Securing Implantable Cardioverter Defibrillators Using Smartphones

Jiwan Ninglekhu[1]*, Ram Krishnan[1], Eugene John[1], and Manoj Panday[2]
[1]The University of Texas at San Antonio, One UTSA Circle, San Antonio, TX 78256, USA
iiw057@my.utsa.edu, ram.krishnan@utsa.edu, eugene.john@utsa.edu
[2]University of Texas Health Science Center, San Antonio, TX, USA
manojpanday@hotmail.com

Abstract

In this paper, we propose a novel security framework to protect Implantable Cardioverter Defibrillators (ICDs) using Smartphones. ICDs are small battery powered Implantable Medical Devices (IMDs) that are introduced in the patient's body to treat irregular heartbeats known as arrhythmias. These devices are programmed and accessed wirelessly for diagnosis and therapy by a programming device known as External Programmer (EP). Previous studies have demonstrated that ICDs are susceptible to attacks via unauthorized EPs. These attacks may not only pose privacy concerns, but can also do serious physical harm to a patient. While it is crucial that these devices need to be secured by all means possible, a medical practitioner should be allowed to access ICDs when needed, especially under emergency situations. In this paper, we investigate techniques for using a patient's smartphone for authenticated and authorized communication between the patient's ICD and the EP operated by a physician treating the patient. An application running in the smartphone serves two major purposes. (1) mediates secure communication, and (2) keeps the patient in-the-loop by providing an audiovisual interface, to be aware of and take control over the communication occurring between the ICD and EP. Due to the fact that smartphones are becoming more cheaper and their versatility becoming greater, using smartphones as a security device is a feasible option. As a proof-of-concept, the proposed Kerberos based security scheme is implemented using simulated EP, ICD, and an Android-based smartphone.

Keywords: Implantable Cardioverter Defibrillator (ICD), Implantable Medical devices (IMD), security, safety, Smartphones

1 Introduction

A medical device is defined as *implantable* if it is either partly or totally introduced surgically into the human body and is expected to remain in the body after the procedure [19]. Millions of people around the world live with Implantable Medical Devices (IMDs) [16]. A recent study has shown a lot of improvement in quality of life and increase in length of life among people who used IMDs. IMDs come in a range of devices and perform a variety of functions, such as deep brain implants for the treatment of Parkinson's disease, insulin pumps for diabetes treatment, drug infusion, and cardiac pacemakers for patients with heart-rhythm disorders. Many of these IMDs are electronic, and are generally capable of sensing, computing, transmitting and receiving data over wired and wireless network. They can be programmed to implement and adjust prescribed therapy. Typically, IMDs use short-range telemetry to communicate wirelessly from inside the human body to an external equipment, as it is impractical to perform frequent surgery for data retrieval or therapy modifications [19].

Journal of Internet Services and Information Security (JISIS), volume: 5, number: 2 (May 2015), pp. 47-64
*Corresponding author: Department of Electrical and Computer Engineering, The University of Texas at San Antonio (UTSA), One UTSA Circle, San Antonio, TX 78256, USA, Tel: +1 210 458 7753

The Implantable Cardioverter Defibrillator (ICD) is just one among many different types of IMDs. ICDs are electronic devices engineered to help treat irregular heartbeats called arrhythmias [10, 21]. They can sense a rapid heartbeat and can administer electric shocks or pulses to help control arrhythmias that could result in sudden cardiac arrest. It can also log information that can be viewed by a health professional with access via an EP. Once implanted, ICDs are expected to remain inside the body for several years. Modern ICDs are equipped with pacemaker technology that are designed to be programmed by EPs and monitored by external monitoring devices, wirelessly, and without surgery [6, 10].

To enable wireless communication between the ICD and the EP, an extended device from the EP, known as a magnetic wand, is placed over the skin where the ICD is implanted. The wand magnetically opens a switch in the ICD for wireless communication. Recent advancements in technology has made EP to contact the ICD, using radio frequency without the need for a wand [2, 7, 5, 10, 22]. Patients can also be monitored by a wireless transreceiver called cardiac event monitors, placed usually by the side of the patient's bed, which receives wireless data from the ICD and sends it to the doctor or hospital via the Internet. Recently, researchers have found that communication-messages between these devices (ICD and EP/Transreceiver) were in plain text or unencrypted, and unauthorized access to the ICD was possible. Researchers were able to establish communication with an ICD using a simulated EP. One big issue with this is the risk of patient's privacy, wherein the unauthorized party could collect and read private data from the ICD. Moreover, unauthorized access could render control over the ICD's operation and disable therapeutic services or deliver malicious shocks to the patient's heart [10, 12, 13]. The transmitted messages could be altered and modified, or the ICD could just be engaged in constant communication that would drain the battery power. The fact that some ICDs are capable of sending information across the Internet opens doors for numerous other threats.

While security is a critical aspect in medical devices, a bigger challenge is to ensure that security measures do not disable one's accessibility for ICD. A trained medicine practitioner should be able to access the system with ease, especially in an emergency situation. Any security feature must not be a hindrance. Therefore, a system that demonstrates secure communications for possible threats, consumes little power, and that can open-up during emergency situations must be designed [3, 10].

Researches in the past have shown that the use of an external device can help secure the ICD [1, 22]. Implementing security systems requires energy, therefore using the battery power optimally is critical in designing a computing system. We propose the use of smartphone as a security proxy to mitigate the problems discussed. Among many benefits of using smartphones for information exchange, they are getting more readily available and becoming cheaper, while their functionality and computation power have attained a whole new level. They are suitable for a portable security proxy for the ICD. They are programmable devices carried almost all the time where security can be implemented easily [14]. In this article, smartphone's computing capability and audio-visual system for security and real-time monitoring functions are utilized. The aforementioned problems are addressed by portraying realistic scenarios, and their corresponding solutions. The smartphone based security scheme proposed in this paper contributes the following:

i Implements a technique based on Kerberos security protocol [20] in the system where smartphone acts as an authentication and authorization proxy that protects ICDs against intrusions and attacks.

ii Presents scenarios where any EP can be used to program patient's ICD.

iii Utilizes efficient symmetric key cryptosystem to protect ICD from adversaries.

iv Authorizes patient as the chief communication process authenticator. An approach that keeps the patient aware of what is happening and lets the patient to allow or deny an EP device from communicating.

v Presents smartphone as a real time monitoring device that keeps the patient aware of irregular heart activities and displays a secret code in emergency cases, that could be used by field medical practitioner to access the ICD.

vi Presents scenarios where ICD's security can be maintained in the absence of smartphone.

vii Addresses secure access during emergency conditions.

viii Implements a proof-of-concept design and analyzes the proposed security approach in detail.

