Issues in Information Systems
Volume 22, Issue 2, pp. 63-72, 2021

DOI: https://doi.org/10.48009/2_iis_2021_63-73

Security implications in the transformation of healthcare through internet of things devices

George Ray, *Shepherd University, gray@shepherd.edu*
Ephais Ruhode, *Cape Peninsula University of Technology, ruhodee@cput.ac.za*
Albert Mubako, *Institute for Digital Business Strategy, albert.mubako@institutedbs.com*
Jeff Ray, *University of Maryland, jeffray@umbc.edu*
Walter Kashiri, *Institute for Digital Business Strategy, walter.kashiri@institutedbs.com*

Abstract

Africa has a growing industry producing medical devices for the developing world that are ASSURED: Affordable, Sensitive, Specific, User-friendly, Rapid, Equipment-free and Deliverable to end-users. This industry and more generally healthcare in Africa benefits by adding security to ASSURED. This paper investigates two questions related to security for IoT medical solutions: 1.) What are the vulnerable security points in an IoT based medical system; and 2.) How can these vulnerabilities be hardened? To answer these questions, a security reference architecture is identified that can be the framework for identifying, understanding, teaching and mitigating threats in the various modules of an IoT healthcare solution.

Keywords: Internet of Things, Information Security, Healthcare

Introduction

The use of Internet of Things (IoT) devices is expanding into all industrial sectors. In healthcare such devices are used to monitor patient vital signs and apply artificial intelligence to analyze the data. The global market for IoT healthcare devices is forecast to grow at an annual rate of 25.9% between 2021 and 2028 (Fortune Business Insights, 2021). In addition, Africa is expected to experience the fastest growth rate in the use of IoT medical systems (Singh, 2019). Africa has a thriving industry in medical devices for the developing world that are ASSURED: Affordable, Sensitive, Specific, User-friendly, Rapid, Equipment-free and Deliverable to end-users (Mtamzeli, 2020).

IoT systems generally are susceptible to hacking attacks that exploit security vulnerabilities. This is more pronounced in healthcare because of privacy concerns. Proposals have been presented on securing IoT communications to protect patient confidentiality (Han & Bae, 2021). Innovative companies at the for-front of the African medical devices industry could greatly benefit from a comprehensive framework to perform security analysis of medical devices as well as disseminate findings. This paper examines the complete architecture of an IoT solution for security vulnerabilities and recommends hardening approaches.

Methodology

The research approach for this article is an Integrative Literature Review. This is a research method that synthesizes existing literature to gain a more comprehensive understanding of an issue. As it pertains to

healthcare, an Integrative Review is conducted to improve practice and contribute further to policy on a topic (Whittemore & Knafl, 2005). The methodology consists of framing a question, purposeful selection of literature to provide insights on the question, and synthesis of the literature to propose answers to the research question.

The healthcare research question this paper investigates is in two parts: 1.) What are the vulnerable security points in a IoT based medical system; and 2.) How can these vulnerabilities be hardened? The authors selected literature to obtain insights into the nature of the architecture of IoT systems, discover security vulnerabilities and understand approaches to harden such vulnerabilities. The appraisal of the literature was based on the experience the authors have in teaching information security at university undergraduate and graduate levels as well as the development of embedded systems, IoT systems, and the use of sensors and machine learning in Smart Cities. The synthesis is in the form of a narrative presented in the results section.

Results

Security vulnerabilities in IoT healthcare systems

A complete view of IoT security vulnerabilities begins with an understanding of the architecture of IoT systems. In addition, threats facing IoT systems must be understood so that the vulnerabilities can be identified. The architecture consists of sensors, gateways, applications and the platform. These will be explored in more depth to better understand the threats and vulnerabilities.

