: Sensor devices are generally restricted in power and processing capabilities. The scalability of the application is restricted based on the sensor nodes' ability to meet the operational energy requirement. For example, an ingestible sensor may require hours and years for the wearable and environmental sensor. However, the current technology of available power narrates power sources in batteries for data transmission and processing. Nevertheless, there is a growing trend in improving battery power by adopting solar, fuel, thermal, and biochemical power cells. It is transparent that new technologies are evolving to consume less power for processing, lightweight message protocols, and low power radio modules for data transmission.

2) Interoperability: Medical sensor nodes come from different manufacturers, platforms, APIs, functionalities, hardware, default security configurations, network support, and capabilities. The interoperability of a vast collection of such smart sensor devices in a smart hospital, smart home, or smart social care system is chaotic and paramount. It requires a refined IoT architecture with extra layers of security measures and support.

3) Reliability and security: The reliability and security of data collected, transferred and stored vary based on healthcare applications. However, critical healthcare data must be protected from vulnerabilities in different layers of IoT architecture. Consequently, it increases the payload, power consumption, and scalability of the application. The challenge is finding the right hardware, software, and storage platform based on application needs to ensure reliability, robustness, and security of medical sensor networks and data.

4) Durability: The durability of medical sensors that are body-worn or environmental sensors are controversial and are prone to damage by accidents, sweat, rain, wind, vandalism, the friction of cloth and abrasion with body parts or other objects. It is challenging for manufacturers to give due care to durability to make the devices survive for a more extended period regardless of the conditions specified above.

TABLE III. KEY SECURITY REQUIREMENTS

	Key security requirements that ensure privacy and integrity
Data confidentiality	Unauthorize users and eavesdropping must be prevented in multi-sensor networks such as WBAN and environmental sensors in smart healthcare systems. Data confidentiality should be implemented as the primary goal as exposing data could let the attackers correlate the information about the individual and cause risk. The common approach used to ensure data confidentiality is to use ciphers to encrypt the data [8].
Data integrity	The data received at the endpoint must be consistent and free from meddling by malicious attacks or accidental communication errors during transmission. Cryptography based integrity checks are one form of ensuring the integrity of data. Commonly used crypto-algorithms include AES128/256, MD5, SHA, and S-box [8].
Authentication	The identity of sensor nodes and aggregators is required to ensure the authenticity of the patient and the medical team. Various approaches to ensure authentication can be used including the exchange of authentication keys, digital signatures, and digital certificates. Authentication helps to protect against attacks related to forgery and masquerading healthcare electronic records (EHR) and Personal health records (PHR) [8].
Non-repudiation	Guarantees that a sensor node cannot deny sending a message it previously sent. Nonrepudiation can be implemented using digital signatures paired with public key infrastructures [8].
Authorization	Authorization guarantees access rights and only approves the right nodes and users to access the EHR, PHR, and other network services or files. This could be established by defining the right access control to the right user at the software application level [8].
Freshness	Replay attacks could be prevented by ensuring the freshness of the data received. This includes verifying the data received from the medical sensors are current, ordered, and non-duplicated. Freshness is normally implemented through the use of sequence numbers and timestamps in the packets transmitted by the sensor [8].

TABLE IV. HOW TO ENSURE PRIVACY IN HIoT [10]

Confidentiality policy for everyone who deals with specific data	Design a healthcare context-based confidentiality policy and extend the application of such policies to associated partners as well.
Comprehensive training for staff	Train clinical staff, medical practitioners on privacy preservation practices, and applicable data protection regulations and legislations.
ISO security and privacy standards **ISO 25237:2017** **ISO/IEC 27701** **ISO/IEC 27002**	The listed International Organization for Standardization (ISO) standard provides various techniques including pseudo-randomization to anonymize the data in the health domain. Adapting the standards allows the patients to trust in e-Healthcare enterprises while also allowing for healthcare record sharing for research without compromising privacy.
Secure storage and security	Ensure all EHR and PHR are securely stored and sufficient security measures are in place such as authentication, authorization, accountability, and encryption. ISO/ International Electrotechnical Commission (IEC) 27002 is one of such measures in place for healthcare.
Privacy-preserving access control	Introduce strict access control policies that are proven as the best way to access information [10]. Sahi *et al.*, state, it is advisable to implement a hybrid privacy policy in which a combined approach of anonymization and access control to hide the user's identity while controlling the flow of information. This hybrid approach could solve privacy issues related to PHI and EHR (i.e., preventing unauthorized access to PHI, storing and handling data in an anonymized manner, and sharing data with outside third parties without compromising patient privacy) [10].

