Secure Medical Internet of Things Framework based on Parkerian Hexad Model

Nidal Turab[1]
Networks & information security Dept, Faculty of IT
Al-Ahliyya Amman University, Amman-Jordan

Qasem Kharma[2]
Computer Science Dept,Faculty of IT
Al-Ahliyya Amman University, Amman-Jordan

***Abstract*—Medical Internet of Things (MIoT) applications enhance medical services by collecting data using devices connected to the IoT. The collected data, which may include personal data and location, is transmitted to mobile device and to health care provider via Internet Service Provider (ISP). Unfortunately, connecting a device to a network or sending data via wide network may make those devices and data vulnerable to unauthorized access. In this research, a secure 3-tier MIoT framework is proposed. Tier 1 includes the devices and sensors that will collect data. Those devices and sensors are based upon limited resources; therefore, they cannot apply complex security and privacy algorithms. Tier 2 includes the devices that will collect data from Tier 1 and submit it to Tier 3 via Internet Service Provider (ISP). Tier 3 includes the Health Information System. The framework defines the controls that are needed between layers to secure user privacy and data based on the Parkerian Hexad Model.**

Keywords—MIoT; Perkerian Hexad; PRMS; Lightweight Encryption

I. Introduction

IoT is defined as a network that enables every object or device on the planet to interact, connect, and exchange data with other objects. The concept of IoT began in 1998, where Brave, et al. [1] designed a haptic prototype to support distance-communication between people. Also, the term “Internet of Things" was first used by Kevin Ashton in 1998 to describe the system that connects different objects using sensors [2]. Since that time, the IoT has numerous promising application domains such as in smart homes, smart Cities, smart power grids, farming, transport systems, wearable clothes and devices, industrial Internet, and healthcare.

One important application of IoT is in healthcare due to the rapid increase in world population, along with increased life expectancy and chronic diseases. Hence, it is vital to develop medical electronics and wearable devices that improve healthcare services by reducing cost, reducing the frequency of clinic visits, reducing the length of hospitalization, reaching patients in distant places, and monitoring patients continuously.

The term MIoT (Medical Internet of Things) means the applications of Internet of Things technologies in the medical field including the integration of healthcare devices with IoT enabled technologies (sensors, Wi-Fi, etc.) and applications to communicate with health care systems. MIoT can reduce the frequency of hospital visits by allowing patients to connect remotely and transfer data to their physicians. According to the Frost & Sullivan analysis, the global MIoT market was worth $22.5 billion in 2016, and is expected to reach $72.02 billion by 2021 [3]. Today, there are many applications based on MIoT. Some current MIoT applications include:

- Patient Remote Monitoring System (PRMS): the use of IoT based technologies helps to monitor patients and record their vital signs through medical sensors in real time. Pulse oximeters and other sensors collect vital signs including blood pressure, body temperature, pulse, breathing rate, blood glucose, and patients’ height, weight, and body mass index [4] [5] [6]. The aforementioned data are collected and sent to medical care centers where they are analyzed, and relevant medical information is extracted and forwarded to the intended physicians.

- Healthcare for elderly and disabled persons: The number of elderly and disabled people is increasing each year. Smart homes can provide comfortable and independent living for elderly and disabled people rather than staying in dedicated facilities (elderly or disabilities nursing homes). They can utilize wearable devices utilizing wireless technology to control home appliances, light sources, climate control, etc. In addition, sensors placed in different locations at home can track movements and other information for family member(s), or even send any urgent vital signs and health alerts to physicians immediately [7].

- Healthcare for rustic public health monitoring and control: Many patients living in rural areas encounter the problem of a lack of nearby healthcare centers. Using IoT based health monitoring and control technologies can help to overcome this problem by monitoring patients’ health symptoms and urgent information. RFID sensors are used to record the patient health information. These data are sent through the Internet to the nearest health care center, or send alert messages to doctors directly [8] [9].

- Ingestible Sensor: The ingestible sensor developed by Proteus Digital Health helps to monitor patients’ behavior of taking prescribed medication. The Proteus ingestible sensor can be consolidated with any pharmaceutical products to reach the stomach (via swallowing) where it powers up and sends signals through the patient’s tissue to a patch on the skin that detects the signal and records the exact time the medication has been taken. Furthermore, the patch can record heart rate, body position, and other activity. Using wireless technology, the patch sends information to a mobile phone application, which in turn can send the collected data to a physician or health care center [10] [11].

