ISSN: 2458-8989

Natural and Engineering Sciences

Supplement, 2018, 3(3):12-22

-REVIEW ARTICLE-

Data Security and Privacy Issues of Implantable Medical Devices

Yalcin Isler[1,4*], Lutfu Tarkan Olcuoglu[2], Mustafa Yeniad[3]

[1] Department of Biomedical Engineering, Izmir Katip Celebi University, Turkey
[2]Evaluation, Selection & Placement Centre, Turkey
[3]Department of Computer Engineering, Ankara Yildirim Beyazit University, Turkey
[4] Islerya Medical and Information Technologies Company, Turkey

Abstract

Implantable medical devices (IMDs) have a great improvement over the last decade. They have access to human health data at any time. They also regulate the problems in the human body. The most common IMDs are namely, insulin pumps, cardiac pacemakers, and so on. Since IMDs are directly affect human health, the primary design criterion of such devices includes the effectiveness of human health. On the other hand, there is a strong trend in using the Internet of Things (IoT) based Industry 4.0 principles in medical devices. However, the data security and privacy issues of those devices are not adequately addressed yet. In this work, we will summarize the related literature and show the state-of-art situation.

Keywords:
Implantable medical device, Security, Privacy, Cryptographic systems

Article history:
Received 15 November 2018, Accepted 25 December 2018, Available online 30 December 2018

* *Corresponding Author: Yalcin Isler, e-mail: yalcin@islerya.com*

Introduction

As the connected devices through the internet increased around the world and our lives go online, data is accessed in many innovative and new techniques such as the Internet of Things (IoT). IoT is a recent communication paradigm that envisions a near future, in which the objects of everyday life will be equipped with microcontrollers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, becoming an integral part of the Internet (Zanella et al. 2014). IoT (Internet of things) is the combination of a variety of information sensing devices such as radio frequency identification (RFID) devices, infrared sensors, global positioning systems, and Internet IoT devices can be classified further into two categories (Das et al. 2012):

- **Physical objects:** These can be the smartphone, camera, sensor, vehicle, drone, and so on.
- **Virtual objects:** These include the electronic ticket, agenda, book, wallet, and so on.

The information accessed by the IoT devices can be also accessed by various users (e.g., a smart home user in a home application and a doctor in a health-care application) (Gubbi et al. 2013). Data sharing and cloud computing initiatives are also rising, data and resources often no longer reside only in the internal network. Gartner Inc. (Information Matters 2018) forecasts that the number of connected IoT devices will reach 20.4 billion by the year 2020. With the adoption of different information sources, the growing volume and sensitivity of data being stored necessitate about how data is being protected and also managed. Hence, data security and its privacy have become very important and caused reputation issues and is an essential topic of information technology (IT). The success of IoT depends on the standardization of security at various levels, which provides secured inter-operability, compatibility, reliability, and effectiveness of the operations on a global scale (Bi et al. 2014; Li & Lou 2010).

Today, data security and privacy become more critical and important than ever and organizations become vulnerable to various types of threats. As a result, institutions and people are heavily investing in IT cyber defense capabilities to protect their critical assets. To protect any asset from illegal access or providing controls for critical infrastructure, people and technology are the crucial elements for incident detection and to protect private information.

Data security and privacy refer to protective digital measures oriented from unauthorized access and modification, destruction and disclosure. While data security provides protection for information and its confidentiality, integrity, and also availability, in the meantime, data privacy assures that institutional and personal data are collected, processed, protected and destructed legally. Consequently, data security focuses on the ensuring privacy while protecting personal or institutional data.

Security requirements in IoT architecture

As the health-care industry is growing, the amount of data gathered from patients is rapidly increasing and become more diverse. The health-care industry devices collect medical records and images, which is used for both health monitoring and epidemiological research programs. Data security is also very important for health-care records, so health advocates and medical practitioners are working toward implementing electronic medical record (EMR) privacy by creating awareness about patient rights related to the release of data to laboratories, physicians, hospitals and other medical facilities. Collected and stored data through all these methods needs to be accessed legally also be secured in privacy concepts. With the recent advances in wireless sensor health-care networks that are enabling remote medical services, IoT can also help people to collect health data through connected wearable devices. The collected data from wearable devices helps to provide personalized analysis of a person's health and appropriate actions can be taken (Das et al. 2018).