5) Biocompatibility: As the MWSN rapidly grows, the research carried out in the biocompatibility of medical sensing devices is becoming essential and challenging. The side effects of using wearable body sensor networks are unknown. However, there are allergic reactions to sensor material and long-term sensor contact to the body could cause skin irritation. For example, ECG electrodes must be replaced after 7-10 days of direct skin contact to minimize skin irritation.

6) Privacy and data ownership: Personal sensitive data must be protected especially in the healthcare industry. EHR and PHR require privacy preservation while at rest, processing, and transit. Countries' laws and regulations must be fully obeyed, and security measures must be in place to ensure data ownership and privacy of collected data using various medical sensors. Data ownership is an issue when transferring data between two parties. In the health domain, it is essential to ensure data ownership when storing data in the cloud platform, sharing data between medical suppliers and transfers.

V. Related Work

Security and privacy of IoT solutions are imminent but mostly flouted. Authors in this study investigate existing literature on security and privacy measures in HIoT and its deceptions to embrace trending technologies that enable highly secure systems.

Wazid et al. [11] discuss secure key management and user authentication mechanism for an IoT environment that uses fog computing. The two-part security mechanism is called SAKA-FC, and it has three-factor key management and user authentication protocol. The key management is dealt with by establishing secure communication using a pairwise secret key management procedure between the IoT devices and fog servers, and between fog servers and cloud servers. It uses a combination of password, biometric, and mobile authentication to strengthen security. The second part generates and uses a mutual authentication-based session key after a legal user registration to ensure the security between users and IoT devices. SAKA-FC uses an efficient one-way cryptographic hash function, bitwise XOR computations for the IoT devices. Further, the Elliptic Curve Point multiplication and biometrics fuzzy extractor method are applied for users and fog servers. SAKA-FC considers CK Advisory model in addition to the DY model. Authors [11] also states that the SAKA-FC session key-based solution provides enhanced security compared to the formal approach that uses the AVISPA tool. They also argue that the SAKA-FC is resilient against replay and man-in-the-middle attacks, fog server impersonation, user impersonation, smart device impersonation, and offline password guessing. It also prevents ephemeral secret leakage (ESL) and preserves anonymity and untraceability.

Wazid et al. [12] in another study, discuss the security of implantable medical devices (IMD) such as pacemaker and insulin pump. In this study, the authors propose elliptic curve cryptography (ECC)-based three-factor lightweight remote user authentication scheme for IMDs. This security scheme is a system model that is associated with IMD, Controller Node (CN), and user (U), where the Dolev-Yao threat model is used to illustrate the application of the proposed scheme. The security is strengthened in the proposed scheme [12] by introducing a three-factor authentication for remote monitoring by U and CN mutually authenticating each other using a session key, and pairwise key establishment between CN and IMD to ensure secure communication between them. In another two interesting studies by Challa et al. [13][14], authors propose a similar security scheme for wireless healthcare sensor networks and also biometric-based three-factor authentication for cloud-assisted CPS environment. However studies [12][13] did not address the utilization of the fog server model, well device model for anonymity and privacy of the user data.

In another study [15], Wazid et al. introduce LAM-CIoT, a lightweight authentication mechanism for a cloud-based IoT environment. One-way cryptographic hash functions are used in this scheme along with bitwise XOR operations. In addition, a fuzzy extractor mechanism is used for user end local biometric verification. The scheme is accomplished in seven steps and uses three-factors of authentication. 1) The smart card of the user 2) password of the user 3) biometric of the user. The scheme preserves the anonymity and untraceability properties by using a timestamp whilst all clocks are synchronized in the application environment.