IoT Architecture

IOT devices perform enactment with their environment, which at a minimum is the collection of information about that environment through sensors but may also involve enacting strategies in the environment through actuators (Weick, 1979). This involves communication of data, its analysis, communication of resulting instructions, presentation of data driven functionality to users, storage of data, and interfacing with other facility systems. The architecture of the system that includes the medical device and its integration into the facility can be organized into four parts: 1.) devices; 2.) gateways; 3.) applications; and 4.) platform (Lea, 2018; Tamboli,2019). These are the four partitions of a medical device architecture and are shown in Figure 1.

Sensors and Gateways

Sensors and actuators are the core of the devices (Abed, 2017; Hegde, 2016; Uviase & Kotonya, 2018). The purpose of a sensor is to measure various health related properties and translate them into electrical or digital data. The purpose of an actuator is to take electrical or digital data and perform an appropriate action in the environment.

Gateways are needed by devices, which are embedded in the physical environment, to communicate with the facility information processing environment. Some devices can communicate with an IP gateway using communication protocols such as REST, MQTT, AMQP, CoAP, and other protocols that will be identified and maintained in the repository (Lea, 2018; Tamboli, 2019). Other devices are not capable of direct IP connectivity and they utilize gateways with dual communication technologies: one to enable communication with the sensors or actuators downstream, and the other to communicate upstream.
Typical gateways in this category use technologies like GSM and RF, GSM and Bluetooth, WiFi and Xbee, LoRaWAN and Ethernet (Hillar, 2018; Lea, 2018; Tamboli, 2019). Gateways may also perform data aggregation, deduplication, clean-up and other edge computing services.