The service-oriented architecture is successfully applied to IoT design, where the applications are moving towards service-oriented (SOA) integration technologies. Services reside in different layers of the IoT such as: sensing layer, network layer, services layer, and application-interface layer. The services-based application will heavily depend on the architecture of IoT. Fig. 1 (Li & Lou 2010) depicts a generic SOA for IoT, which consists of four layers: a) sensing layer is integrated with end components of IoT to sense and acquire the information of devices; b) network layer is the infrastructure to support wireless or wired connections among things; c) service layer is to provide and manage services required by users or applications; d) application interfaces layer consists of interaction methods with users or applications (Bi et al. 2014).

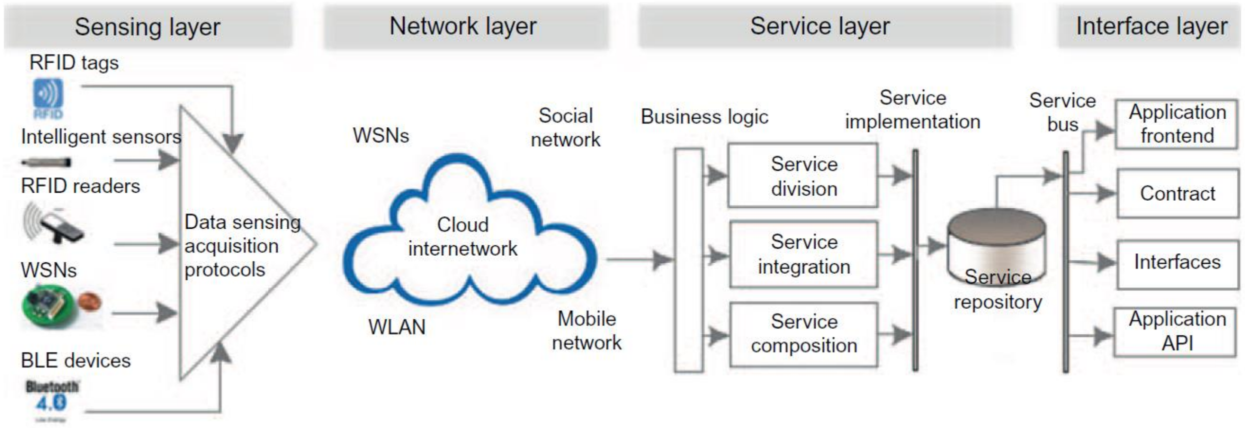

Figure 1. Service-oriented architecture for IoT

The following requirements are essential components to establish a secure IoT network (Das et al. 2018; Techopedia 2018; Li & Xu 2014):

- **Authentication:** One of the most commonly encountered methods of practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data is granted.
- **Confidentiality and Integrity:** Concerns about to privacy of the data from unauthorized access and disclosure of information and protect data from accidental or intentional modification, destruction or disclosure through using of physical security, administrative and logical controls and other safeguards to limit accessibility.
- **Availability:** Process of ensuring that data is available to authorized users and applications, when and where they need it. Typically, data availability calls for implementing products,

services, policies, and procedures that ensure that data is available in normal and even in disaster recovery operations.

- **Non-repudiation:** To prevent a mischievous entity from action logs and maintain an audit trail of changes made by each user and device so that it is impossible to refute actions taken in the system.
- **Authorization and Freshness:** Authorization confirms that only the legitimate IoT sensing (smart) devices supplying information to network services. Also, freshness confirms this information is fresh and the old messages cannot be replaced by any adversary.

Security Concerns in the IoT Ecosystem

Many security and privacy issues in IoT (especially for health-care which is focused in this proceeding) that are not likely to be solved by conventional security mechanisms the currently used such as expensive firewall software and anti-malware solutions. Hence, this article is aimed to present an overall perspective for security and privacy issues of implantable medical devices.