- IoT based Healthcare automated patient records system: The use of MIoT based technologies enables doctors to reduce time spent on daily routine tasks such as documenting patient history and medication rather than physical examinations and monitoring. These technologies are based upon using smart glasses accompanied with voice command systems to transmit data to hands-free, encrypted HIPAA-certified systems [12] [13].
- Adverse Drug Reaction System: Adverse drug reaction (ADR) is any harm caused by taking a medication. It can result from lengthy treatments or even a single drug dosage. In a typical IoT based ADR system [13], healthcare applications using NFC-enabled devices read data about drugs and compares them against patients' allergy profiles and medical histories, utilizing unified health data located at national health care centers. If a patient has an ADR, an alarm will be triggered [14].
- Heart disease monitoring system: The time it takes to arrive at a health care center is life-or-death for persons suffering from a heart attack; in some cases, patients are unconscious and unable call the healthcare center. This delay in notifying healthcare professionals could result in death. MIoT solutions can send real time (instant) patient vital signs (electrocardiography, blood pressure, pulse rate) to physicians. Additionally, they can send the patients' location, facilitating reaching them at the appropriate time [8].
- Compliance with Guidelines on Hand Hygiene in Health Care: according to the WHO Guidelines on Hand Hygiene in Health Care, infections are caused by various factors related to human behavior or systems and processes of health care suppliers [15]. Fortunately, infections are preventable; one basic measure to reduce infection is hand hygiene. MIoT hand-hygiene compliance monitoring (HHCM) systems would detect the degree of cleanliness in a healthcare worker by transmitting information about when the person enters or leaves a healthcare facility sterilization unit [15].
- Hearing Aids IoT based technologies: studies show that over 5 percent of the world's population starts having hearing difficulties after the age of 25. MIoT created wearable ear hearing aid devices. They can connect to and control a variety of household devices and mechanical tools [16].
- Oxygen Saturation Monitoring: Oxygen saturation monitor displays the percentage of blood saturated with oxygen. It is a wearable sensor placed on a thin part of the patient's skin, allowing it to determine the oxygen absorbance due to the pulsing arterial blood [17].
- Although having a variety of medical devices connected to MIoT to increases its efficiency and reduces the cost of medical services, connecting devices to a wider network makes those devices more vulnerable to attacks. Therefore, any devices connected to IoT must be controlled in order to protect those devices from unauthorized access [18]. In this paper, a secure MIoT is proposed to protect patient data and privacy. The structure of this paper is organized as follows: Section 2 reviews related work on securing e-health systems. The challenges of the Medical IoT are discussed in Section 3. Section 4 presents a proposed secure structure of the e-health system in which there is a set of security criteria related to each user of a health system. Finally, the paper conclusions are in Section 5.

II. Related Work

- A lot of work has been done to address the issues of medical IoT safety and privacy. D. Salvi, E. V. Mora and M. T. A. Waldmeyer [19] listed all of the security problems related to patents' remote monitoring systems with some possible solutions. They proposed a security architecture based upon the legal basis of European Recommendation No R(97)5, the architecture based on renowned technologies such as web services for patients monitoring devices and service providers. D. Lake, R. M. R. Milito, M. Morrow and R. Vargheese [20] have identified some emerging standards and regulatory bodies for e-health. P. Gope and T. Hwang [21] described some security and privacy issues in BSN based healthcare systems. Further, they proposed a secure IoT based healthcare security system called BSN-Care, which mitigates some security issues of the BSN based healthcare system. S. Khoja, H. Durrani, R. E. Scott, A. Sajwani, and U. Piryani [22] have developed tools that cover all aspects of the Khoja–Durrani–Scott [KDS] framework for e-health systems. The proposed tools have been developed for healthcare governance, healthcare providers, and patients to understand their e-health programs. F. Rezaeibagha, K. T. Win, and W. Susilo [23] investigate the requirements of security and privacy of e-health from a technical perspective. The conducted literature is compared with ISO/IEC 27002:2013 and ISO/IEC 29100:2011 standards. They concluded that access control policies should be mandated to provide patient privacy. W. Leister, M. Hamdi, H. Abie and S. Poslad [24] presented an evaluation framework for adaptive security of e-health applications. The framework is based on security and QoS requirements for a generic e-health model, and a generic assessment framework. They presented three scenarios: home, hospital, and emergency scenarios.
- O. Olakanmi, I. Kamil and S. Ogundoyin [25] proposed a recommendation security and privacy framework to achieve anonymous authentication during the recommendation process and a trust model for efficient

selection of health care specialists. In Lee J the authors proposed a service-oriented security framework for remote medical services. The proposed framework supports dynamic security elements in accordance with demands of remote medical services. It enables confidentiality, integrity, and availability for all parties of remote medical systems.

- D. Y. Weider, L. Davuluri, M. Radhakrishnan and M. Runiassy [26] evaluated the gaps in security-oriented (SOD) enterprise frameworks especially Australian and the US frameworks reviewing existing frameworks and compared their risk-based methodologies. They established a guide to develop adequate threat mitigations that meet the needs of the healthcare stakeholders. W. Leister, M. Hamdi, H. Abie and S. Poslad [24] developed a framework to validate and assess the context-aware adaptive security eHealth solutions. They developed scenarios for patients with chronic diseases who use biomedical sensors. D. P. Mirembe [27] investigated the current trend in Telemedicine, E-health and Wellness (TEW) research and development, including their technologies, standards, services, and security implementations. In addition, they developed a framework that describes any TEW system. B. Ondiege, M. Clarke and G. Mapp [28] reviewed remote patient monitoring RPM they used Microsoft threat modelling tool, to explore current threats in IEEE 11073 standard devices then they propose a new security framework for remote patient monitoring devices. B. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins and R. Jardim-Goncalves [29] proposed an ontology-based framework for securing e-health composed of two approaches: design time and run time. H. Mora, D. Gil, R. M. Terol, J. Azorín and J. Szymanski [30] proposed a distributed framework for monitoring human biomedical signals. the proposed framework can be applied to other mobile environments, with high processing and have high data volumes. L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi and L. Tarricone [31] proposed IoT-aware architecture, for Smart Hospital System (SHS) for RPM, network infrastructure relying on a CoAP, 6LoWPAN, and REST paradigms has been implemented for UHF RFID and WSN.

R. Piggin [32] explains ways to resolve issues concerning safety and security, also they highlights approaches that medical devices' manufacturers should take to improve security throughout lifecycle of their products.

III. Challenges of Medical IoT

One of the most significant threats that IoT poses is to data security and privacy. Healthcare records contain various types of private information, including a patient's name, email address, date of birth, social insurance number, and medical history. That information is valuable to hackers and is usually stored in one place, rarely changed (not as credit card numbers), and can be sold at higher prices on the black market (dark web). Hence, MIoT applications must take in consideration data security and privacy.