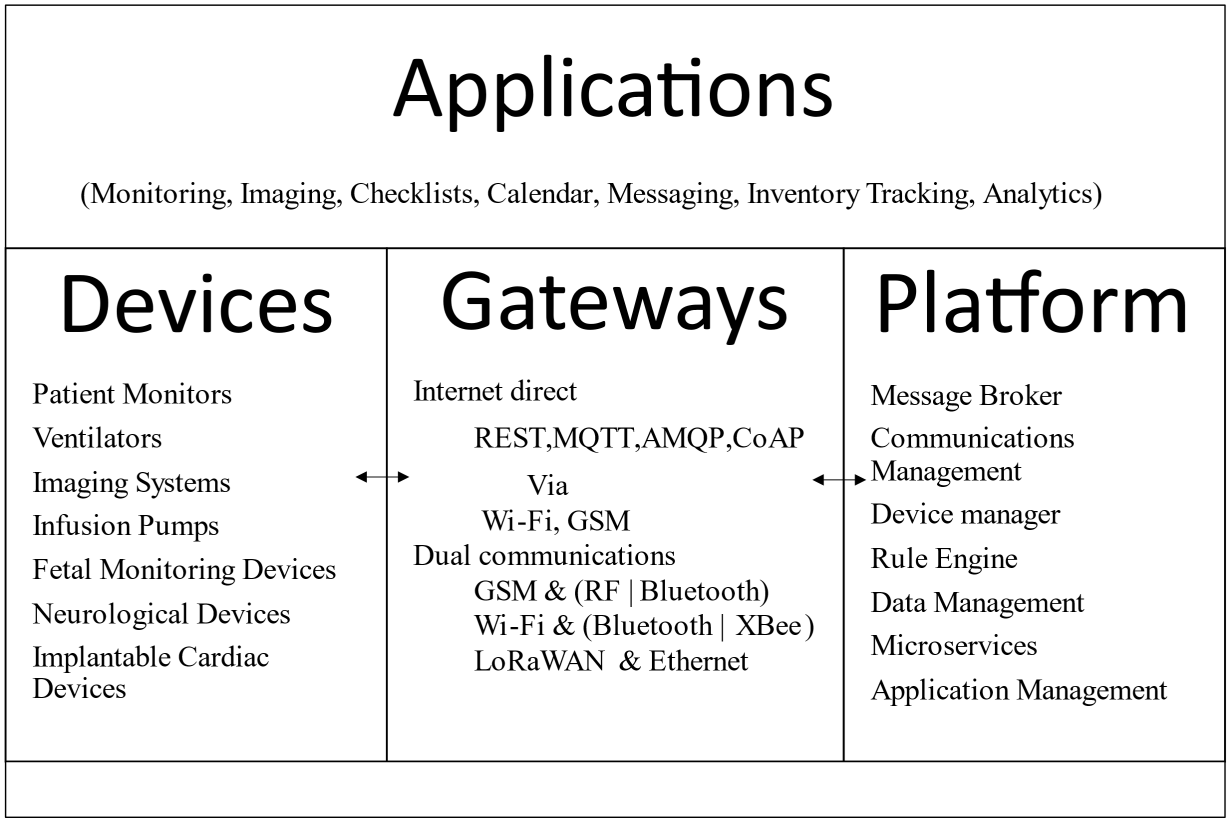

Figure 1. IoT architecture

To illustrate how an IoT based system can be compromised and information accessed without authorization, Englender (2017) describes the approach taken to access signals of a commercial alarm system that might be found in a hospital. The process of intercepting a signal depends on the protocols used, but this is representative of IoT vulnerability.

Governmental communication authorities require vendors to submit detailed descriptions of their devices including the operating frequency, circuit diagrams and protocols used. With many IoT based devices sold and used in the United States, the Federal Communications Commission (FCC) of the US government is a source of useful information on compromising IoT devices. A simple search on a system of interest yields the manual submitted to the FCC and an FCC ID for the device (FCC, 2021). With the obtained FCC ID (CFS8DL5800TM-1 in this example) the FCC.IO site yields block diagrams, circuit diagrams, operating frequencies, protocols, test plans and other useful insights into the operation of the device.

Decoding the signal of the IoT device can be accomplished on a standard PC using Python or C programming languages along with an RTL-SDR transceiver (Laufer, 2014). The sensor transmission is captured by RTL-SDR, the raw bytes converted to bits and the protocol used by the sensors is then applied (Endlender, 2017). Using this information, Englender then detailed how to compromise the commercial alarm system. In addition to IoT devices, a wide variety of other signals can be intercepted, decoded and analyzed including aircraft transponders and avionics communicating with the air traffic control system, train telemetry, maritime identification system, satellites and P25 communication networks.

Applications and IoT platform
Applications present functions to the end user that are relevant for the sensor data. They also enhance the data through analysis and can apply classic as well as state-of-the-art machine learning algorithms. Applications also present data to other systems and enable inter-application data exchange (Dang, 2019).

The Platform arranges or directs the elements of an IOT architecture to produce a desired effect, orchestrating the operation (Bauer & Bui, 2013). These platforms can be hosted on the cloud and increasingly this is a popular option because of the IOT framework services offered by major cloud vendors such as Amazon AWS and Microsoft Azure. This part of the architecture communicates with the downstream devices through gateways to ingest potentially large amounts of data. The platform stores data appropriately for further analysis.

In Africa, the platform will work with the health systems which have been deployed within the African context such as HISP, DHIS, DHIS2, and others such as Jembi. Jembi is from the Medical Research Council and facilitates links between country programs on the African continent and the wider international open-source communities (Jembi, 2019).

Threats in Healthcare IOT
We can categorize threats as: threats to devices, threats to gateways, platform threats, and application threats. Malicious data can be sent to and from gateways (Salter, 2019; Symantec, 2016; Whitman & Mattord, 2014). Likewise, sensitive data can be intercepted going to or from gateways. Consider the case of a gateway with GSM and Bluetooth for upstream and downstream communications. If the version of Bluetooth on the device does not support encryption there is a vulnerability in the communication between sensor and gateway.

Likewise, device vendors may choose to not use code signature verification and secure boot so that malicious code may be installed on the devices such as backdoors, sniffers, data collection software, and data transfer software (Symantec, 2016). In turn, applications may have weak verification models that can be easily bypassed, which means they can be induced to trust malicious systems. The first device compromised can remain trusted, and so become a vehicle for compromising the rest of the IOT platform (McKinsey&Company, 2020; Symatntec, 2016; Whitman & Mattord, 2014) or even the healthcare facility IT system.