Yang et al. [16], propose a lightweight data sharing scheme with traceability (LiST) for mobile health solutions. In this model, the system is comprised of WBSN (data owner), healthcare staff (data user), the public cloud and the Key Generation Center (KGC), where KGC is considered as a fully trusted entity that generates public parameters for the entire system and distributes secret keys to data users. Encryption mechanism is seamlessly integrated into this scheme where fine-grained data access with a keyword search over encrypted EHR, traitor tracing, and user revocation are interlaced. According to the authors [16], LiST provides lightweight encryption, lightweight keyword trapdoor generation, lightweight test algorithm, lightweight decryption and verification, lightweight user revocation, and lightweight traitor tracing. The privacy of EHR is protected in this scheme by using the lightweight revocation mechanism to remove unauthorized users and decryption privileges.

Meng et al. [9] propose a Software Defined Network (SDN) based security architecture for the healthcare sector. The SDN separates network policy from networking devices and eliminates device-level configurations. In the context of healthcare and cybersecurity, authors believe SDN enables the protection of wireless medical sensor networks from an array of attacks such as denial of service and flooding attacks. The outcome of the survey carried out proposes a trust-based SDN approach using Bayesian inference for WMSN, in terms of both packets' status and device profile. Authors' surveys suggest this solution is effective and scalable in detecting malicious devices under various conditions. However, the authors also suggest further work to be done on the same to assess the effectiveness in a broader context.

A study carried out by *Porambage et al.* [17] considering the privacy of IoT systems presents the requirements of a privacy framework and the challenges encountered. The authors also highlight the rigor in implementing the traditional bulky privacy protocols due to the nature of the heterogeneous IoT devices. *Porambage et al.* states, despite the availability of lightweight privacy protocol, employing such protocols are not safer as those are easily traceable by the attackers.

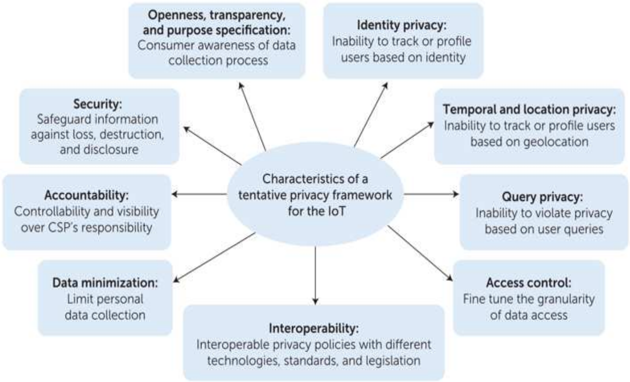
Openness, transparency, and purpose specification:
Consumer awareness of data collection process
Identity privacy:
Inability to track or profile users based on identity
Security:
Safeguard information against loss, destruction, and disclosure
Temporal and location privacy:
Inability to track or profile users based on geolocation
Characteristics of a tentative privacy framework for the IoT
Accountability:
Controllability and visibility over CSP's responsibility
Query privacy:
Inability to violate privacy based on user queries
Data minimization:
Limit personal data collection
Access control:
Fine tune the granularity of data access
Interoperability:
Interoperable privacy policies with different technologies, standards, and legislation

Fig. 2. Characteristics of the privacy framework for IoT solutions [17].