In this paper, a *smartphone* refers to a patient's smartphone and the *ICD* represents that patient's ICD. In both the cases the terms are used interchangeably. The rest of the paper is organized as follows. Section 2 presents the overview of the proposed scheme and defines components and scenarios in general. System design of the proposed technique is decribed in Section 3. Section 4 explains implementation details and evaluation of results. Related work is presented in Section 5 and Section 6 concludes the paper with future research direction.

2 System Configuration

2.1 Overview

The proposed security scheme in general consists of four main entities: a patient's ICD, EP, the Patient, and the Smartphone. Each component is explained briefly.

- **The ICD:** The ICD system is comprised of a pulse generator and one or more leads for pacing and defibrillation electrodes. Other components include batteries, DC converters, resistors, capacitors to store charges, microprocessors, and integrated circuits to control the analysis of rhythm and the delivery of therapy. It also has memory chip to store electrographic and other data. Once installed, usually remains inside the body for prolonged length of time, sometimes up to ten years [8]. It can communicate with external programmer via wireless radio up to several meters away [1].

- **External Programmer:** EP is the device that provides a console for medical practitioner to send data, retrieve data, and change therapy via wireless radio frequency.

- **The Smartphone:** Smartphones are wireless telephones that have high computation and interactive properties than a regular phone. In this research, smartphones are implemented under the assumption that a patient possesses one. In our design, it acts as a proxy for security and as a monitoring module.

- **The Patient:** A patient is an individual with the ICD implanted in her body. Our proposed security model designates a patient as an authentication stage, i.e., the patient possesses an authority to allow or deny external device.

A top-level overview of the general message exchange scenario where smartphone sits between ICD and EP and behaves as proxy between is shown in Figure 1. It depicts the most common scenario. Communication steps are marked with numbers and summerized as follows. (1) An EP requests the patient's smartphone to get access to the patient's ICD. (2) Patient is notified. (3) Patient authenticates the EP and enters an authorization command in the smartphone. (4) Smartphone sends authorization token to the EP. (5) EP requests ICD for required information. (6) ICD replies with the requested information.

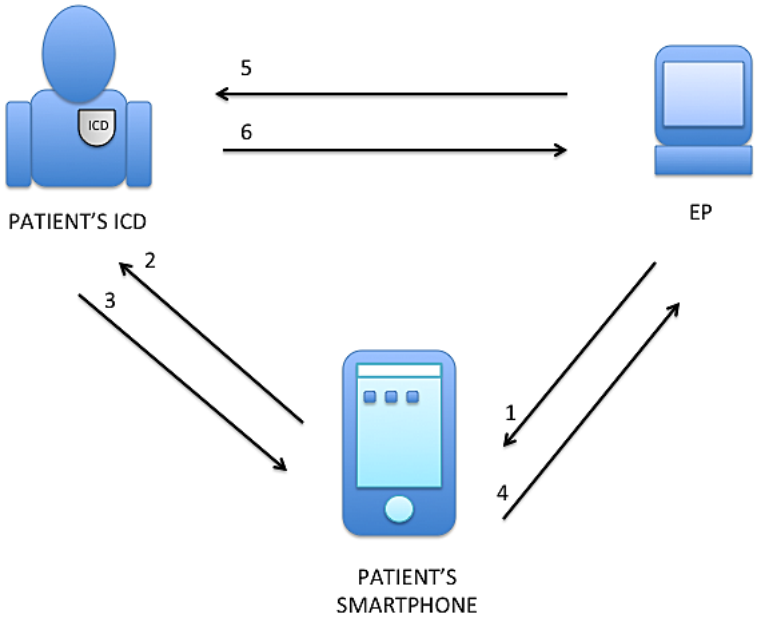

Figure 1: General security configurations of ICD and an EP with smartphone. Steps: (1) EP requests access to the ICD. (2) Smartphone notifies the patient. (3) Patient authorizes the EP by entering a code. (4) Smartphone sends a reply to EP. (5) EP requests ICD for information. (6) ICD replies to EP.

2.2 Adversary Models

To generalize adversaries, they can be classified under two different types: passive adversary and active adversary. Passive adversaries eavesdrop or retrieve information by listening to the message exchanged without patient's knowledge. Active adversaries are classified as more dangerous for they can penetrate into the patient's ICD and disrupt or modify information on therapy settings to physically harm the patient that can be deadly. Active adversaries also include attackers that try to maintain unnecessary communication with the ICD or smartphone that can drain out power. An adversary is assumed to be located nearby the patient and attacks are carried out wirelessly. The attack is assumed to be possible at any time and place.

2.3 Scenarios

We have divided the problem into four major real life scenarios. Each of them is explained below:

2.3.1 Scenario 1: Clinical Consultation, Smartphone Present

A patient is required to visit hospital during implantation and for regular consultation after the ICD has been implanted. It is proposed that the patient's smartphone be registered to the patient's ICD during implantation. There can be two cases within this scenario. As the patient comes back to hospital for regular clinical consultation, the patient may encounter either a new EP that is unknown to her ICD or the one that has been registered with ICD.

An unknown EP has to register itself with the Smartphone to communicate with the ICD. This paper proposes two options for registration. It could either be registered temporarily or permanently. A registration in which the registry lasts only for current programing process and the EP is forgotten after programing process ends, is referred to as temporary registration. In permanent registration, the registry

of an EP is saved into the smartphone's database. This EP information can be used without re-registration in the future.

In a clinical scenario, when an unknown EP requests the patient's smartphone access to the patient's ICD, their registered smartphone (registered with the ICD) will alert the patient about this new unknown device and will ask for a permission to continue the process by prompting a message. The proposed approach provides a unique way to register an unknown EP by giving the user (patient) an authority to provide a secret code in the smartphone and the new EP, simultaneously. Once the user enters the session secret code on both the devices, the two devices can recognize each other on the basis of the key derived from the secret code and can communicate with each other. At this point the unknown EP becomes a registered EP. The patient can choose to use temporary registration by using a secret code each time a new EP is used for programming. This scenario is depicted in Figure 2 and is explained in more detail in Section 3, where we explore detailed design process.

2.3.2 Scenario 2: Clinical Consultation, Smartphone Absent

Although it is recommended that smartphone should be carried by the patient at all times, there might be a situation where the patient's smartphone may be absent. Patient's ICD must still be protected in such a scenario. More importantly, at any given situation, an authorized EP must be able to access patient's ICD. This paper proposes an approach that will maintain the security of patient's ICD even if her smartphone is not present.

To address this situation and still maintain security, a key must be pre-shared between patient's ICD and the patient. A secret code, called the Master Secret code, is given to the patient. The master secret code can be printed into a piece of jewelry worn by the patient or the patient can choose to memorize the code. A key derived from the master secret is kept in the ICD's database. In occasions where the patient's smartphone is not present, this key will facilitate EP's communication with the ICD. This master secret should be a one-time secret and for security reasons, should be required to change every time after its usage. Figure 4 presents a block diagram, and Section 3 explains the scenario in detail.