Platforms may fail to encrypt the data so it can be intercepted in the clear during transmission or at rest. Likewise, a threat may come over the Internet, through the Platform to the downstream devices. It is important to examine the interactions within each part of the architecture, because those interactions are potential vulnerabilities.

Vulnerabilities
IOT systems are vulnerable to the following threats (Hillar, 2018; Lea, 2018; McKinsey&Company, 2020; Slater 2019; Symantec, 2016; & Tamboli, 2019; Whitman & Mattord, 2014):

1. Malicious data sent across connections
2. Sensitive data read across connections
3. Vulnerabilities and misconfigurations being exploited
4. Malicious code from lack of code signature verification and secure boot
5. Poorly implemented verification models which can be bypassed.
6. Use of weaknesses to install
    a) Backdoors

b) Sniffers
c) Data collection software
d) File transfer capabilities to disseminate sensitive information out of the system
e) Malicious software that loads directly into the memory of a running IoT and disappears on re-boot, doing extensive damage while active

7. Attacks on these vulnerabilities can come through:
a) An internal IT network connected to an industrial or IoT network.
b) Over the Internet
c) Through direct physical access to the device.
d) Unsecured gateway communications

Trusted devices that become infected are a pathway for infecting other parts of the network. It is critical that all the potential vulnerabilities be mitigated. This may be difficult in the healthcare industry where vendors often bar medical facilities from modifying the equipment, even to add security. It is important to have a security assessment upfront. Potential vulnerabilities are summarized in Figure 2.