Unfortunately, most of the IoT sensors and devices lack data protocols and standards. In addition to that, there is significant ambiguity regarding data ownership regulation. All these factors make the data highly susceptible to cybercriminals who can hack into the system and compromise Personal Health Information (PHI) of both patients as well as doctors. Moreover, continuous access to health records is essential for the safety of patients because if the healthcare provider looses access to medical records, patients' lives could be at risk. Some security vulnerabilities that can compromise healthcare systems are:

- Data forgery or corruption: the attacker can modify or delete medical records to achieve some illegal purpose. Modifying vital health records may result in system failure and cause patient death.
- Medical staff: doctors, nurses and medical staff at the health care centers have easy access to medical records and patient files. This can be used for identity theft or other purposes such as blackmail.
- Unsecured medical sensors and devices: medical devices with access to healthcare centers' devices must meet security standards so they do not leave networks vulnerable to malware, eavesdropping, and phishing.
- Stolen medical devices or sensors: Any stolen medical device can be used to access the healthcare provider network if no security measures are applied.
- The risk of revealing or stealing personal data of patients and their medical history for the purposes of extortion or defamation might be one of the largest security threats to health care systems.
- Unrestricted access to healthcare provider devices and systems: systems and devices with no restricted areas can easily and altered be accessed by unauthorized personnel [33].

IV. Secure Structure Model for MIoT Systems

The most crucial aspect in the medical field is to preserve the privacy of health care records and systems. Patients must be confident that their data is stored and processed in a secure manner, with no security breaches. If the trust relationship between patients and health care systems is broken, they will not reveal information necessary to deliver the health care they need. Medical records at healthcare providers contain sensitive and personal information about patients. Therefore, healthcare providers should ensure the privacy of information, especially because the patients' data can be increasingly stored accessed remotely. Protecting patients' medical records and information, and weighing sharing this information with different medical users is the main challenge of health service providers. Consequently, it is pivotal for healthcare service providers to have well structured, secured, and reliable system for storing electronic medical records in their health information systems.

In this paper, a three-tier layered network architecture is used to secure the medical records transferred from the patient to the healthcare provider. The three tiers are|:

Tier 1: This consists of medical sensors, devices, and scales that measure the vital signs of the human body, whether or not they are wearable. Examples include BPM, ECG, glucose meters, hearing aid devices, weight scales, brain activity monitors, and so on. The aforementioned devices and sensors have constrained resources (memory processing power and power supply), thus they cannot perform complex algorithms required for security and privacy implementations. Compact hardware and software implementations with low power, RAM, and ROM usage are desirable.

Tier 2: This includes smart phones, PDAs, tablets, and wireless access points. Tier 2 devices receive wireless signals form tier 1 devices and transmit them to the MIoT provider via ISP or cloud service provider.

Tier 3: This can be considered as the MIoT, consists of health record servers, medical database servers, and storage devices. Physicians can access data stored on the MIoT provider's infrastructure to track and diagnose patient health. Tier 3 devices require complex security measures as they represent the medical data and records repository.

The three-tier network architecture is illustrated in Fig. 1.

The CIA Triad composed only of the three elements: Confidentiality, Integrity and Availability, but does not adequately address and satisfy the requirements of ownership and continuity of the medical records and health care systems. Therefore, the Parkerian Hexad model is a more suitable model than the CIA triad, since the Parkerian Hexad model adds three extra elements to the CIA triad: Possession or Control, Authenticity, and Utility [32] [34]. The rational of using Parkerian Hexad model as central structure of this study is that its attributes cannot be broken down into further ingredient; and not overlap with each other. The following subsection addresses each facet of the Parkerian Heaxd model as related to three-tier architecture:

Facet 1: Authentication: Authentication means to identify a person or device to another person or device, usually by using usernames and passwords. The three-tier network authentication takes place at two points: between tier 1 and tier 2 devices, and between tier 2 and tier 3 devices. For authentication between tier1 and tier 2, authentication protocols are limited to lightweight authentication protocols that give a reasonable level of authentication while preserving the constrained device resources. There are a variety of lightweight authentication protocols that provide authentication; they vary according to data size, key size and application:

1) LMAP: 896-bits authentication protocols designed for resource constrained RFID tags [35].

2) ALIKE: 80-bits and above asymmetric key based on RSA scheme for resource constrained RFID tags [36].

3) ELLI: Elliptic Curve-based authentication scheme: Elliptic curve cryptography offers the same security level as RSA with smaller key sizes and less processing power, and can offer authentication for resource constrained devices [37].

4) IBS: Identity-Based Signatures: verifying users' digital signaturesusing only public users' identifiers or any other public information [38].