The study also suggests as in Figure 2, the characteristics of a tentative privacy framework for the IoT solutions. Authors believe the interlacing of Internet Service Providers and Cloud Service Provider for transferring and storing user data, poses privacy threats and attacks. Remote health monitoring is one of the key features of HIoT where availability and accessibility of user data are comparatively high. This in consequence exposes privacy threats and requires enhanced privacy frameworks in place to protect users and patients. Nevertheless, multiple privacy-enhancing technologies (PETs) are in use, the underlying technology and scenario-based PETs are more prominent in the context of WSN. Internal and external privacy attacks on WSNs are protected using cryptography-based privacy solutions. However, computationally powerful attacks could succeed while complex cryptographic algorithms could create resource and power overhead to WSN. Therefore, the PETs require complementary solutions that could be adapted to the nature of the IoT application. Furthermore, authors [17] also suggested privacy solutions such as 'privacy coach', and ‘proxy as a broker’ for the privacy-enhancing mechanism that enables scalability and interoperability in IoT applications. Public key cryptography and forwarding agent could be used for location and identity protections in similar environments. Another key solution prescribed by [17] includes PbD, a prominent privacy solution for IoT networks. It is one of the protruding methods that ensure the privacy of the solution entirely at the design level utilizing machine learning, big data analytics, cloud computing, legal policies, and sensing technologies.

Yang et al. [18] present a privacy-preserving system for big data storage and self-adaptive access control in medical care. This solution has three distinguished functions, namely 1) Cross domain data sharing, 2) self-adaptive access control in normal and emergency situations, and 3) smart deduplication. This system outperforms the other privacy-preserving mechanism. The authors of this study list the versatile functions that comprise this solution 1) Attribute-based encryption, 2) Cross domain, 3) Break Glass Access (BGA), and 4) Password-based Break Glass Key (BGK). The mechanism is unique and provides a method for a fine-grained method for accessing encrypted data, sharing data among hospitals using a cross-domain approach, accessing data in emergency situations using BGA and BGK approaches. The use of the BGK method that uses a password is an expedient feature of the privacy-preserving system proposed in this study.

Nevertheless, the three-factor authentication using biometrics, smartcard, and mobile authentication is used to overcome the security loopholes that existed in conventional password-based verification in the studies above [11][12][13] [15][14], there was no end to end solutions that was prescribed in the previous studies. Further, healthcare IoT applications generate a massive amount of data, the process at the device level, transmit, store, process, and feed data into applications for efficient decision making. It is manifested that the previous studies carried out by various authors in the above discussions [16-23], and also in the extensive survey conducted by *Quadri et al.* [1] that the security and privacy of IoT applications were overlooked, solutions prone to attacks and doesn’t prescribe a robust security solution for healthcare IoT spectrum. It is also clear less research was carried out in the healthcare IoT in the past.

VI. Proposed Novel Technologies for Security and Privacy in HIoT

Understanding the elements of IoT applications [7], and the applications and its context of IoT in healthcare help the technologists and users to develop solutions and deliver highly secured privacy endorsed solutions. Major security requirements for healthcare IoT consist of 3 stages: (1) secure cryptographic key generation (2) authentication and authorization of each healthcare IoT component, and (3) robust and secure end-to-end communication between sensor nodes and health caregivers are critical requirements.

In the IoT paradigm [19], several challenges are faced by system designers and users from using the current security and protection techniques due to resource, power and processing capabilities and the size of nodes. To mitigate the risks cited above, robust and lightweight hybrid security mechanisms are needed to establish end to end security of HIoT; and this could be implemented using novel technologies as discussed below.

A) Novel Technologies for HIoT Security Architecture

Machine learning (ML), deep learning (DL), blockchain, SDN, biometric solutions, nanotechnologies, and fog computing are a few of the novel solutions that could fill the gaps and enhance the existing security architecture of HIoT. We proposed a security and privacy architecture for HIoT, as shown in Figure 3.

1) Machine Learning Solutions: Hussain et al. [20] present an ML and DL-based security solution at the data center (processing layer) that fills the gaps of a standard IoT security architecture. ML and DL-based attack detection and mitigation algorithms in IoT could enable an enhanced security architecture for HIoT. According to authors [20], machine learning algorithms such as NaiveBayes, K-Nearest Neighbour, K-Means Algorithm, Random Forest and Decision Tree (DT), Support Vector Machines (SVM), Recurrent Neural Networks (RNN), Principal Component Analysis, Q-Learning, and Deep Learning algorithms are used for;

- Authentication
- Attack Detection and Mitigation
- Distributed DOS attack
- Anomaly detection / Intrusion Detection

- Malware Analysis

2) Blockchain: Hussain at el. [20] and [1] further states data management. The security can be enhanced by employing Blockchain for HIoT. This solution uses a computational model to deter unauthorized modifications. However, there is limited research carried out in the context of HIoT security and privacy.