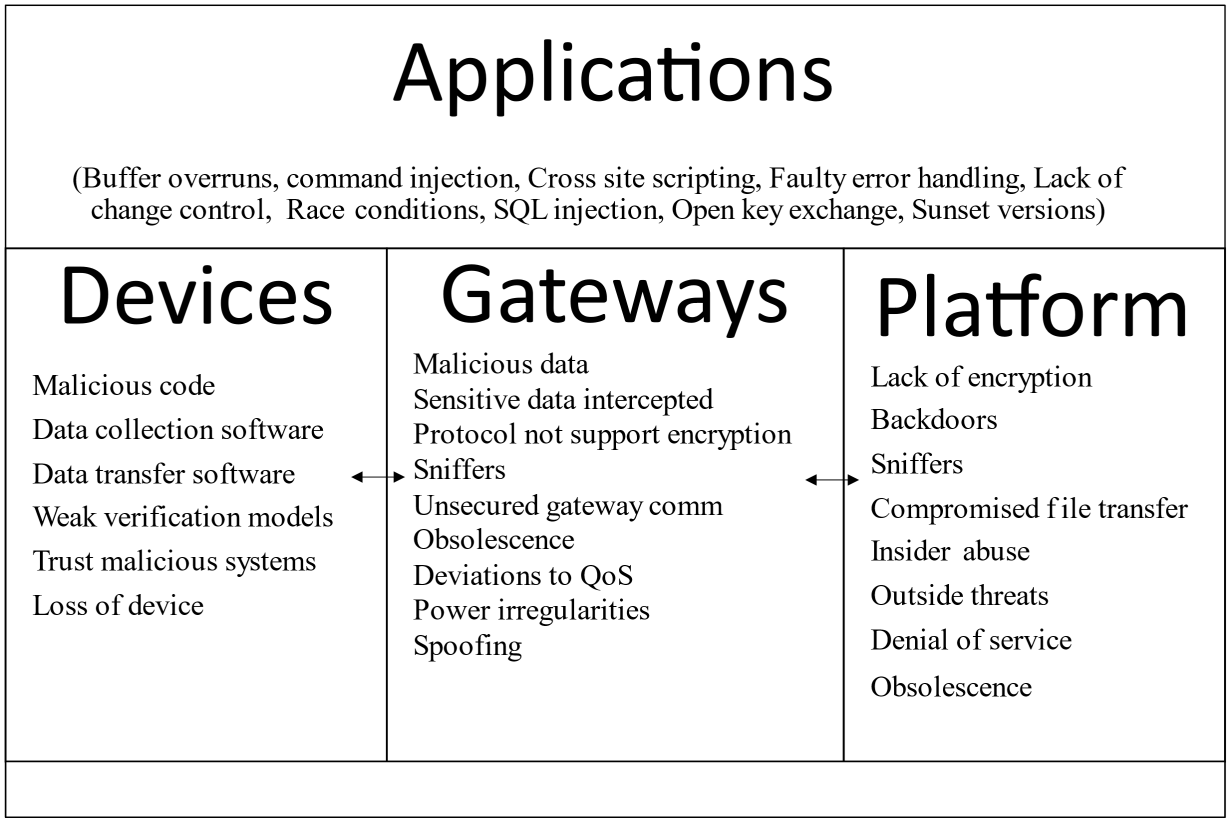

Figure 2. IoT architecture vulnerabilities

Hardening Approaches

The general principles to harden a healthcare IOT system are first protection and second detection and response. Protection must cover all facets of the IOT system including the medical device, the communications, gateways, the applications and must continue to protect in the future with over the air (OTA) device management to update the applications and firmware (Lea, 2018). This can be accomplished with code signing, data encryption, authentication, application authentication, and authorization. Violating the protection principle in any of its facets makes the medical device vulnerable to attack.

There are numerous protocols that can be used to protect the four blocks of an IoT solution and the interfaces between them. One example is Message Queue Telemetry Transport protocol (MQTT), which is a distributed computing system with three components: 1.) a broker; 2.) a publisher; and 3.) a subscriber. A publisher circulates messages on topics through the broker to appropriate clients that subscribe to the topics (Eclipse Foundation, 2021). The topic messages can be medical device readings, images, configuration settings or instructions to the device to perform some action. Transport Layer Security or Secure Socket Layer protocols can be used to secure communications across the components in an MQTT link. X509 certificates can be generated with Openssl and those certs added to the MQTT configuration (Lea, 2018). With this done, the transmissions over the MQTT link will be encrypted.

Part of protection is identifying trustworthy components. Device certificates can also be used to establish lineage and authenticity of a device. Likewise, the pedigree of communications can be established by applying certificates to encrypt messages so that at decryption it will be clear if the communication is from a trusted source (Symantec, 2016; Whitman & Mattord, 2014).

In addition to protection, tools that detect irregularities in operational traffic, code dates and sizes or other irregularities are important to medical device security. The IOT network must be baselined and machine learning (ML) applied to detect anomalies. Even with the wide variety of protocols used in IOT, modern ML can work on the IOT for intrusion detection. Intrusion prevention and detection is less invasive in detect mode such that false positives have minimal impact on the system (McKinsey&Company, 2020; Symantec, 2016; Whitman & Mattord, 2014).

A medical device must have capabilities for secure system function (Lea, 2018; Symantec, 2016; Whitman & Mattord, 2014). A critical aspect is code-signing and configuration signing for ensuring the integrity of the device by verifying information transferred for these purposes is authorized. Another critical aspect is a key management system to easily use public-key encryption to create and distribute cryptographic keys. Telemetry management and control must include physical security, sensor range, access point and wireless switch locations and wired network interfaces.

Sensor telemetry data for IOT devices must be securely transmitted across a variety of signals such as radio frequency, Bluetooth, WiFi, Xbee, LoRaWAN and Ethernet. This includes the ability to securely aggregate telemetry for device-based technologies to protect measurements of various health related properties that are translated into electrical or digital data. The other aspect of enactment to be covered is device-based technology that takes upstream electrical or digital data to perform an appropriate action in the environment through the use of actuators.