2.3.3 Scenario 3: Patient Incapacitated, Smartphone Present

A heart patient can fall incapacitated or near to incapacitated because of heart irregularities. An approach proposed by this paper assumes a patient's ICD to be continuously monitoring their heart's health and periodically sending updates toward the smartphone while the patient's smartphone is continuously listening to the patient's ICD. A patient's ICD is configured to react to a specified threshold before it sends an emergency alert message to the smartphone. If any unusual (emergency) signal is encountered, then it sends out an emergency alert message with a temporary access code to the smartphone. This situation can occur anywhere and can be considered as an emergency.

Provided that the emergency medical help arrives at the scene on time, this paper proposes a solution should the patient be in need of medical assistance and her smartphone available. With a temporary access code, a medical practitioner can access the patient's ICD to get important patient's information to treat the patient. This scenario is further explained in later section with block diagram in Figure 5.

2.3.4 Scenario 4: Patient Incapacitated, Smartphone Absent

This scenario is similar to scenario 2, except that the patient is incapacitated. We provide a method by which a secure communication can be established between the EP and patient's ICD in a case where patient's smartphone is inactive and the patient is incapacitated. We assume a scenario in which if an emergency medical personnel arrives at the scene and on time, they should be able to access the patient's

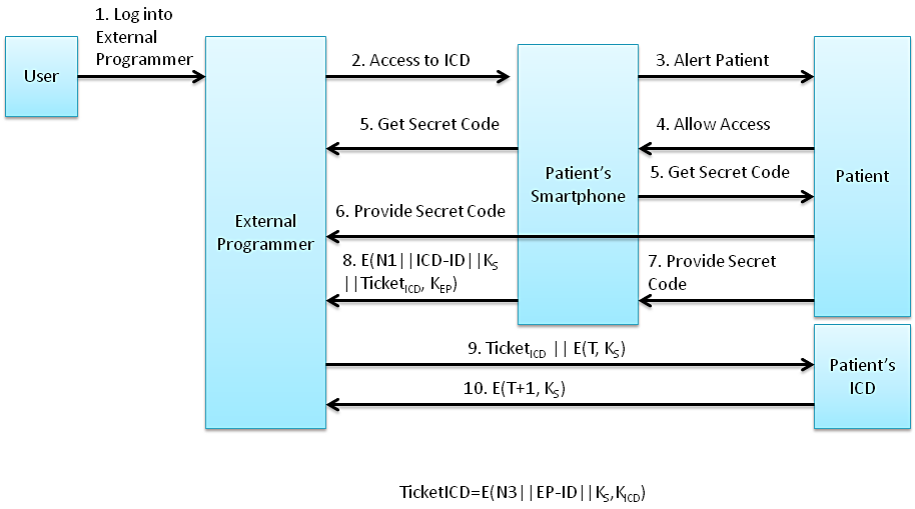

Figure 2: Registration and message exchange between new EP and the patient's smartphone

ICD via EP securely without problem. There can also be a situation where the ICD may need to be examined even after the patient is incapacitated. We recommend that patient's biometric information, such as fingerprints, be used as a source of the secret key. Biometrics is unique for each person and therefore extremely difficult to be forged directly by adversaries. Since the biometric information is kept inside the smartphone only, it can be considered relatively secure. Key derived using biometric information of the patient is stored in patient's ICD. This paper also assumes that an EP is equipped with biometric scanner with a capability to convert biometrics into a standard digital key.

3 System Design of The Proposed Scheme

In this section, we present concrete protocols to address the four scenarios discussed earlier. The protocols are based on Kerberos. Note that we only provide a hige-level design. In particlular, the presented protocol is not claimed to be formally secure.

3.1 Device Registration

The key exchange between the devices is known as registration. A smartphone is registered to the ICD and EPs are registered to the smartphone. Only one smartphone can be registered to an ICD. There can be two ways in which the symmetric keys can be established between the devices: Before the ICD implantation or after the device has been implanted. A patient is required to visit the hospital for regular consultation after the ICD has been implanted. If the key is exchanged between the smartphone and the EP before the implantation then programming can be carried immediately otherwise the EP has to go through the registration process with the smartphone. There can be two cases when the patient visits a hospital after the implant. Either the patient's smartphone is available, or unavailable. Furthermore, there can be a case where the EP is used for the first time with the smartphone.

For a scenario where the smartphone is present and brought to the consultation for the first time, the EP contacts the smartphone. The smartphone displays a message that asks if the EP should be allowed. If the patient allows it, smartphone displays an input dialog box for secret code and sends a message to the EP. As the EP gets the message, it also generates a display message to input the secret code. A secret code of choice is insert by the patient-user in both the devices. They generate the key from this

secret code to recognize each other. This key can be stored in the smartphone and EP databases for future references. Our scheme also provides an option to select a secret code each time a new EP is brought into the system. The message exchange between the devices in different scenarios is explained in following sub-sections.

3.1.1 Scenario 1: Patient in Clinical Consultation

i. New Programmer, Smartphone Present

A new EP contacts the patient's smartphone with its identity (ID), EP-ID. The patient's smartphone alerts the patient about EP by prompting a message on the smartphone's screen as shown in Figure 6(a), which gives patient an authority to allow or deny the request. If denied, no further communication takes place. If allowed, the patient's smartphone searches for the key in its database to ascertain whether it has information on this EP. Figure 2 depicts the message exchange process. Since it is a new EP, patient's smartphone will provide an option to register this new EP by generating a dialog box to create the secret code (Figure 6(b)). It also sends the same message to the EP about its state. EP also gives an option to enter the secret code, shown in Figure 8 (line 8). The user has to provide same secret code in both the devices. Once the code is entered into the smartphone, it immediately converts the code into its 128-bit key from secret code's hash for communicating with this new EP. Now the EP is temporarily registered with the smartphone. The smartphone, which acts a KDC (Key Distribution Cener), as in Kerberos protocol, generates a random temporary key, K_S, dedicated for communication between the EP and ICDs, and a ticket for the ICD, $Ticket_{ICD}$. It sends the temporary key, K_S concatenated with identity of ICD, ICD-ID, a random nonce, N_1, and $Ticket_{ICD}$, encrypted with key, K_{EP}. K_{EP} was generated from the secret code entered by the patient-user. The ICD-ID is sent to the EP to inform that K_S is only for ICD. The $Ticket_{ICD}$ contains the EP-ID, the temporary key, K_S and a nonce N_2, encrypted with a pre-shared key, K_{ICD}, shared between ICD and the smartphone. The structure of the $Ticket_{ICD}$ is shown in the lower portion of Figure 2. The ICD sends the $Ticket_{ICD}$ concatenated with a timestamp, T. Timestamp T is encrypted with the key, K_S. The ICD then reads $Ticket_{ICD}$, decrypts it with the key, K_{ICD}, gets the temporary key, K_S, and identifies the information that the key, K_S can be used only with the EP. It decrypts the message, gets the timestamp T, and sends back the acknowledgement, T+1, encrypted with the key, K_S. Now the EP can request service from patient's ICD.

ii. Registered External Programmer, Smartphone Present

The proposed protocol also permits the designer with a feature to allow an EP to be registered with the patient's smartphone permanently. The process simply stores the key generated from the secret code into the database. This way, if the same EP accessed the patient's smartphone in the future, it does not need to go through registration process. Figure 3 depicts how a registered EP would request services from patient's ICD with patient's permission.