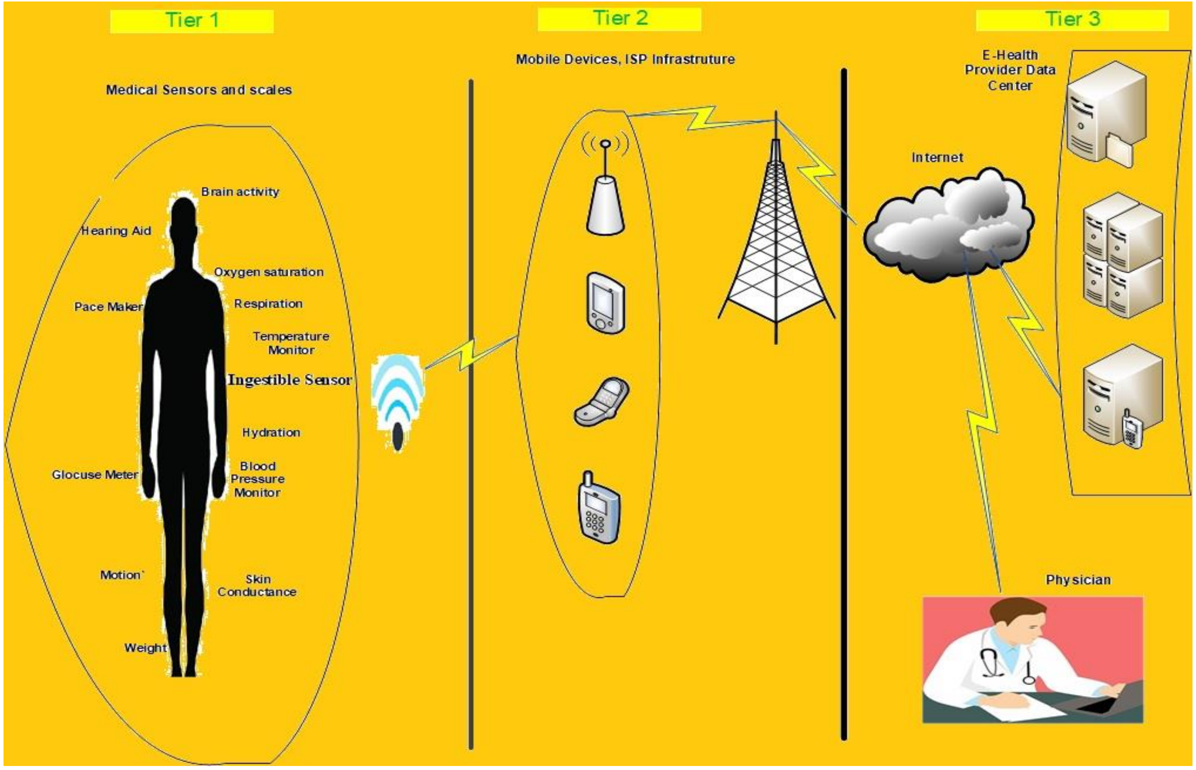

Fig. 1. The Proposed Secure three-Tier MIoT Architecture.

Regarding tiers 2 and 3, any authentication protocol (either PPP or AAA) could be used as there are no constrained resources. Any PPP authentication such as Password Authentication Protocol (PAP), Challenge-handshake Authentication Protocol (CHAP), Extensible Authentication Protocol (EAP), and any AAA authentication such as TACACS, Remote Authentication Dial-In User Service (RADIUS), and Diameter and Kerberos can be deployed.

Facet 2: Integrity: Data integrity technique means data generated by a medical device is transmitted and stored in the healthcare center but neither altered nor tampered with [39]. Integrity between tiers 1 and 2 is limited to lightweight integrity designed for constrained device resources. There is a variety of lightweight integrity that varies according to hash functions and permeation size; some of them are described briefly below:

- Photon: is 256 bits hash function with permutation sizes up to 288 bits [40].
- Spongent: is 256 bits hash function with permutation sizes up to 272 bits [41].
- Lesamnta: is 256 bits hash function with permutation size 384 bits [42].

Between tiers 1 and 2, Public Key Infrastructure (PKI) can be used for medical data integrity but the requirements of key management and public keys distributions on large environments such as Medical IoT make it difficult to adopt. Thus, another promising choice is the use of blockchain technology to provide medical data integrity. Keyless Signature Infrastructure (KSI) provides integrity and identity associated with medical digital assets. By integrating KSI into healthcare systems, regardless of whether medical data is transmitted or stored, every medical device, system configuration, and digital health record can be verified. KSI hash is a one-way function such that there is no mathematical formula or process to recover the file from the hash. KSI forms a unique distributed database across the medical servers. Records can only be added to the database, never removed. The KSI Infrastructure consists of a distributed network of devices configured as cores, aggregators, and gateways. Hierarchical structure works as follows: low-level aggregation servers collect and process requests from clients and then send them to the upper level servers. Each server receives the request from the downstream server, adds them to the hash tree, and sends the local root hash to its preceding upstream server [43] [44] [45].

Facet 3: Confidentiality: Only authorized parties can explore the information, this can be achieved through the process of encryption involving encoding information into a new, ciphered form that can be understood only by authorized parties who have the secret key. An interceptor may illegally interfere with the information in unencrypted form. As with authentication, encryption takes place at two points: between tier 1 and tier 2 devices, and between tier 2 and tier 3 devices.

Encryption between tier 1 and tier 2 is limited to lightweight encryption protocols that offer a reasonable level of encryption while preserving the constrained device resources. There are a number of lightweight encryptions that vary according to data size, key size, and application. Some of them are briefly described below:

1) Camellia: Camellia block cipher has key sizes of 128-bit, 192-bit, and 256-bit, and can be implemented either by hardware or software [46].

2) TWINE: A Lightweight, Versatile Block Cipher, has key sizes of 80-bit and 128-bit, and can be implemented either by hardware or software [47].

3) Trivium: Hardware oriented synchronous stream ciphers with 80-bits key length [48].

4) SIMON and SPECK: are two families of block cipher with 80-bit, 96-bit, and 128-bit that are implemented on both hardware and software [49].

5) PRESENT: Block cipher with 80-bit and 128-bit key lengths. PRESENT is suitable for RFID tags and sensor networks [50].

6) PICALO: A block cipher that supports 80-bit and 128-bit keys. PICALO can be implemented in hardware and it is suitable for RFID tags and sensor networks [51].

7) LEX: A 128-bit key stream cipher. LEX is based on AES [52].

8) LED: 64-bit and 128-bit key block cipher encryption is based on AES and is dedicated for hardware implementation [53].