Code management guidelines have been published by the Open Web Application Security Project (OWASP) for dependable software and configuration management over the air (OTA). In similar manner, the Open Mobile Alliance has published standards to inventory device configurations on IoT devices. Standard information security approaches can be used to harden the central platform that reads downstream sensor data or sends downstream instructions to actuators (Whitman, Mattord, 2014; Newman, 2010). Mitigations are summarized in Figure 3.

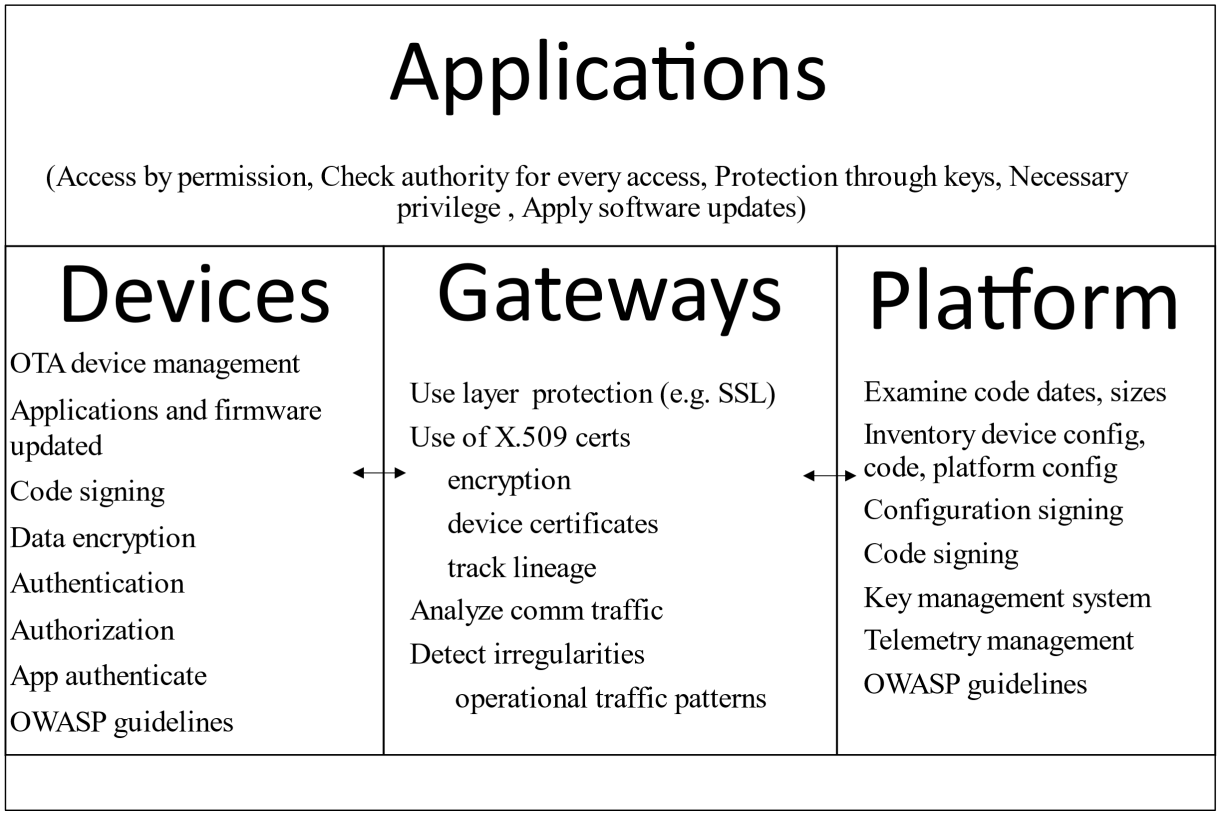

Figure 3. IoT architecture hardening

Discussion

IoT devices composed of sensors and actuators are here to stay both in healthcare and a myriad of other uses in smart cities. Information will increasingly be obtained directly from purposefully deployed sensors or indirectly from sensors deployed for another purpose but which gather and share useful information. With this information, freely exchanged, complex systems can be managed in real-time and, with sufficient integration, to minimize unintended consequences (Maddox, 2016). As dependence on sensors grows, so to will the need that they be secure and that the systems to which they are connected will be able to securely integrate with them. This paper has identified vulnerabilities in the IoT solution architecture and in the process identified a medical device security model based on an architecture with four partitions and examined the potential security threats and proposed mitigations for hardening the systems.