3.1.2 Scenario 2: Clinical Consultation, Smartphone Absent

Figure 4 depicts the block diagram for a situation when the patient visits her regular hospital for clinical consultation without her smartphone.

In a situation where the patient's smartphone is not present, the EP has to contact the patient's ICD directly. The doctor enters the master secret code previously exchanged between the ICD and the patient into the external programmer (EP). The EP generates a key based on the hash of the master secret. Then the EP encrypts the message-request with the key generated from the master-secret and sends it to the ICD. The ICD is able to recognize the request as it already has the key derived from the pre-shared master secret. The ICD decrypts the message, identifies the request, generates a random session-secret key, and

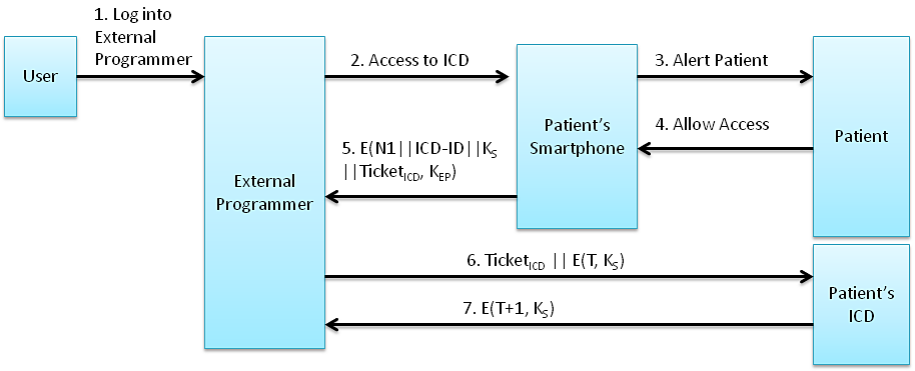

Figure 3: Message exchange in a preregistered EP

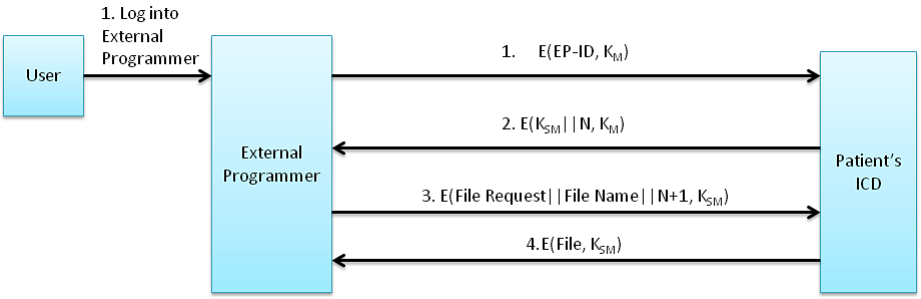

Figure 4: Message exchange between EP and ICD in absence of smartphone

sends back this session-secret key concatenated with a nonce, N, encrypted with the master-secret key, K_M, to the EP. The EP is able to extract the session secret key and use it to request further service or file from the patient's ICD. In Figure 4 the EP makes a request of a file by sending a file-request command concatenated with filename and nonce, N+1, encrypted with session key, K_{SM}. The patient's ICD delivers the file to the EP encrypted with session key, K_{SM}.

3.1.3 Scenario 3: Patient Incapacitated, Smartphone Present

The ICD sends an encrypted alert message and a secret code to the continuously listening smartphone, if an extremely irregular activity is encountered, as shown in Figure 5. The alert message is prompted on the smartphone with a sound and vibration. If the patient feels nothing threatening, the patient can discard the message. Provided that the patient is incapacitated and the rescue team arrived on time, the emergency medics can still get the information from the ICD using that key derived from the temporary access code sent to the patient's smartphone.

As shown in Figure 5, the emergency medical practitioner on site obtains one-time temporary secret from the patient's smartphone and uses it in the EP to request file directly from the patient's ICD. A one-time temporary secret is a code that can be used only once. Request contains request command and required file name encrypted with the temporary key derived from the temporary access code. A temporary one-time secret must be updated after its usage. Since, the code is provided automatically by the ICD and is used by the field medics and not by patient's doctor, it is recommended to have limited access with respect to access-level and time.

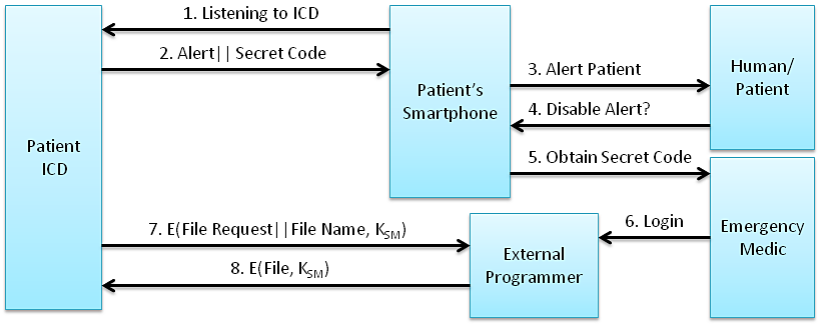

Figure 5: Temporary secret code sent for emergency medical practitioner

3.1.4 Scenario 4: Patient Incapacitated, Smartphone Absent

The solution to this scenario is similar to the Scenario 2, as shown in Figure 4, except that the master secret key K_{MS} is replaced by digital key generated from the patient's biometrics, such as her fingerprint.

4 Design Implementation and Evaluation

In this section, we present and discuss in detail, the results as a proof-of-concept implementation of the scheme proposed and evaluation of the simulation results.