In IoT, each connected device could be a potential doorway into the IoT infrastructure or personal data (Roe 2014). Privacy risks will arise in the IoT since the complexity may create more vulnerability that is related to the service. In IoT, much information is related to our personal information, such as date of birth, location, budgets, etc. This is one aspect of the big data challenging, and security professions will need to ensure that they think through the potential privacy risks associated with the entire data set. The IoT should be implemented in a lawful, ethical, socially, and politically acceptable way, where legal challenges, systematic approaches, technical challenges, and business challenges should be considered (Li & Xu 2017). Security must be addressed throughout the IoT life-cycle from the initial design to the services running. To illustrate the security requirements in IoT, Li and Xu (Li & Xu 2017) modeled the IoT as four-layer architecture: sensing layer, network layer, service layer, and application interface layer and each layer is able to provide corresponding security controls, authentication, data integrity and confidentiality in transmission, availability, and the ability of antivirus or attacks. The most important security issues in IoT are summarized in Table 1.

Table 1. The most important security concerns in IoT

Security concerns	Interface layer	Service layer	Network layer	Sensing layer
Insecure web interface	+	+	+	
Insufficient authorization	+	+	+	+
Insecure network services		+	+	
Lack of transport encryption		+	+	
Privacy concerns		+	+	+
Insecure cloud interface	+			
Insecure mobile interface	+		+	+
Insecure security configuration	+	+	+	
Insecure software / firmware	+		+	
Poor physical security			+	+

Security Challenges in IoT Systems

Cryptography is one of the techniques used to communicate and store information securely without being intercepted or accessible by third parties and is a broad field with applications in many critical areas of our lives (Learn Cryptography 2018). It is widely used in networks to protect private communications and a number of ciphers have been developed, such as Data Encryption Standard (DES) but DES is an outdated symmetric-key method of data encryption (Rouse 2014). DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. To encrypt electronic data, DES has been superseded by the more secure Advanced Encryption Standard (AES) algorithm by Ron Rivest, Adi Shamir and Leonard Adleman (RSA) which is the first practical public-key cryptosystem (Li & Xu 2017). The RSA cryptosystem is the most widely used public key cryptography algorithm in the world (Ireland 2018).

In IoT systems, most of the smart things are typically small, inexpensive, with limited security capabilities and the existing advanced cryptographic algorithms are unable to process since the low CPU cycles and low effective encryption and traditional cryptography is not designed for these environments and is mathematically intensive, which requires CPU power. Because producing complex keys is not easy, and making them in high volumes can quickly become a bottleneck (Li & Xu 2017).

Security Issues for Implantable Medical Devices (IMDs)

There are enormous works in the literature for IMDs. Most of them are related to their design and the effectiveness on the human health. In this work, we will review the literature related to the data security of these devices.

The data security of IMDs is not adequately addressed yet. There is a lack of works in the literature related to their data security. Data security is one of the most vital parts of any design of such devices. Since technology is now mobile almost every side of our life, data security of such devices has become very important.

The data security design of any IMD consists of data integrity, robustness and capability run on devices with lower computing power. For that reason, lightweight cryptosystems are the best solutions for IMDs. Simply, any lightweight cryptosystem ensures the high level of security using low computer energy.

In this work, we will summarize the data security of IMDs from the literature with respect to the design pattern of security conditions and the usage in the IMDs. Moreover, we will compare the designs which give the roadmap to future works such as the data security on an electronic prosthesis.

The most important publication is *Security and Privacy for Implantable Medical Devices* (Halperin et al. 2008). The article is given a general framework for evaluating the security and privacy of next-generation wireless IMDs.

The next work in this area is *Design Challenges for Secure Implantable Medical Devices* (Ransford et al. 2014). The article discusses sound security principles to follow and common security pitfalls to avoid.

The other publication is *Security of Implantable Medical Devices: Limits, Requirements, and Proposals* (Ellouze et al. 2014). They state the main vulnerabilities of IMDs. Eavesdropping attacks, unauthorized accesses to IMDs, attacking the IMD availability, deceiving forensic examiners.

The last publication is about the state-of-art security solutions for IMDs: *A Lightweight Cryptographic System for Implantable Biosensors* (Ghoreishizadeh et al. 2014).