A potential use of a security architecture model is to create a threat information collection system for healthcare and to assemble, examine, and disseminate information on medical device security across the entire healthcare system. The model can also be extended to investigate the connection between IOT medical devices and the existing medical facility IT network where it is installed to identify different threats, and recommend risk mitigations.

There are many IOT architectural patterns, but most provide similar functionality, under differing branded names. A variety of IoT frameworks are in existence today to include: Amazon IOT Reference Architecture; Azure IOT Reference Architecture; Calvin Framework; SOCRADES; AllJoyn; FRASAD; ARIoT; AVIoT; HP Edge; Watson IOT; as well as custom architectures for unique solutions. There are

over 500 IOT platform combinations in the market today (Tamboli, 2019, p.3) using a variety of communication protocols, applications, and gateways.

These various combinations could be mapped to the four blocks in the model described in this paper. Doing so would enable the application of the security vulnerabilities identified in the results section along with hardening approaches to this diversity of architectures available from device vendors. Security consultants can overlay the security architecture on the framework used by the vendor of the healthcare device and apply an analytic methodology to appraise that device using the answers to the two research questions.

References

Abed, A. (December 2017). Internet of Things (IoT): Architecture and Design. Computer Engineering Department/University of Basra

Bauer, B., M. Boussard, N. Bui, J. DeLoof, C. Margerkurth, S. Meissner, A. Nettstrater, J. Stefa, M. Thoma, & J. Walewsk (2013). IoT Reference Architecture. Enabling Things to Talk, DOI 10.1007/978-3-642-40403-0_8,

Benadda, B. (2018). Secure IoT solution for wearable health care applications, case study Electric Imp development platform. Int J Commun Syst. 2018;31:e3499

Dang, L., P. Piran, D. Han, K. Min, & H. Moon (June 10, 2019). A Survey on Internet of Things and Cloud Computing for Healthcare. Electronics 143-747(05006

Darwish, D. (August 2015). Improved Layered Architecture for Internet of Things. International Journal of Computing Academic Research (IJCAR) Volume 4, Number 4, pp.214-223

Donnelly, C. (November 2015). Philips uses AWS and IoT to deliver healthcare in the home. Computer Weekly

Eclipse Foundation (2021). Eclipse Mosquitto: An open source MQTT broker. Retrieved from https://mosquitto.org/

Englender, D. (2017). Honeywell 345 Mhz Protocol. Retrieved from https://denglend.github.io/decode345/

Federal Communications Commission (2021). 8DL5800TM-1 security transmitter User Manual N6716V2_RevD Honeywell. Retrieved from https://fccid.io/CFS8DL5800TM-1/User-Manual/II-with-FCC-Part-15-Statment-581102.

Fortune Business Insights (June 2021). Internet of things (IoT) in Healthcare Market Size, Share & COVID-19 Impact Analysis, By Component (Devices, Software, and Services), By Application (Telemedicine, Patient Monitoring, Operations and Workflow Management, Remote Scanning, Sample Management, and Others), By End-User (Laboratory Research, Hospitals, Clinics, and Others), and Regional Forecast, 2021-2028. Fortune Business Insights, Report ID: FBI102188.

Han, K. & W. Bae (2021). Proposing and verifying a security-enhanced protocol for IoT-based communication for medical devices. Cluster Computing; 20210101, Issue: Number Preprints p1-7, 7p.