4.1 Design Implementation

The implementation consists of three programs that simulate the patient's ICD, EP, and the patient's smartphone. The ICD and EP are two Java programs that run in two different computers that simulate the ICD and EP, respectively. All the messages are encrypted with symmetric key crypto. We utilize 128-bit Advanced Encryption Standard (AES) algorithm. AES also offers option of 192 bits or 256 bit encryption/decryption. For simplicity, we use TCP/IP over a wireless local areas network among ICD, Smartphone and EP. The simulated programs for each system are described briefly as follows:

- ICD: Six different classes represented the functionality of an ICD. These classes control the logic of messages, file transmission and reception, and key generation. A separate class is run as monitoring module to simulate ICD-monitoring and delivery of alert messages.

- Smartphone: Smartphone's functionality is simulated in seven different classes in Android SDK. It has main activity and service activity. Main activity runs and faces the interactive system and display system. Service activity runs in the background that does background functions such as the background processing, listening to the ports, transmitting messages etc. A separate class is created for monitoring the alert message from the patient's ICD.

- External Programmer: The External Programmer program has six different classes that control main communication and interactive functions. The classes control the logic of messages, file transmission and reception, key generation etc. The following sub-sections discuss how the simulation was carried out and the results are explained.

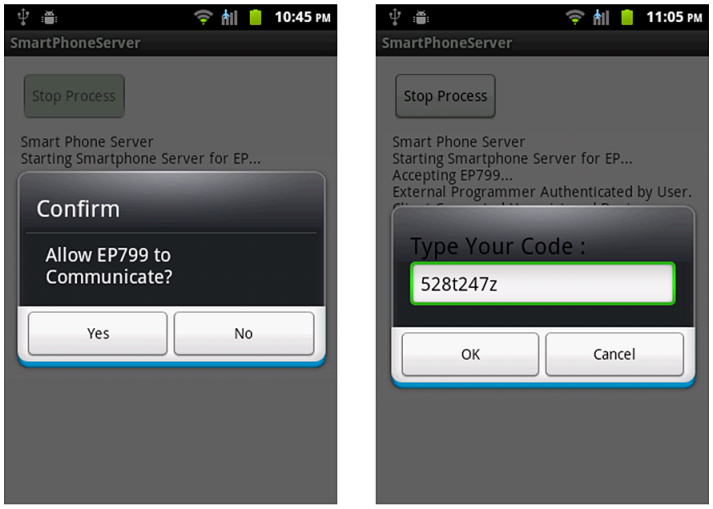

Figure 6: Smartphone screen displays (a) Authorization dialog box (b) Option to enter the secret code in smartphone

4.1.1 Scenario 1: Clinical Consultation

i. New Programmer, Smartphone Present

In a clinical scenario, an external EP attempts to contact smartphone that serves as a proxy, to get to the patient's ICD. The smartphone alerts the patient by displaying a dialog indicating whether to allow the external programmer as shown in Figure 6.1(a). Provided that patient authenticates and allows this new EP, a new option to put a session secret code is displayed and same information is sent to the EP. EP simultaneously generates a similar option to enter the same session secret code. The patient user will enter an alphanumeric session secret code such as "528t247z" as shown in Figure 6(b). Figure 6(a) and Figure 6(b) show dialog boxes generated for user consent and the session secret user input dialog box, respectively.

The secret code derived by using MD5 message digest algorithm is converted into a 128-bit hash value. Using the inbuilt KeyGenerator() function in Java, a 128-bit secret key is derived based on AES cryptographic algorithm. The patient's smartphone and EP are registered at this point. Should we choose, we can store the key derived from the secret code permanently and use it later. The in depth procedure was discussed in Section 2. Each time a program is run, a new session key is generated randomly using AES algorithm and a session secret key is valid only for a limited time. The patient is given the authority to stop the file transfer process between EP and patient's ICD by pressing the 'Stop Process' button in the smartphone server application. The 'Stop' button is shown in Figure 7.

Figure 8 shows the process and messages exchanged as seen on the EP. It indicates that the EP first contacted the smartphone. As the EP is unknown, the patient authenticates it by entering a random secret code. For example an alphanumneric code 528t247z is shown in Figure 6(b). The smartphone sends a temporary key that is used to request the file from ICD. It also shows a file request to the ICD and delivery of file **report.txt**. Figure 9 shows the communication activities on the ICD. Among other messages, it shows smartphone **SP1254** being authenticated, temporary key received upon authentication, file (**report.txt**) requested by the EP, delivery of the file and finally end of the delivery process.

In a regular clinical consultation, where a patient is going to regular hospital for clinical consultation, it is most likely that a registered programmer will be used and the patient is equipped with smartphone.

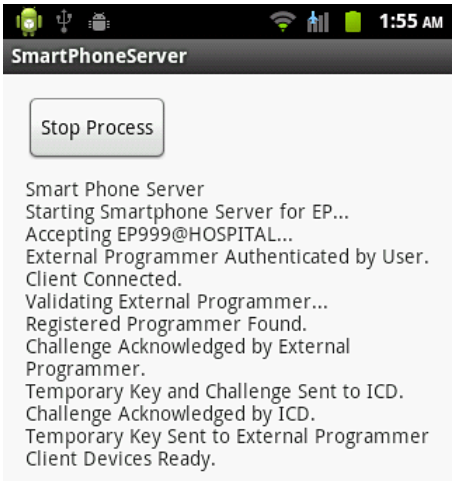

Figure 7: Log messages displayed on the smartphone indicating the exchange of messages

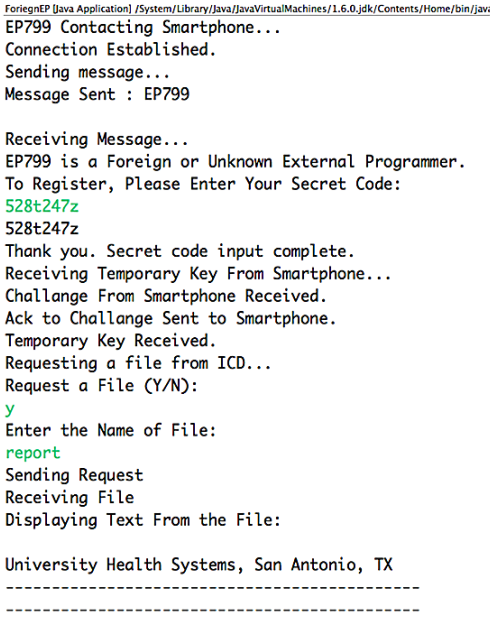

Figure 8: Log messages of exchange activity in EP

Figure 9 shows messages indicating the ICD establishing contact with the smartphone and the EP. One of the simple ways to register an external programmer was described in the previous section.

ii. Registered External Programmer, Smartphone Present

In a clinical setting, the EP at the hospital is assumed to be registered with the smartphone and smartphone is registered with patient's ICD, at least after the first visit. Trusted EP's information is kept permanently in patient's smartphone after authorized registration. Then during following visits, the patient's ICD can be accessed via EP without going through the registration process again. The access process is similar to the new or foreign EP as explained in previous section. As shown in Figure 6(a), the authorization message box pops up as the smartphone is contacted by the registered EP. Since the registration has already been done previously, rest of the authentication process is automatic, once the