3) Biometric-based Cryptography for Data Encryption: Medical sensor nodes rely on cryptographic algorithms to securing their communication. The use of secure keys and robust key generation algorithms play a significant role in data encryption. Due to pre-deployment needs orthodox key generation mechanisms, to require computational power and latency during network and consequent adjustments. Biometric cryptography is one of the best solutions to implement secure cryptography in a resource constraint environment.

Biometric end to end encryption is a trending encryption technology in HIoT that securely generates a digital key from a biometric or bind a digital key to a patient's biometric known as Biocrypt. This makes the process more secure and optimizes for the resource-constrained environment by not storing the biometric template. It must be computationally difficult to retrieve either the key or the biometric from the stored Biometric Encryption (BE) template, which is also called "helper data." The helper data could include an Advanced Encryption (AES-128 or AES-256) based key, or pseudorandom number generated using the Fibonacci linear feedback shift register using sensor data such as an inter-pulse sequence of ECG readings. The real-time data encryption is proposed to be performed by stream cipher and data-in-rest is to be done using a block cipher. BE is considered fuzzy due to the uniqueness and variability of the biometric. Biometric information collected from healthcare monitoring nodes such as the electrocardiogram (ECG), fingerprints, face identification, iris, and other biometric data is used for the medical sensor monitoring application.

4) Biometric-based Identification and Authentication: Medical sensor devices must be protected from physical theft and unauthorized access. Biometric information could also be used as a means of identification and authentication mechanism. The key for data encryption should be separated from those used for authentication. Authentication and authorization of each healthcare IoT components could also be implemented using a combination of biometric authentication and Datagram transport Later Security (DTLS) mechanism.

5) Mutual Authentication and Authorization of IoT Components: In HIoT, the data collected by medical sensors are not only collected and transmitted to the end-users such as medical practitioners or smart hospital network but also the end-users must be able to connect to the sensor nodes in a specific type of applications such as pacemakers. In such situations, the mutual authentication and authorization of end-users and devices are imperative (authentication and authorization of such operations). Moosavi et al. [19] proposed a solution using a fog layer component where the smart health gateways perform the authentication and authorization of remote end-users securely and efficiently on behalf of medical sensors. Mutual authentication between the medical device and the smart gateway is required during initialization.

6) Security Protocols and Verification: The introduction of the fog layer and hosted smart HIoT gateways let the heavyweight security protocols and certificate validations efficiently and protect the system as gateways and end-users are sufficiently devised with resources.

7) Use of End to End Lightweight Security Platform for IoT Devices: A purpose-built IoT end to end lightweight security and management platform could be another solution to protect the whole health care system. NanoLock is such a platform that self-provisions, protect, manage and secure firmware over the air (FOTA) device update, control and monitors connected devices and include robust features for monitoring device security¸ device to cloud integrity¸ version management¸ attack detection and alerts from the cyber-physical system to the cloud [9].

8) Nanotechnology: Considering the technology solutions, end to end solution such as NanoLock could benefit any IoT solution that requires protection from eavesdropping, data theft, authentication and authorization, encryption, privacy preservation, securing data at rest, process and transit, prevention from malicious attacks such as WannaCry, hacking, FOTA and secure life cycle management. However, the need for such a solution is based on requirements, budget, and stakeholder needs. For healthcare IoT systems, a vast collection of heterogeneous devices joins from in-house networks and external patient networks. Security threats such networks pose health data privacy preservation, consequences of failed security measures such as fatalities, blackmailing, and financial loss must be taken into account when designing security solutions.