Hegde, S. (May 2016). Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges. 1st International Conference on Innovations in Computing & Networking (ICICN16), CSE, RRCE

Hillar, G. (May 22, 2018). Hands-On MQTT Programming with Python: Work with the lightweight IoT protocol in Python. Packt Publishing; 1st edition.

Jembi (2019). Work We Are Doing. Jembi.org

Laufer, C (2014). Hobbyist Guide to RTL-SDR. RTL-SDR.com

Lea, P. (January 22, 2018). Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security. Packt Publishing; 1st edition

Lea, P. (March 6, 2020). IoT and Edge Computing for Architects: Implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security. Packt Publishing; 2nd edition

Maddox, T. (2016). Smart cites: 6 essential technologies. Innovation

Mastoi, Q., T. Wah, R. Raj,& A. Lakham (2020) A Novel Cost-Efficient Framework for Critical Heartbeat Task Scheduling Using the Internet of Medical Things in a Fog Cloud System. Sensors 2020, 20, 441; doi:10.3390/s20020441

McKinsey&Company (2020). Cybersecurity in a Digital Era. McKinsey&Company.

Miranda, J., J. Cabral, S. Wagner, B. Ravelo, M. Memon, M. Mathiesen & C. Peterson (2016) An Open Platform for Seamless Sensor Support in Healthcare for the Internet of Things. Sensors, 16, 2089; doi:10.3390/s16122089

Monowar, M & M. Alassaf (2020). On the Design of Thermal-Aware Duty-Cycle MAC Protocol for IoT Healthcare. Sensors, 20, 1243; doi:10.3390/s20051243

Mtamzeli, B. (2020). NEXTGEN HEALTH. Council for Scientific and Industrial Research.

Newman, R. (2010). Security and Access Control Using Biometric Technologies. Cengage.

NIST 800-14 (1996). Generally Accepted Principles and Practices for Securing Information Technology Systems. U.S. Government Printing Office.

Reistad, B. (2018). Microsoft Azure IoT Reference Architecture Version 2.1. Microsoft

Saldeen, Y. & K. Qureshi (June 2018). New Trends in Internet of Things, Applications, Challenges, and Solutions. TELKOMNIKA, Vol.16, No.3, pp. 1114~1119

Singh, S. (October 8, 2019). IoT Medical Devices Market worth $63.43 Billion by 2023. M2PressWIRE. Accession Number: 16PU1021413193

Slater, D. (2019). Create smarter operations by capturing, analyzing and acting upon data where it's created — at the Intelligent Edge. Hewlett Packard Enterprise.

Slobodyan Y. & S. Haziyev (2016). Internet of Things Reference Architecture & Case Studies. Software Engineering Institute, Carnegie Mello University

Symantec (2016). An Internet of Things Reference Architecture. Symantec

Tamboli, A. (April 29, 2019). Build Your Own IoT Platform: Develop a Fully Flexible and Scalable Internet of Things Platform. Amazon Kindle.

Takabayashi, K. (2019). Integrated Performance Evaluation of the Smart Body Area Networks Physical Layer for Future Medical and Healthcare IoT. Sensors, 19, 30; doi:10.3390/s19010030

Uviase , O. & G. Kotonya (2018). IoT Architectural Framework: Connection and Integration Framework for IoT Systems. First workshop on Architectures, Languages and Paradigms for IoT. EPTCS 264, 2018, pp. 1–17, doi:10.4204/EPTCS.264.1

Weick, K. (1979). The Social Psychology of Organizing. New York, NY: McGraw-Hill

Whitman, M. & H. Mattord (2014). Principles of Information Security. Cengage Learning.

Whittemore, R. & K. Knafl (December 2005). The integrative review: updated methodology. Journal of Advanced Nursing, Volume52, Issue5, Pages 546-553. Wiley.

Youngblood, G. (July 2002). A Software-Defined Radio for the Masses. QEX