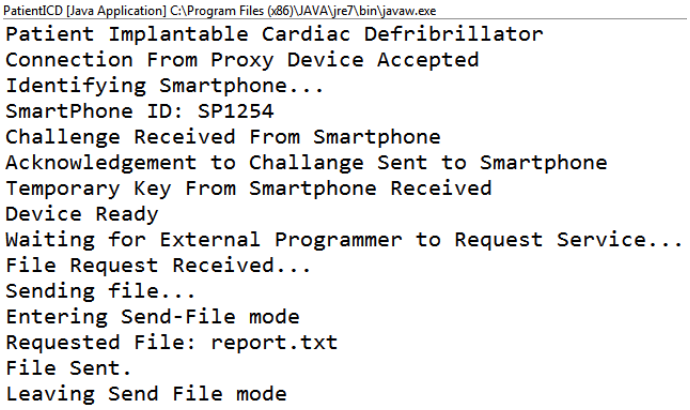

Figure 9: Message exchange activity in ICD

patient authorizes the EP by pressing the 'Yes' button on the screen. The message exchange process between the EP, smartphone and the ICD is similar to the one shown in Figures 7, Figure 8 and Figure 9, except for the secret code input for registration. The registered EP can then request services from ICD when both the devices are ready. The process is shown in Figure 3.

The proposed scheme makes use of session keys intensively. As suggested by the Kerberos, the $\text{Ticket}_{\text{ICD}}$ itself is timed. Each session secret key is timed. In our simulation, once the patient's ICD gets the temporary key, it records a time stamp and sets up a specified timer. Only the service request message encrypted with the temporary key, K_S, received from an EP within specified time period is served by the ICD. Otherwise, the service request is discarded and the process is ended. We experimented the timer with 30 seconds and 1 minute.

4.1.2 Scenario 2: Clinical Consultation, Any External Programmer, Smartphone Absent

In this scenario the external programmer (EP) will contact the ICD directly. The EP-user enters the master secret code to log into the ICD. EP and ICD for direct communication were simulated with java programs in two computers. This scheme can also be applied in an emergency scenario between ICD and EP as discussed in Scenario 4.

4.1.3 Scenario 3: Patient Incapacitated, Smartphone Present

Heart activity monitoring is a key characteristic of an Implantable Cardioverter Defibrillator (ICD). This paper proposes an extended feature of ICDs that makes it capable of transmitting information to the patient's smartphone. In that case, patient's smartphone is continuously listening to the patient's ICD, which plays a key role in delivering important messages during emergency.

In our investigation, a random number generator (RNG) simulated the monitoring process in the ICD's end. For instance, if the number generated by RNG appears to be less than 100000, it is declared that an irregular heart activity has been encountered and that random number is sent to the smartphone to simulate the temporary access code delivery. As soon as the random number is selected and sent, a time stamp is recoded and timer is turned on. This timer will represent the temporary nature of that access code. The patient's smartphone on the other end runs a service in android platform that is always listening at a dedicated port for alert messages from the ICD. In reality a patient's ICD is programmed to collect heart activity and a certain threshold of signals will initiate it to supply shock to the heart. This feature can be exploited to a bigger extent. Any possible life threatening or unusual activity can be sent as alert to the smartphone.

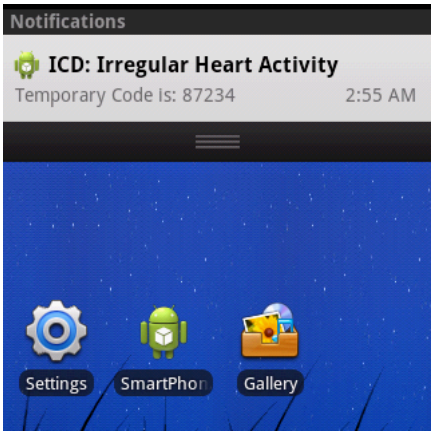

Figure 10: Screenshot shows simulation of irregular heart activity and secret code delivery in Smartphone

The alert message contains a message and a temporary access code. The smartphone displays the alert message with sound and vibration to alarm the patient. A patient can discard the message if everything is fine. If the cause of the irregularity is an extreme physical activity for instance, the patient may reduce the intensity of ongoing activity. But, if for some reason the patient falls incapacitated, the message is still on the phone and provided that medical practitioner arrived at the scene, the patient's heart activity history can be extracted by using temporary access code displayed on the phone. The temporary access code is time limited and session specific. The screen-shot of monitoring activity from the smartphone is presented in Figure 10. It simulates the display of temporary code **87234** in the smartphone that was generated and sent from the ICD as an indication of some unusual activity in patient's heart. The message reads **ICD: Irregular Heart Activity. Temporary Code: 87234**. Handling the situation after this point can be done in many interesting ways such as recording and sending geographic coordinates with SMS or making an auto emergency call. This can be a future research for incident response and effective information management.

The scenarios explained above are assumed to be the most general cases. The proposed scheme is able to handle both the active and passive adversaries. The strategy of using secret key involves using temporary and session keys derived from the secret code rather than the secret key itself. This will limit the exposure of shared secret key to a minimum, thus reducing the possibility of replay attacks from the adversaries [11]. The use of private keys system is free and consumes a lot less computation power than public key cryptography [15, 17, 18].

Another key feature of a Kerberos based scheme is that it is stateless [20]. That is, in any case, the session keys are not shared with the ICD directly and always delivered via EP through the $\text{Ticket}_{\text{ICD}}$. That way, the ICD does not retain the state of the session key before the EP gets the session key. With this property, this scheme is least vulnerable to the replay attacks. The proposed scheme delivers robustness, by maintaining security and privacy even when the smartphone isn't available. Using human biometric data such as the patient's fingerprint, can apply exactly similar process, provided that EP is capable of translating fingerprint into a unique digital key.

The MacBook Pro was used to simulate the EP. It was equipped with 2.5 GHz processor, 8 GB main memory and OS X 10.9.6 operating system. Dell N5010 was used in simulating the patient's ICD, which was had a 2.53 GHz processor, 3 GB memory and 64 bit Windows 7 Home Premium operating system. The snapshots for smartphone display are from Huawei U8650 smartphone with 600 MHz processor that ran Android 2.3.6 Gingerbread operating system. Android Studio IDE was used to develop the Android application.