9) Fog or Edge Computing: IoT systems with a Fog layer for monitoring patient health. In a 3-layer healthcare IoT system, the (1) device layer, where the physical devices such as wearable devices, implanted devices, and other monitoring devices are attached to a micro wireless module to collect contextualized personal medical data. In the (2) fog layer, consists of interconnected smart gateways. This layer allows the IoT network to host a local repository for interconnected subnetworks and provide intelligence to the edge node. Smart gateways receive data from subnetwork, do protocol conversion, and provide higher-level services. The last layer (3) cloud layer comprises of big data analytical servers and data warehouses, a remote healthcare server that periodically synchronizes with the hospital database.

10) Zone-based IoT Architecture: Microsoft proposes a segment-based threat modeling approach that devises optimized security architecture for HIoT. The architecture is divided into a device zone, field gateway zone, cloud gateway zone, and service zone. Each zone often has its own data and authentication and authorization requirements. Zones can also be used to isolate the damage and restrict the impact of low trust zones on higher trust zones.

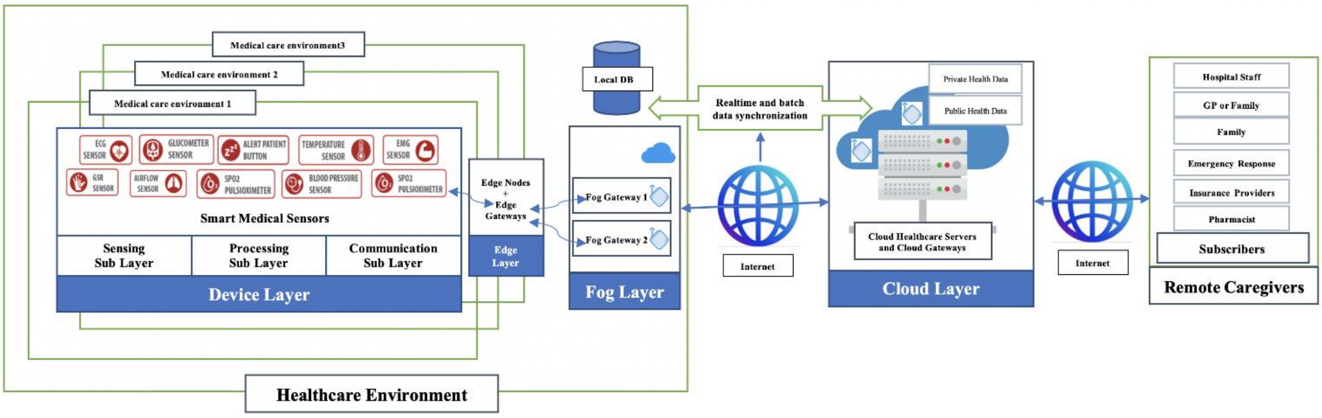

Fig. 3. Proposed Architecture for Security & Privacy in HIoT

B) Lessons Learned and Proposed Architecture

Standard IoT frameworks such as the one developed by Microsoft and Amazon Web Services (AWS) could be used off the shelf with limited adjustments that suit HIoT monitoring needs while ensuring information governance and standards are thoroughly followed. This includes SaaS (Software as a Service) on a subscription basis and is centrally hosted, PaaS (Platform as a Service) for working collaboratively especially with external partners, and IaaS (Infrastructure as a Service) for delivering cloud computing infrastructure such as servers, storage, network and operating systems as an on-demand service. On the other hand, a custom-made IoT framework could be integrated for more flexible IoT solutions for healthcare monitoring systems that guarantee the security and privacy of HIoT.