9) CLEFIA: a block cipher with 128-bit, 192-bit, and 256-bit key sizes, CLEFIA supports AES. [54]

10)Enocoro: 80-bit key stream cipher encryption dedicated to hardware implementation [55].

Regarding tier 2 and tier 3, any encryption protocol (either symmetric key or public key) could be used because there are no constrained resources. Some of encryption algorithms are Triple DES, RSA, Blowfish, AES, Elliptic curve, and more.

Another emerging category of encryption is the authenticated encryption that provides authentication besides message integrity; it consists of encrypting the plain text then computing the hash value. Authenticated encryption requires fewer resources than a serial operation of encrypt and authentication. Some of authenticated encryption schemes are:

1) The Hummingbird-2: An authenticated encryption algorithm that has a 128-bit key. Hummingbird-2 is a good choice for passive RFID systems [56].

2) Phelix: An authenticated encryption that combines stream cipher and MAC function. Phelix uses a 256-bit key [57].

3) Fides: A single pass block cipher authenticated encryption algorithm, FIDES uses either 80-bit or 96-bit keys [58].

4) ACRON: 128-bit authenticated encryption algorithm efficient in both hardware and software implementations [59].

5) Grain-128a: 128-bit stream authenticated encryption algorithm that uses non-linear functions of authentication and encryption [60].

6) SCREAM and iSCREAM: 128-bit tweakable block ciphers with authenticated encryption [61].

7) ALE: a 128-it key based on AES, an online single-pass lightweight authenticated encryption that uses Nonces. [62]

8) LAC: 80-bit key block cipher authenticated encryption, and has a similar structure to ALE [63].

9) ASC-1: Stream cipher authenticated encryption with key size of 128-bit [64].

10)Quark: A family of lightweight authenticated encryption algorithms that support 256-bit key size, dedicated for constrained hardware security [65].

11)Ascon: A family of lightweight block cipher authenticated encryption algorithms that support key lengths of 96 and 128 bits. [66].

12)Joltik: 64-bit and 128-bit tweakable block cipher authenticated encryption algorithm [67].

13)Ketje: 182-bit cipher authentication and encryption algorithm based on sponge structure [68].

14)Sablier: 80 and 256 bits key authenticated encryption that is hardware-efficient [69].

Facet 4: Possession or Control: Medical records and data obtained by medical sensors, diagnoses, and laboratory tests are valuable because any breach can infringe upon patients' privacy. Rightful ownership of medical records varies from country to country. In the United States, there is no federal law regarding ownership of medical records; the Health Insurance Portability and Accountability Act (HIPAA) gives patients the right to access and modify their Medical records, but do not specify ownership of the medical records. In the United Kingdom, the Secretary of State for Health owns NHS's medical records. In Canada, the patient owns the information contained in the medical records, but the healthcare provider owns the records themselves [70] [71]. Broadly speaking, as no data is stored in the medical sensors located at tier 1, controlling data is the responsibility of the healthcare provider in tier 3.

Facest5: Utility or Usability: ISO defines usability as "The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" [72]. In tier 1, the medical device (or sensor) must have a measure or procedure to ensure that any health information or data (measured or collected) by it remains usable and useful across the lifetime of the medical device, and can be transferred to any successor medical device(s) [32].

The international standard ISO/IEC 62366: Medical Devices Application of Usability Engineering to Medical Devices assures that medical device manufacturers follow a systematic usability process. Besides medical devices design, manufacture and development process manufacturers will need to change the way they design, manufacture, and develop in order to comply with the standard.

Some of the important usability concerns defined by the standard are:

1) The design and manufacture of the medical devices must assure that when it used under the intended purpose and under the suitable operating conditions, it will not harm the safety of patients. Moreover, this shall include:

a) Reducing the risk of use error due to the required levels of technical knowledge, experience, and training required to achieve the required operation of the device

b) Considering the physical conditions of intended patient (normal or disabled users)

2) The measurement, monitoring and display scale must be indicative, easy to understand and simple to use, while maintaining the intended purpose of the medical device

3) Operating instructions must avoid misuse for devices emitting radiation

4) Device instructions are in layman's terms easy to understand by patients [73] [74].

From the tier 3 prospective, usability of computer software and applications described in the ISO 9241 ISO/TR 16982:2002 standard that provides information on usability methods used for design and evaluation of any objects such as software, computer, tool, website, and process [75].

Facets 6: Availability: It is beneficial for any health service provider to affirm that health records are available to the authorized people at the proper time. Lack of availability could decrease the health service quality, and increase the risk of litigation for the health service provider.

Confidentiality, Authentication and Integrity of electronic health records are basic elements of availability. In addition, health care systems must have backup components, such as fault-tolerance systems. Thus, if a software or hardware component goes down or malfunctions, the system can switch to a backup component. Moreover, healthcare providers must apply ISO/IEC 24762:2008 standard guidelines for providing the provision of information and communications technology disaster recovery services to ensure business continuity [76] [77].