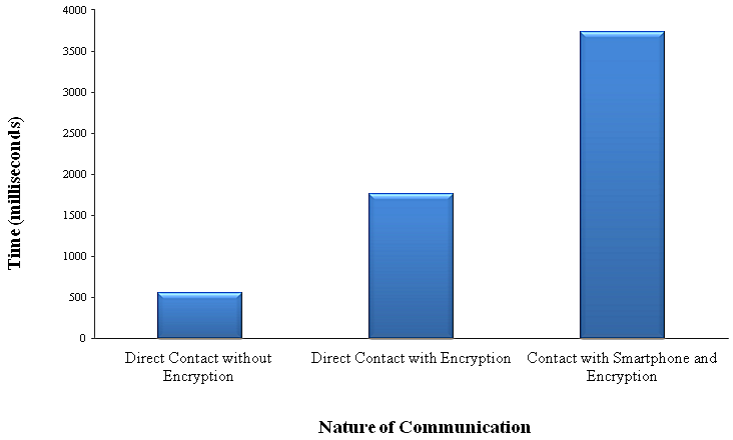

Figure 11: Timing overhead in different types of communication

4.2 Timing Overhead Evaluation

The average timing overhead evaluations were done for three different types of scenarios. Firstly, timing overhead was measured for the process of contacting the ICD directly from EP without any encryption. Secondly, the ICD was contacted directly by the EP with an 128-bit AES based encryption. Thirdly, the timing overhead for a general scenario of a registered EP with patient's smartphone to contact the patient's ICD that demonstrated 128-bit AES based encryption algorithm was measured. In all three cases, a file of size 200KB was requested and received by the EP. Timing overhead was recorded for each case for 100 times and average for each case was computed. A bar diagram depicted in Figure 11 shows the difference in overall timing overhead in different types of communication tested. It presents the ratio of three different time values in different types of communication.

Direct communication made between the EP and the ICD without encryption took 556.68 milliseconds in average. Direct contact of the ICD by the EP with an AES encryption took 1763.27 milliseconds and it took 3726.7 milliseconds in average for communication encrypted with the 128-bit AES cryptographic algorithm with smartphone. A rough estimation of ratio among three time values is 1:3:6, respectively.

Table 1 indicates the size of the Java code and lines of codes written to simulate the three devices: The EP, ICD and Smartphone, respectively.

Table 1: File Size and Lines of Code

Code	EP	ICD	Smartphone
Size of Code	48KB	47KB	45.4KB
Lines of Code	535	583	1787

5 Related Work

In [10], the authors proved that the information exchanged during communication between an ICD and an EP is in clear text and thus unprotected. They demonstrated that the information could be viewed and modified and battery-powered ICD could be manipulated to communicate with any unauthenticated

device. The adversary could change the information in the ICD including therapy settings such as shock levels that could be deadly to the patient. Their work also presented a defense mechanism for unauthorized attacks, which the authors referred to as Zero Power deterrence and prevention system.

Denning et al. in [4, 22] gave new research directions regarding a defensive technique called Communication Cloakers. It protects the IMD from unauthorized access but allows open access during emergencies. The messages are encrypted using symmetric key cryptography but during emergencies, a cloaker is removed from the system to contact the IMD directly by the programmer in plain text.

Xu et al. [22] provided a technique for using an external device that they named Guardian and the scheme as IMDGuard. The IMDGuard is explained as a comprehensive security scheme for heart related IMDs. It describes a mechanism that uses Electrocardiogram (ECG) signals from different locations of the body. ECG signals from the heart area and other from the wrist, where the Guardian is worn, are taken to share a symmetric key between the IMD and the Guardian. The Guardian has a list of legitimate external device programmers and their corresponding public keys. The Guardian authenticates the programmers by sending a challenge and validating their signature. It also addresses patient safety by introducing an emergency protocol wherein the IMD itself sends two consecutive nonces in specified time intervals. The programmer picks up these nonces, calculates hash of the sum and sends back to the IMD. The IMD checks the received message for further communication. They also proposed a signal jamming mechanism, for the signal from spoof-attackers that try to force the IMD to go to an emergency condition.

In [9] and [1], the authors described techniques to secure IMDs from active and passive adversaries without changing the design with the help of an external Shield. This approach would benefit all the existing IMD's and can be implemented in new IMD's preventing the recall of the existing devices. The shield acts as a gateway that relays messages between the IMD and the EP. It uses physical layer to secure the communication with the IMD and uses a standard cryptographic approach to communicate between the authorized parties. The Shield provides confidentiality by continuously listening to the transmissions and jams them so that it is impossible for eavesdropper to decode. It can simultaneously listen to IMD's signal and transmit a jamming signal. The channel creates a linear combination of transmitted signals. Jamming signal with a random signal provides a form of one time pad encryption, where only parties that recognize the jamming signal can decrypt the message.

The work in [18] suggests using an internal co-processor to secure IMDs. The IMD processor is divided into two modules. The author claims that it is possible to secure IMD by introducing a co-processor that will coexist with the main IMD processor without consuming too much energy.

Research in [4, 5, 22] shed light on design challenges and preferences in regard to human values, interests and assurance. This motivates our work to involve the patient or other human user in authentication and assurance.

6 Conclusion and Future Work

This paper proposed a new defense technique in improving security and privacy of patient's information, and safety of the patient with implantable cardioverter defibrillators using smartphones. Symmetric key crypto was employed in all the communications involved for confidentiality. Symmetric key cryptosystem is cost effective and consumes low power, and hence preferred over public key cryptosystem in this scheme. Session keys were used whenever possible to minimize replay attacks and maintain perfect forward secrecy. Random nonces were implemented with messages to validate the received message and keep the transmitted message fresh. The proposed approach divided the external programmers into two categories: Registered and Unknown (unregistered or new), and addressed the security scenarios accordingly. The proposed scheme addressed both the active and passive adversaries. Smartphones are

utilized to do most of the computation, key distribution, and delivery of notification messages to the patient. A patient can play a significant role in protecting herself from the adversaries by involving herself in the security loop. A patient(user) is also given an authority to allow or deny a from continuing the communication.

This paper addressed regular clinical consultation and emergencies scenarios and the techniques to handle them securely and safely. It further stretches the idea of secure communication between EP and patient's ICD emergency situations, and in absence of patient's smartphone. It also explained how a master secret code could be used in regular scenarios and biometric information could be utilized during emergency, when smartphone is absent. A unique monitoring functionality in patient's ICD and the smartphone where the ICD would send an alert message about irregular heart activity with a temporary access code to the patient's smartphone was observed. This would help the emergency medics at the scene to access the ICD if the patient was incapacitated.

Since smartphones have become a part of our lives for numerous good reasons, carrying it all the time will not distress the patient physiologically. Smartphones are computationally powerful and applicably versatile. Therefore, a lot more feature can be exploited to make the patient's life easier and more secure.