As discussed, HIoT monitoring system architecture could benefit from zone-based architecture described in Figure 3 that isolates security issues such as ransomware and malicious attacks from spreading to the whole network as each zone has its own counter security measures for STRIDE - Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. The components in each zone and the data during the transition could be subject to STRIDE. It is advisable to implement improved purpose-built IoT end to end security solutions listed in the previous section. Further, a fog layer could be configured to utilize heavyweight security functionalities that are required, suitably between device zone and field gateway zone, and also between field gateway zone and cloud gateway zones. End to end encryption using Biometric data as described in the previous solution could be used to ensure the security of data and preserve privacy while data is at rest, process, or transmit. Tiny ML could be employed at the device level to detect anomalies as discussed in the previous section. An alternative way of implementing a security solution is by implementing an SDN and considering PbD. However, SDN is considered immature and requires further research. A blockchain mechanism that requires higher computational power could be employed at the cloud gateway zone to ensure the privacy of big data at rest.

VII. Future Research Direction and Conclusion

HIoT is a critical IoT application that involves trillions of devices, lives, and the security and privacy of data and networks. It is a multimillion industry that can also save millions of monies while contributing to the economy. Whilst examining the security and privacy solutions for HIoT, it is vital to look into the open research areas as future directions by employing security and privacy in HIoT and to improve the HIoT paradigm.

1. Poor management of sensitive data where there is no proper strategy in place for information gathering using appropriate sensors. Additionally, computing operations can be performed over encrypted data using homomorphic encryption.

2. Naming and Identity Management – due to the burst in IoT applications and devices involved, it is challenging to assign unique identifiers to each device. At present, IPV4 and IPV6 are utilized for HIoT network devices. However, the exponential growth in IoT devices in healthcare and other industries will bring challenges in defining unique identifiers.

3. Trust management and policy is another topic to investigate with sharp vision. Sensitive and personal data of patients must be preserved with secure channels.

4. The transmission and processing of big data collected from HIoT devices in real-time is another challenge for IoT specialist encounter.

5. Nevertheless, intelligent machine learning algorithms provide enhanced security and privacy solutions. However, implementing them on IoT devices faces challenges due to the resource constraint device configurations.

Acknowledgement

Muhammad Khurram Khan is supported by Researchers Supporting Project number (RSP-2020/12), King Saud University, Riyadh, Saudi Arabia.

References

[1] Y. A. Qadri, A. Nauman, Y. Bin Zikria, A. V. Vasilakos, and S. W. Kim, "The Future of Healthcare Internet of Things: A Survey of Emerging Technologies," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020.

[2] Aruba Networks, "IoT Heading for Mass Adoption by 2019 Driven by Better-Than-Expected Business Results," *arubanetworks.com*, 2017. [Online]. Available: https://news.arubanetworks.com/press-release/arubanetworks/iot-heading-mass-adoption-2019-driven-better-expected-business-results. [Accessed: 28-Jul-2020].

[3] P. A. H. Williams and V. McCauley, "Always connected: The

security challenges of the healthcare Internet of Things," in *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016*, 2017, pp. 30–35.

[4] FDA, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," *FDA Guid.*, p. 6, 2018.

[5] M. Burhan, R. A. Rehman, B. Khan, and B. S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors (Switzerland)*, vol. 18, no. 9, pp. 1–37, 2018.

[6] A. M. Rahmani *et al.*, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Futur. Gener. Comput. Syst.*, vol. 78, no. February, pp. 641–658, 2018.

[7] OWASP, "OWASP Internet of Things Project - OWASP," *2018*, 2019. [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project. [Accessed: 31-Jul-2020].

[8] M. J. McGrath, C. N. Scanaill, M. J. McGrath, and C. N. Scanaill, "Regulations and Standards: Considerations for Sensor Technologies," in *Sensor Technologies*, Apress, 2013, pp. 115–135.

[9] Nanolock, "NanoLock Security," *nanolock.com*, 2020. [Online]. Available: https://www.nanolocksecurity.com/solution/. [Accessed: 31-Jul-2020].

[10] M. A. Sahi *et al.*, "Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions," *IEEE Access*, vol. 6, pp. 464–478, 2017.

[11] M. Wazid, A. K. Das, N. Kumar, and A. V. Vasilakos, "Design of secure key management and user authentication scheme for fog computing services," *Futur. Gener. Comput. Syst.*, 2019.