Security and privacy for implantable medical devices

Design criteria for any device should be determined well in order to produce an integrated structure. Over the last decade, with technological improvement, IMDs have also the improvement in the same way. There are a lot of works in the literature about the design of IMDs but lack of them are about the security concern. Here we will start with the first definitions of IMDs and their security concern.

In this paper, they present a general framework of next-generation wireless IMDs' security and privacy evaluation. Since they also pointed that others have considered the security and privacy of the device as a priority, they are looking for the answer of the question: What should be the security and privacy design goals for IMDs?

To answer those questions they suggest some criteria for IMDs. These criteria separated into Safety and Utility Goals and Security and Privacy Goals (Table 2).

Table 2. The security goals of both safety & utility and security & privacy for IMDs

Safety and Utility Goals	Security and Privacy Goals
Data access,	Authorization,
Data accuracy,	Availability,
Device identification,	Device software and settings,
Configurability,	Device-existence privacy,
Updatable software,	Specific-device ID privacy,
Multi-device coordination,	Measurement and log privacy,
Auditable, and	Bearer privacy, and
Resource efficient.	Data integrity.

After those definitions, they classify the adversaries with respect to passive, active, coordinated and insiders. The tensions are given by security versus accessibility, security versus device resources and security versus usability. They also state that the elimination of those tensions might be possible but they emphasize security and privacy-related research and other technological improvements might also lower some tensions. These are categorized by Fine-grained access control, open access with revocation and second-factor authentication, accountability, patient awareness via secondary channels and shift computation to external devices.

Finally, they emphasize the security standards and solutions can be done by the collaboration of the experts from different fields like the medical and security communities, industry, regulatory bodies, patient advocacy groups, and all other relevant communities.

Design challenges for secure implantable medical devices

The above work is about the basic definition of IMDs and their basic security concerns. With the recent developments in wireless technology, IMDs started to use this technology, as well.

This paper firstly gives some definitions about the security to achieve IMD security design principle. Next, they emphasize security challenges in the design of IMD and finally, they sketch the solutions for the security threads.

They state the security goal for designers as follows:

- Security design in early phases,
- Sensitive traffic encryption,
- Third-party device authentication,
- State-of-art cryptographic building blocks,
- Code analysis, and
- Security analysis.

After that design patterns, they have given the Threat Modeling. In this part, they state the severity of vulnerabilities in IMDS differs from other devices because of the sensitivity of the data or the consequences of actuation of IMDs. For instance, an attacked glucose sensor exposes more risk than defibrillator that can deliver disruptive electrical shocks to a heart.

The threats are divided into a passive adversary and active adversary. They described any passive adversary as an eavesdropper who has access to an oscilloscope, software radio, directional antennas, and other listening equipment. This kind of attacks could compromise the patients' data privacy by eavesdropping on unencrypted communication. Unlike the passive adversary, an active adversary has an improved role since they have the ability to generate radio transmissions which addressed to the IMD, or re-command the control with replication. They have described another adversarial capability as binary analysis which inspects the system and related operations with the analysis of the software.

Next, they offer examples of IMD systems posing different security challenges since the design and usage difference. The common thread among all three devices insulin pump systems, implantable cardioverter defibrillators, and subcutaneous biosensors is that security is a crucial design concern. After that illustrations, the next section describes the common threads and cryptographic solutions to those threads. The first example is insulin pump systems. Simply, insulin pump system is an open-loop IMDs: pump settings can be changed by the interaction of patient. This interaction is done with the remote control. Lots of crucial information like control signal carried out with remote-control. They focused on finding vulnerabilities at this part. Li et al. (2011) showed that communication is encrypted which can lead to a leakage in a patient's private data. The next example is defibrillators. Defibrillators (implantable cardiac defibrillators ICDs) are devices implanted under the skin which pulses small electricity to the heart muscle in order to maintain a healthy heart rate. Security analysis of defibrillators has done (Halperin et al. 2008). The analysis was done by the use of software radio tools to get the transmissions of records between the ICD and clinical programming console. The analysis showed that patient information is stored in the unencrypted form which can result to control of ICD with radio tools. The last example is implantable biosensors. Implantable biosensors are devices that send data to another device which more powerful than them and measures biological phenomena for storage or analysis. Since they use a wide range of signal and processing techniques they are broader devices than insulin pumps and defibrillators. Any biosensor can be used as a high data-rate imaging device for brain or eye to low-data-rate sensors for glucose or other metabolites in the blood. Therefore, biosensor data is confidential and kept in encrypted form in order not to be used in illegal or unethical ways.