TABLE I. LAYERED NETWORK ARCHITECTURE AND ITS RELATION TO PARKERIAN HEXAD FACETS

Facet	**Supporting Protocols/Standards**	**Recommend implementation**	**Network tier(s)**
Authentication	1. Lightweight Authentication protocols (LMAP, ALIKE, ELLIE ,IBS) 2. PPP & AAA authentication (PAP, CHAP, EAP, TACACS, RADIUS, Diameter and Kerberos	LMAP, ALIKE, ELLIE ,IBS	Between Tier1 & Tier2 devices BetweenTier2/Tier3 devices
Integrity	1. lightweight integrity: Photon, Spongent: Lesamnta: 2. PKI and KSI	Photon, Spongent (approve by Lightweight Cryptography Working Group [37])	Between Tier1 & Tier2 devices BetweenTier2/Tier3 devices
Confidentiality	1. Lightweight encryption protocols: Camellia, TWINE, Trivium, SIMON, RESENT, PICALO,LEX, LED, CLEFIA, Enocoro 2. Symmetric key or public key: Triple DES, RSA, Blowfish, AES, Elliptic curve.	PRESENT, CLEFIA, SIMON and SPECK (all with key size of 128 bits minimum to meet NIST requirements)	Between Tier1 & Tier2 devices BetweenTier2/Tier3 devices
Integrity/Confidentiality (authenticated encryption)	The Hummingbird-2, Phelix. Fides, ACRON, Grain-128a. SCREAM and iSCREAM, ALE, LAC, ASC-1, Quark , Ascon, Joltik, Ketje, Sablier:	ALE: 128 Photon: Quark Grain-128a (approve by Lightweight Cryptography Working Group [37])	Between Tier1 & Tier2 devices
Possession or Control	Possession of medical sensors and devices plus medical records. Possession of health records and data		Tier 1 Devices Tier3 component and devices
Utility	Comply with (ISO/IEC 62366) ISO/TR 16982:2002 standard		Tier 1 devices Tier 3 network components and devices
Availability	ISO/IEC 62366 Comply with ISO/IEC 24762:2008		Tier 1 devices Tier2 & Tier 3 network components and devices

V. CONCLUSIONS

Advances in mobile devices, medical sensors, and IoT technologies are expected to provide revolutionary innovations in healthcare. However, connecting devices that collect data from patients to wide network are vulnerable to unauthorized access, and patient data must be protected. Therefore, Medical IoT (MIoT) must take in consideration data security and privacy when collecting data and sending data from a device to another.

This paper proposes 3-tier architecture to ease the process of transmitting, storing, and transferring medical data. The lowest layer in the architecture, tier 1, it consists of sensors and devices collecting data from the patient. The middle layer, tier 2, includes smart devices and wireless access points. The last layer, tier 3, contains the servers maintaining healthcare databases.

In order to handle the security issues in the architecture, the architecture is based on the Parkerian Hexad model, which adds three levels of security to the traditional CIA Triad to address the special requirements of health records and data. Sets of algorithms were investigated to recommend the appropriate security level for each layer in the architecture based on capabilities of the devices in that layer to maintain the QoS since the devices have different capabilities in each layer in terms of processing, memory, and power. Table I summarizes those algorithms and recommends the appropriate algorithm in each tier according to Ᵽarkerian Hexad model.

Some of the limitations of the study are concerning patient safety and privacy. In addition, more details of the proposed framework needs to be studied in the future.

REFERENCES

[1] S. Brave and A. Dahley, "inTouch: a medium for haptic interpersonal communication," in CHI'97 Extended Abstracts on Human Factors in Computing Systems, 1997.

[2] K. Ashton, "That 'internet of things' thing," RFID journal, vol. 22, no. 7, pp. 97-114, 2009.

[3] D. V. Dimitrov, "Medical internet of things and big data in healthcare," Healthcare informatics research, vol. 22, no. 3, pp. 156-163, 2016.

[4] H. Banaee, M. Ahmed and A. Loutfi, "Data mining for wearable sensors in health monitoring systems: a review of recent trends and challenges," Sensors, vol. 13, no. 12, pp. 17472-17500, 2013.

[5] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 40, no. 1, pp. 1-12, 2010.

[6] K. Zeitz and H. McCutcheon, "Observations and vital signs: ritual or vital for the monitoring of postoperative patients?," Applied Nursing Research, vol. 19, no. 4, pp. 204-211, 2006.

[7] R. Das, A. Tuna, S. Demirel, K. NETAS AS and M. K. Yurdakul, "A Survey on the internet of things solutions for the elderly and disabled: applications, prospects, and challenges," International Journal of Computer Networks and Applications, vol. 4, no. 3, pp. 1-9, 2017.

[8] C. Li, X. Hu and L. Zhang, "The IoT-based heart disease monitoring system for pervasive healthcare service," Procedia Computer Science, vol. 112, pp. 2328-2334, 2017.

[9] B. Singh, S. Bhattacharya, C. L. Chowdhary and D. S. Jat, "A review on internet of things and its applications in healthcare," Journal of Chemical and Pharmaceutical Sciences, vol. 10, no. 1, pp. 447-452, 2017.

[10] E. Rich and A. Miah, "Mobile, wearable and ingestible health technologies: towards a critical research agenda," Health sociology review, vol. 26, no. 1, pp. 84-97, 2017.

[11] P. Belluck, "First Digital Pill Approved to Worries About Biomedical 'Big Brother'," New York Times, 2017.

[12] A. J. Jara, F. J. Belchi, A. F. Alcolea, J. Santa, M. A. Zamora-Izquierdo and A. F. Gómez-Skarmeta, "A Pharmaceutical Intelligent Information System to detect allergies and Adverse Drugs Reactions based on internet of things," in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on, 2010.

[13] M. Kang, E. Park, B. H. Cho and K.-S. Lee, "Recent patient health monitoring platforms incorporating internet of things-enabled smart devices," International neurourology journal, vol. 22, no. Suppl 2, p. S76, 2018.

[14] V. Kalaiselvan, P. Kumar, P. Mishra and G. Singh, "System of adverse drug reactions reporting: What, where, how, and whom to report?," Indian Journal of Critical Care Medicine, vol. 19, no. 9, p. 564, 2015.