A proof-of-concept of the proposed protocol was implemented to support hypothesis but the actual implementation still needs to be investigated. Since, ICDs are battery-powered devices that remain inside patient's bodies for many years, power utilization in using this protocol is a good area for investigation. It will be interesting to examine the proposed technique by simulating practical attack scenarios. Our future research also includes actual implementation of a proposed scheme in real bare metal ICD, EP and Smartphone, and investigation of power consumption and sustainability. Although smartphones fit just right for the solution proposed, whether it can be used efficiently as a cardiac event monitor is also open to research. Because smartphones can easily connect to the Internet or other form of communication, many interesting and novel information management can be done in the future.

References

[1] H. Al-Hassanieh. Encryption on the air: non-invasive security for implantable medical devices. MA. Thesis, Massachusetts Institute of Technology, 2011.

[2] E. Blaguszewski. Researchers find implantable cardiac defibrillators may expose patients to security and privacy risks; potential solutions suggested, 2008. http://www.washington.edu/news/2008/03/11/researchers-find-implantable-cardiac-defibrillators-may-expose-patients-to-security-and-privacy-risks-potential-solutions-suggested./.

[3] W. Burleson, S. S. Clark, B. Ransford, and K. Fu. Design challenges for secure implantable medical devices. In *Proc. of the 49th Annual Design Automation Conference (DAC'12), San Franciso, USA*, pages 12–17. ACM, June 2012.

[4] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel. Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Proc. of the 28th ACM Conference on Human Factors in Computing Systems (CHI'10), Atlanta, GA, USA*, pages 917–926. ACM, April 2010.

[5] T. Denning, K. Fu, and T. Kohno. Absence makes the heart grow fonder: New directions for implantable medical device security. In *Proc. of the 3rd USENIX Workshop on Hot Topics in Security (HotSec'08), San Jose, California, USA*. USENIX, July 2008.

[6] J. P. DiMarco. Implantable cardioverter–defibrillators. *The new england journal of medicine*, 349(19):1836–47, November 2003.

[7] fcc.gov. Medical device radiocommunications service (medradio), 2013. http://www.fcc.gov/encyclopedia/medical-device-radiocommunications-service-medradio.

[8] K. Fu. Inside risks: Reducing risks of implantable medical devices. *Communications of the ACM*, 52(6):25–27, 2009.

[9] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: non-invasive security for implantable medical devices. In *Proc. of ACM Special Interest Group on Data Communication (SIGCOMM'11), Toronto, ON, Canada*, pages 2–13. ACM, August 2011.

[10] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Proc. of the 29th IEEE Symposium on Security and Privacy (SP'2008), Oakland, California, USA*, pages 129–142. IEEE, May 2008.

[11] Helena. How many people use smartphones in the world, 2012. http://zeendo.com/info/how-many-people-use-smartphones-in-the-world/.

[12] W. Kainz, J. P. Casamento, P. S. Ruggera, D. D. Chan, and D. M. Witters. Implantable cardiac pacemaker electromagnetic compatibility testing in a novel security system simulator. *IEEE Transactions on Biomedical Engineering*, 52(3):520–530, March 2005.

[13] D. B. Kramer, M. Baker, B. Ransford, A. Molina-Markham, Q. Stewart, K. Fu, and M. R. Reynolds. Security and privacy qualities of medical devices: an analysis of fda postmarket surveillance. *PLoS one*, 7(7):e40200, July 2012.

[14] R. Krishnan and J. Ninglekhu. Smartphone-based secure authenticated session sharing in internet of personal things. In *Proc. of Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2015, San Francisco, California, USA*, volume 9411. International Society for Optics and Photonics, February 2015.

[15] A.-R. Mohammad, A. Rjoub, and A. Baset. A low-energy security algorithm for exchanging information in wireless sensor networks. *Journal of information assurance and security*, 4(1):48–59, March 2009.

[16] E. A. Moore. How to keep hackers away from your pacemaker, 2011. http://www.cnet.com/news/how-to-keep-hackers-away-from-your-pacemaker.

[17] S. U. Rehman, M. Bilal, B. Ahmad, K. M. Yahya, A. Ullah, and O. U. Rehman. Comparison based analysis of different cryptographic and encryption techniques using message authentication code (mac) in wireless sensor networks (wsn). *International Journal of Computer Science Issues*, 9(2):96–101, January 2012.

[18] D. Siskos. A co-processor for a secure implantable medical device. MA. Thesis, TU Delft, Delft University of Technology, March 2011.

[19] J. Slobbe. On security of implantable medical devices. MA. Thesis, Eindhonven University of Technology, 2013.

[20] M. Stamp. *Information security: principles and practice*. John Wiley & Sons, 2011.

[21] M. A. Wood and K. A. Ellenbogen. Cardiac pacemakers from the patient's perspective. *Circulation*, 105(18):2136–2138, March 2002.

[22] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li. Imdguard: Securing implantable medical devices with the external wearable guardian. In *Proc. of the 30th IEEE International Conference on Computer Communication (INFOCOM'11), Shanghai, China*, pages 1862–1870. IEEE, April 2011.

Author Biography

Jiwan Ninglekhu is doctoral candidate in Electrical Engineering (Computer Software and Security Engineering) at The University of Texas at San Antonio, TX, USA. He received his bachelor's degree in Electronics and Communication Engieneering from Tribhuvan University, Nepal. He holds an MS in Electrical Engineering and an MS in Computer Engineering from Wichita State University, KS, USA and The University of Texas at San Antonio, TX, USA, respectively. His research includes security in Medical Devices, Smartphones, Internet of Things (IoT) and Cloud Computing. He is a member of IEEE-HKN.

Ram Krishnan is assistant professor of Electrical and Computer Engineering at the University of Texas at San Antonio, TX, USA. His research includes but not limited to foundational aspects of computer security: Access control, Security Models, Security Policy Enforcement, Formal Policy Analysis, etc. His current research is mostly focused on security aspects of Cloud Computing.

Eugene John is professor of Electrical and Computer Engineering at the University of Texas at San Antonio, TX, USA. His research area is VLSI system design in all kinds of applications focused on Low Power Circuits and Systems, Power Estimation and Optimization, Multimedia and Network Processors, Computer Architecture, Performance Evaluation and Biometrics.

Dr. Manoj Panday is board certified in Internal Medicine, Cardiovascular Diseases, Nuclear Cardiology, and Clinical Cardiac Electrophysiology. He is an Assistant Professor of Medicine and Head of the Section of Cardiac Electrophysiology at the University of Texas Health Science Center at San Antonio. His practice involves the implantation of permanent pacemakers, internal cardioverter-defibrillators, and cardiac resynchronization therapy devices. In addition, he performs electrophysiology studies, catheter ablations for supraventricular and ventricular tachycardias, laser lead extractions, and various other complex procedures to treat a variety of arrhythmia disorders.