The common thread in IMDs is the vulnerability of data migration on radio links. This vulnerability can be achieved with the encryption but it is not enough for the full secure IMD. According to the authentication, the secret key transfer is still an open problem.

Finally, they emphasize recent analyses of implantable medical devices with security and privacy failings. These failings give opportunities to researchers to develop novel solutions in the design of IMDs.

Security of implantable medical devices: limits, requirements, and proposals

The previous work implies the security concern of IMDs and gives the solution to secure design. For a determined secure IMD design, some of the limitations should be described. In this paper, firstly, the main vulnerabilities of IMDs are given. Then they describe security performance and drawbacks. Finally, security requirements in the design of IMD are given.

Any IMD is a device which is surgically implanted into the patient's body in order to perform some medical treatments. They give an architecture of an IMD as the following parts: Sensor devices, battery, memory, processing unit, stimulator, MICS (medical implant communication system) transceiver, Wireless identification and sensing platform (WISP), Implantable medical device programmer.

The vulnerability of IMDs is exposing of the use of wireless interfaces for communication. They categorize the security threats into four parts:

- ***Eavesdropping attacks:*** This attack is mainly eavesdropping the messages between IMDs and programmers. It can also be applied to the components of IMDs. Lots of IMDs messages are not encrypted so that an adversary can easily analyze the message and apply his attack.
- ***Unauthorized access to the IMD:*** A PIN is used in IMDs. Any adversary capturing the PIN can fully access the IMDs and perform modifications in the configuration that harmful to patient's health.
- ***Attacking the IMD availability:*** It is possible to send repetitive messages to IMDs which causes denial-of-service attacks. This kind of attacks can drain the battery of IMDs and shorten the life of a device.
- ***Deceiving forensic examiners:*** In this attack, the attackers make it impossible to investigate and detect the forms of attack. Mainly, the aim of this kind of attack is the access of the log of the IMDs, the historical data, and the timestamps.

To make secure IMDs the state-of-art technology is proposed. In order to make a secure IMD lightweight cryptosystems can be used. The energy of any IMD is the most valuable part of the system since it directly affects the life of the device. So that, they have given the techniques preserving energy for IMD security with the use of lightweight cryptosystems which needs a low level of energy. The authentication is the next important part of the security design of any IMD. Techniques for access control in emergency situations is given in order to accomplish the authentication. The next technique is controlled access to IMD. Here they have given the instance of the proximity-based access control scheme and rolling code technique. Finally, a biometric-based technique is given. Biometric techniques are used to access IMD in a secure way. Several ways of biometric authentication can be used in order to access: lightweight biometric technique and physiological signal.

After those security design techniques, limitations are given in order to efficiency. With these definitions, they conclude that the challenges need to be addressed when designing a secure IMD.

Design A lightweight cryptographic system for implantable biosensors

With the description of secure design criteria, any IMD can be securely produced. This paper is one of the best instances of a securely designed IMD. It differs from the other papers with respect to a specified solution on security. They present a lightweight cryptographic system integrated onto a multi-function implantable biosensor prototype.

First, the conceptual view of the subcutaneous IMD is given. Simply the design of IMD starts with the receiving power via an inductive link. Then it consists of a sensor array for calibration and metabolite detection. The front-end IC controls and reads out the sensor array and transmits the measured data back to the patch. The front-end IC is where the encryption system is implemented.

Two threat scenarios are considered: (1) trusted patch is removed and placed on a rogue implant (2) rogue patch is used to extract data from a trusted implant. Their scheme also prevents other weakness in the patch or higher levels and Bluetooth link.

For a security module, the lightweight cryptosystem is used. For hash issues, the newest hash algorithm Keccak is used. Also, the most valuable part in IMD is energy so, in order to achieve low power, the opted for a low bandwidth tweak of the Keccak secure hash function used in authenticated encryption mode. They also made aggressive utilization of bit serial architectures in an effort to reduce combinational logic and minimize switching activity.