[15] M. A. Ward, M. L. Schweizer, P. M. Polgreen, K. Gupta, H. S. Reisinger and E. N. Perencevich, "Automated and electronically assisted hand hygiene monitoring systems: a systematic review," American journal of infection control, vol. 42, no. 5, pp. 472-478, 2014.

[16] U. Lindqvist and P. G. Neumann, "The future of the Internet of Things," Communications of the ACM, vol. 60, no. 2, pp. 26-30, 2017.

[17] U. K. Anaesthesia, "Principles of pulse oximetry," Anaesthesia UK, 2004.

[18] R. Rutherford, "Internet of Things–striking the balance between competition and security," Network Security, vol. 2019, no. 2, pp. 6-8, 2019.

[19] D. Salvi, E. V. Mora and M. T. A. Waldmeyer, "An architecture for secure e-Health systems," Universidad Politecnica de Madrid, Spain, vol. 1, pp. 2-4, 2010.

[20] D. Lake, R. M. R. Milito, M. Morrow and R. Vargheese, "Internet of things: Architectural framework for ehealth security," Journal of ICT Standardization, vol. 1, no. 3, pp. 301-328, 2014.

[21] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network," IEEE Sensors Journal, vol. 16, no. 5, pp. 1368-1376, 2016.

[22] S. Khoja, H. Durrani, R. E. Scott, A. Sajwani and U. Piryani, "Conceptual framework for development of comprehensive e-health evaluation tool," Telemedicine and e-Health, vol. 19, no. 1, pp. 48-53, 2013.

[23] F. Rezaeibagha, K. T. Win and W. Susilo, "A systematic literature review on security and privacy of electronic health record systems: technical perspectives," Health Information Management Journal, vol. 44, no. 3, pp. 23-38, 2015.

[24] W. Leister, M. Hamdi, H. Abie and S. Poslad, "An evaluation framework for adaptive security for the iot in ehealth," International Journal on Advances, 2014.

[25] O. Olakanmi, I. Kamil and S. Ogundoyin, "Secure and privacy-preserving referral framework for e-health system," Internal Journal of Information Science, vol. 6, no. 2, pp. 11-25, 2017.

[26] D. Y. Weider, L. Davuluri, M. Radhakrishnan and M. Runiassy, "A security oriented design (SOD) framework for ehealth systems," in 2014 IEEE 38th International Computer Software and Applications Conference Workshops, 2014.

[27] D. P. Mirembe, "Design of a secure framework for the implementation of telemedicine, eHealth, and wellness services," 2006.

[28] B. Ondiege, M. Clarke and G. Mapp, "Exploring a new security framework for remote patient monitoring devices," Computers, vol. 6, no. 1, p. 11, 2017.

[29] B. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins and R. Jardim-Goncalves, "An Ontology-Based Cybersecurity Framework for the Internet of Things," Sensors, vol. 18, no. 9, p. 3053, 2018.

[30] H. Mora, D. Gil, R. M. Terol, J. Azorín and J. Szymanski, "An IoT-based computational framework for healthcare monitoring in mobile environments," Sensors, vol. 17, no. 10, p. 2302, 2017.

[31] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi and L. Tarricone, "An IoT-aware architecture for smart healthcare systems," IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515-526, 2015.

[32] Richard Piggin, "Cybersecurity of medical devices," 2017.

[33] M. Al Ameen, J. Liu and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," Journal of medical systems, vol. 36, no. 1, pp. 93-101, 2012.

[34] W. H. Organization, S. P. f. Research, T. i. T. Diseases, W. H. O. D. o. C. o. N. T. Diseases, W. H. O. Epidemic and P. Alert, Dengue: guidelines for diagnosis, treatment, prevention and control, World Health Organization, 2009.

[35] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estévez-Tapiador and A. Ribagorda, "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags," in Proc. of 2nd Workshop on RFID Security, 2006.

[36] Sandrine Agagliate, "ALIKE: Authenticated Lightweight Key Exchange," 2010.

[37] K. McKay, L. Bassham, M. Sönmez Turan and N. Mouha, "Report on lightweight cryptography," National Institute of Standards and Technology, 2016.

[38] D. Galindo and F. D. Garcia, "A schnorr-like lightweight identity-based signature scheme," in International Conference on Cryptology in Africa, 2009.

[39] M. N. Aman, B. Sikdar, K. C. Chua and A. Ali, "Low Power Data Integrity in IoT Systems," IEEE Internet of Things Journal, 2018.

[40] J. Guo, T. Peyrin and A. Poschmann, "The PHOTON family of lightweight hash functions," in Annual Cryptology Conference, 2011.

[41] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varıcı and I. Verbauwhede, "SPONGENT: A lightweight hash function," in International Workshop on Cryptographic Hardware and Embedded Systems, 2011.

[42] S. Hirose, K. Ideguchi, H. Kuwakado, T. Owada, B. Preneel and H. Yoshida, "A lightweight 256-bit hash function for hardware and low-end devices: lesamnta-LW," in International Conference on Information Security and Cryptology, 2010.

[43] A. Buldas, A. Kroonmaa and R. Laanoja, "Keyless Signatures' Infrastructure: how to build global distributed hash-trees," in Nordic Conference on Secure IT Systems, 2013.

[44] A. Buldas, R. Laanoja and A. Truu, "Keyless signature infrastructure and PKI: hash-tree signatures in pre-and post-quantum world," International Journal of Services Technology and Management, vol. 23, no. 1-2, pp. 117-130, 2017.

[45] J. M. Roman-Belmonte, H. De la Corte-Rodriguez and E. C. Rodriguez-Merchan, "How blockchain technology can change medicine," Postgraduate medicine, vol. 130, no. 4, pp. 420-427, 2018.