[12] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A Novel Authentication and Key Agreement Scheme for Implantable Medical Devices Deployment," *IEEE J. Biomed. Heal. Informatics*, vol. 22, no. 4, pp. 1299–1300, 2018.

[13] S. Challa *et al.*, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 69, pp. 534–554, 2018.

[14] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 1267–1286, 2020.

[15] M. Wazid, A. K. Das, V. Bhat K, and A. V. Vasilakos, "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment," *J. Netw. Comput. Appl.*, vol. 150, no. May 2019, p. 102496, 2020.

[16] Y. Yang, X. Liu, R. H. Deng, and Y. Li, "Lightweight Sharable and Traceable Secure Mobile Health System," *IEEE Trans. Dependable Secur. Comput.*, vol. 17, no. 1, pp. 78–91, 2020.

[17] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, and A. V. Vasilakos, "The Quest for Privacy in the Internet of Things," *IEEE Cloud Comput.*, vol. 3, no. 2, pp. 36–45, 2016.

[18] 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. (Ny).*, vol. 479, pp. 567–592, 2019.

[19] S. R. Moosavi, E. Nigussie, M. Levorato, S. Virtanen, and J. Isoaho, "Performance Analysis of End-to-End Security Schemes in Healthcare IoT," in *Procedia Computer Science*, 2018, vol. 130, pp. 432–439.

[20] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Commun. Surv. Tutorials*, pp. 1–23, 2020.

Sivanarayani M Karunarathne completed her MSc in IoT with Data Analytics from Bournemouth University, UK. Currently, she is working as an Operations & Platform Engineer with Elekta in Crawley, UK. Her research interests include IoT security, data privacy, data analytics, and networking. Contact here at nara_cha@ymail.com.

Neetesh Saxena is an Assistant Professor at Cardiff University (CU), UK and leads the Cyber and Critical Infrastructure Security (CyCIS) Lab. Before joining to CU, he was an Assistant Professor at Bournemouth University, UK, a Researcher at the Georgia Institute of Technology, USA and the Stony Brook University, USA & SUNY Korea. He earned his Ph.D. from IIT Indore, India. He has published several papers in international peer-reviewed journals and conferences. His research interest includes infrastructure security, smart grid, healthcare and IoT security. He was a DAAD and TCS Research Fellow, and currently is a senior member of the IEEE and an ACM member. Contact him at nsaxena@ieee.org.

Muhammad Khurram Khan is currently working as a Professor of Cybersecurity at the Center of Excellence in Information Assurance, King Saud University, Kingdom of Saudi Arabia. He is founder and CEO of the 'Global Foundation for Cyber Studies and Research' (http://www.gfcyber.org), an independent and non-partisan cybersecurity think-tank in Washington D.C, USA. He is the Editor-in-Chief of 'Telecommunication Systems' published by Springer-Nature with its recent impact factor of 1.73 (JCR 2020). He is on the editorial board of several journals including, IEEE Communications Surveys & Tutorials, IEEE Communications Magazine, IEEE Internet of Things Journal, IEEE Transactions on Consumer Electronics, Journal of Network & Computer Applications (Elsevier), IEEE Access, IEEE Consumer Electronics Magazine, PLOS ONE, and Electronic Commerce Research, etc. He has published more than 380 papers in the journals and conferences of international repute. In addition, he is an inventor of 10 US/PCT patents. He has edited 10 books/proceedings published by Springer-Verlag, Taylor & Francis and IEEE. His research areas of interest are Cybersecurity, digital authentication, IoT security, biometrics, multimedia security, cloud computing security, cyber policy, and technological innovation management. He is a fellow of the IET (UK), a fellow of the BCS (UK), and a fellow of the FTRA (Korea). He is the Vice Chair of IEEE Communications Society Saudi Chapter. He is a distinguished Lecturer of the IEEE. His detailed profile can be visited at http://www.professorkhurram.com. Contact him at mkhurram@ksu.edu.sa.