Finally, to protect the wireless data transmission and to provide security and privacy for the IMD information, they have designed and implemented a lightweight security system using a tweaked version of the Keccak secure hash function implemented in an authenticated encryption mode.

Results and Discussion

In this work, we summarize the works related to the security design of IMDs. The aim of this work is the best and novel security design of any IMD. So that, the first paper gives the security framework of IMD with the usage of wireless technology. The second paper is mainly about the design criteria of secure IMD. They also describe the threats and attack on IMDs. The most effective paper is the third one. They describe the secure design criteria of any IMD and give the solutions to attacks. Also, limitations in the security design are given. The last paper is based on the specific example of secure IMD which is designed by state-of-art technology.

The above works are the milestones of the design of any secure IMDs. Since wireless and mobile technology are improving day by day, the devices in the health systems improving on the same route. Not only IMDs but also electronic prosthesis need security in their design. Our future work will consist of the general and standard security design of IMDs and electronic prosthesis with the low-cost cryptographic techniques.

References

Bi, Z., Xu,L. & Wang, C. (2014). Internet of Things for Enterprise Systems of Modern Manufacturing, *IEEE Transactions on Industrial Informatics*, 10(2), 1537-1546.

Das, A.K., Zeadally, S. & He, D. (2018). Taxonomy and Analysis of Security Protocols for Internet of Things, *Future Generation Computer Systems*, 89, 110-125.

Ellouze, N., Allouche, M., Ahmed, H.B. et al. (2014). Security of Implantable Medical Devices: Limits, Requirements, and Proposals, *Security and Communication Networks*, 7(12), 2475-2491.

Ghoreishizadeh, S.S., Yalcin, T., Pullini, A. et al. (2014). A Lightweight Cryptographic System for Implantable Biosensors, In: *Biomedical Circuits and Systems Conference (BioCAS)*, 472-475.

Gubbi, J., Buyya, R., Marusic, S. et al. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, *Future Generation Computer Systems*, 29(7), 1645-1660.

Halperin, D., Heydt-Benjamin, T.S., Ransford, B. et al. (2008). Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, In: *2008 IEEE Symposium on Security and Privacy (SP'2008)*, Oakland, CA, 129-142.

Halperin, D., Heydt, B., Thomas, S. et al. (2008). Security and Privacy for Implantable Medical Devices, *IEEE Pervasive Computing*, 7(1), 30-39.

Information Matters (2018). The Business of Data and the Internet of Things (IoT), http://informationmatters.net/internet-of-things-statistics/. (Accessed on August 2018).

Ireland, D. (2018). RSA Algorithm. https://www.di-mgt.com.au/rsa_alg.html. (Accessed on August 2018)

Learn Crytoraphy. (2018). What is Cryptography? https://learncryptography.com/. (Accessed on August 2018)

Li, C., Raghunathan, A., Jha, N.K. (2011). Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System, In: *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services (HEALTHCOM'2011)*.

Li, M. & Lou, W. (2010). Data Security and Privacy in Wireless Body Area Networks, *IEEE Wireless Communications*, 17(1), 51-58.

Li, S. & Xu, L.D. (2017). *Securing the Internet of Things*. Cambridge, United States: Syngress Publications.

Ransford, B., Clark, S.S., Kune, D.F. et al. (2014). Design Challenges for Secure Implantable Medical Devices. In: *Security and Privacy for Implantable Medical Devices*, 157-173, Springer, New York, NY.

Roe, D. (2014). Top 5 Internet of Things Security Concerns, https://www.cmswire.com/cms/internet-of-things/top-5-internet-of-things-security-concerns-026043.php. (Accessed on August 2018)

Rouse, M. (2014). Data Encryption Standard. https://searchsecurity.techtarget.com/definition/Data-Encryption-Standard. (Accessed on August 2018)

Techopedia (2018). Data Availability, https://www.techopedia.com/definition/14678/data-availability. (Accessed on August 2018).

Zanella, A., Bui, N., Castellani, A. et al. (2014). Internet of Things for Smart Cities, *IEEE Internet of Things Journal*, 1(1), 22-32.