[46] J. Nakajima and S. Moriai, A Description of the Camellia encryption Algorithm, Aug, 2000.

[47] T. Suzaki, K. Minematsu, S. Morioka and E. Kobayashi, "Twine: A lightweight, versatile block cipher," in ECRYPT Workshop on Lightweight Cryptography, 2011.

[48] C. De Canniere and B. Preneel, "Trivium," in New Stream Cipher Designs, Springer, 2008, pp. 244-266.

[49] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith and L. Wingers, "The SIMON and SPECK lightweight block ciphers," in Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, 2015.

[50] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," in International Workshop on Cryptographic Hardware and Embedded Systems, 2007.

[51] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita and T. Shirai, "Piccolo: an ultra-lightweight blockcipher," in International Workshop on Cryptographic Hardware and Embedded Systems, 2011.

[52] A. Biryukov, "A new 128-bit key stream cipher LEX," eSTREAM, ECRYPT Stream Cipher Project, Report, vol. 13, p. 2005, 2005.

[53] M. R. Jian Guo, Thomas Peyrin,Axel Poschmann, "The LED Block Cipher," in Selected Areas in cryptography , 2011.

[54] T. Shirai, K. Shibutani, T. Akishita, S. Moriai and T. Iwata, "The 128-bit blockcipher CLEFIA," in International Workshop on Fast Software Encryption, 2007.

[55] D. Watanabe, K. Ideguchi, J. Kitahara, K. Muto, H. Furuichi and T. Kaneko, "Enocoro-80: A hardware oriented stream cipher," in The Third International Conference on Availability, Reliability and Security, 2008.

[56] D. Engels, M.-J. O. Saarinen, P. Schweitzer and E. M. Smith, "The Hummingbird-2 lightweight authenticated encryption algorithm," in International Workshop on Radio Frequency Identification: Security and Privacy Issues, 2011.

[57] D. Whiting, B. Schneier, S. Lucks and F. Muller, "Fast encryption and authentication in a single cryptographic primitive," ECRYPT Stream Cipher Project Report, vol. 27, no. 200, p. 5, 2005.

[58] B. Bilgin, A. Bogdanov, M. Knežević, F. Mendel and Q. Wang, "Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware," in International Workshop on Cryptographic Hardware and Embedded Systems, 2013.

[59] P. Dey, R. S. Rohit and A. Adhikari, "Full key recovery of ACORN with a single fault," Journal of Information Security and Applications, vol. 29, pp. 57-64, 2016.

[60] M. ? gren, M. Hell, T. Johansson and W. Meier, "Grain-128a: a new version of Grain-128 with optional authentication," International Journal of Wireless and Mobile Computing, vol. 5, no. 1, pp. 48-59, 2011.

[61] V. Grosso, G. Leurent, F.-X. Standaert, K. Varici, F. Durvaux, L. Gaspar and S. Kerckhof, "SCREAM & iSCREAM side-channel resistant authenticated encryption with masking," Submission to CAESAR, 2014.

[62] J. Jean, T. Peyrin, S. M. Sim and J. Tourteaux, "Optimizing implementations of lightweight building blocks," IACR Transactions on Symmetric Cryptology, vol. 2017, no. 4, pp. 130-168, 2017.

[63] L. Zhang, W. Wu, Y. Wang, S. Wu and J. Zhang, "LAC: A lightweight authenticated encryption cipher," Submitted to the CAESAR competition, 2014.

[64] G. Jakimoski and S. Khajuria, "ASC-1: an authenticated encryption stream cipher," in International Workshop on Selected Areas in Cryptography, 2011.

[65] J.-P. Aumasson, L. Henzen, W. Meier and M. Naya-Plasencia, "Quark: A lightweight hash," in International Workshop on Cryptographic Hardware and Embedded Systems, 2010.

[66] C. Dobraunig, M. Eichlseder, F. Mendel and M. Schläffer, "Ascon v1. 2," Submission to the CAESAR Competition, 2016.

[67] J. Jean, I. Nikolić and T. Peyrin, "Joltik v1. 3," CAESAR Round, vol. 2, 2015.

[68] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche and R. Van Keer, "CAESAR submission: Ketje v1, March 2014," URL http://ketje. noekeon. org/Ketje-1.1. pdf.[cited at p. 44, 48, 49, and 67].

[69] B. Zhang, Z. Shi, C. Xu, Y. Yao and Z. Li, "Sablier v1," Candidate for the CAESAR Competition. See also https://competitions. cr. yp. to/round1/sablierv1. pdf, 2014.

[70] K. Judson, "Law & ethics for medical careers," 2002.

[71] D. A. Grant, "MDs still confused about patient access to medical records," CMAJ: Canadian Medical Association Journal, vol. 158, no. 9, p. 1126, 1998.

[72] I. I. O. f. Standardization, ISO/TS 20282-2: 2013 (en). Usability of consumer products and products for public use—Part 2: Summative test method, 2013.

[73] P. Hodgson, "Usability for medical devices: A new international standard," URL http://www. userfocus. co. uk/articles/ISO62366. html, 2010.

[74] M. E. Wiklund, J. Kendler and A. Y. Strochlic, Usability testing of medical devices, CRC press, 2015.

[75] N. Bevan, "Guidelines and standards for web usability," in Proceedings of HCI international, 2005.

[76] A. Tsohou, S. Kokolakis, C. Lambrinoudakis and S. Gritzalis, "Information systems security management: a review and a classification of the ISO standards," in International Conference on e-Democracy, 2009.

[77] N. Innab, "Availability, Accessibility, Privacy and Safety Issues Facing Electronic Medical Records".