Study of Wireless Security Attacks on Medical Devices

Atchaya Arivalagan[1], Naga Nikitha Peddi[2], Wajdi Bazuhair[3], Vahid Emamian[4]

[1]Department of Engineering, St. Mary's University, San Antonio, Texas 78228, atchu2794@gmail.com

[2]Department of Computer Science, St. Mary's University, San Antonio, Texas 78228, nikithapeddi@gmail.com

[3]Department of Engineering, St. Mary's University, San Antonio, Texas 78228, wajdi.bazuhair@hotmail.com

[4]Department of Engineering, St. Mary's University, San Antonio, Texas 78228, vemamian@gmail.com

ABSTRACT

In the treatment of chronic diseases, wireless Implantable Medical Devices (IMDs) are commonly used to communicate with an outside programmer. Such communication raises serious security concerns, such as the ability for hackers to gain access to a patient's medical records. This brief provides an overview of such attacks and the new security challenges, defenses, design issues, modeling and performance evaluation in wireless IMDs. While studying the core ideas and potential vulnerabilities of IMDs, the reader will also learn and get brief introduction about threats, selection of choosing the better technologies based on the criteria for the design of security system involved with physicians and patients network, modeling, and security analysis, thus keeping pace with quickly-evolving wireless security research.

Keywords: Implant medical devices, security, threats, vulnerability

1. INTRODUCTION

The advances in medical device technology has proven to be the effective measure of enhancing the health maintenance of a human body. One dimension of such technology in healthcare services is through wireless communications. When Implant medical devices as well as body sensors injected to human body for the health maintenance, are being transmitted through the patient's network to the physician's network through the wireless medical device network standards. During the transmission of sensitive information between the networks, the basic attributes of the security namely confidentiality, availability, and integrity as well as the extended parameters such as access control, authentication, identification, non-repudiation, etc. are affected.

Compromise of sensitive information from the human body could lead to hazardous acts, affecting the reputation of physicians and business units organizing the manufacture of medical devices and therefore the security measures need to be enhanced. Medical device manufacturers play an important role in developing devices that are safe, reliable, and secure. This added responsibility is extremely important as we develop multiple devices with wireless technology and we develop medical devices that push the link between humans and computers. Building trust for these companies will involve their ability to provide devices that keep people safe and their information secure. The FDA has a major role in developing appropriate security measures for manufacturers to incorporate into the designs of their devices. The FDA does not need to provide legislation that will hinder development of medical devices, but they do need to provide structured guidelines on the acquisition of devices after use, the development of security measures for wireless devices, and device failure protocols. This research focuses on the concepts of securing the sensitive information while communicating through medical devices, the impact and security improvement measures to mitigate the characteristics of vulnerabilities involved in the medical application.

1.1. Background

Implants medical devices as well as body sensors provides external assistance to patients as well as physicians by effective monitoring of human health either through short-range or long-remote location according to the wireless medical device network standards. Examples of implant medical devices are pacemakers, insulin pump, defibrillators, nerve stimulators, active monitoring devices (body sensors), etc. monitoring various organs of the human body. The compromise of sensitive information would be performed by hackers (vital signals, diagnosed conditions, therapies, personal data etc.) which happens when the transmission of data from patients to the physician's network by the hackers raising the insecurity concerns for the patients, hospital administration, physicians. The effect of compromising the sensitive information could lead to great loss to the patient's life, medical device manufacturers, hospital as well as physician's reputation. The history behind the background in the evolution of some of the implant medical devices and their relative attacks have been formulated in the later paragraphs.

In 1920s, Diabetes became a major issue because many people were having complications from the disease leading to death of many diabetic patients. To support the life of several diabetic patients, a first insulin pump is developed in the year 1960 but

faced with several drawbacks. As the number of diabetic patient's rate increases allowing the manufacturers to develop new pumps that allow for the patient's glucose levels to be tested and insulin to be delivered in one system and the newly designed systems have software and wireless capabilities to track and manage patients' glucose levels. By 2012, new insulin pump is developed which is incorporated with Bluetooth 4.0 technology facilitating bidirectional communication information about the patient and allows the insulin to be administered without the need to touch or interact with the pump. In security attack of the insulin pump demonstrated by security researcher, Jay Radcliffe, and shared his findings at the black hat security conference entitled "Hacking medical devices for fun and insulin: Breaking the Human SCADA System". It stated that the attacker intercepting the wireless signals and then broadcasting the strong signals to change the blood sugar level readout on the insulin, taking control of insulin pump and glucose monitoring system. With the continuous process and reverse engineering practices, life of a diabetic patient is threatened and leads to the loss of lives of various diabetic patients.

Similarly, the pace makers faced many structural disadvantages and evolved into new device handling the cardiac problem of heart patients in an effective and efficient manner. In 1932, Albert Hyman developed a machine that he called the artificial cardiac pacemaker. After many advancements, pacemaker is developed with high battery and technical capabilities making pacemakers to implant in the human body. A real-time example of such security attack is the attack of former US Vice president Dick Cheney's pacemaker. This attack is one of the example of cyber warfare/terrorist activities where the attackers intercepted the incoming wireless signals and injected the malware, susceptible to unauthorized access and denial of service which leads his doctors to disable the wireless pacemakers thwarting to save the life of former US vice president, Dick Cheney.

2. MECHANISM

2.1. Communication Standards

The choice of the medical devices to be used in treating and monitoring patient's health is based on the factors like quality of the medical devices, communication standards to the implantable medical devices, security of communication networks, mode of communication, allocation, and usage of spectrum to the medical devices. Based on the above factors, are selected. The three federal agencies, the Federal Communications Commission (FCC), Food and Drug Administration (FDA), and the Centers for Medicare and Medicaid Services (CMS) holds responsible for the selection of the medical devices which are used in hospitals to patients for their treatment and health monitoring (internal and remote).

When the medical devices either internally implanted or externally connected to the patient's body, the information generated from the medical devices has to be transmitted from the patient's network to the physician's network. The transmission of information could of either short-range (within the hospital) or long-range communication (remote network connectivity). The technologies used for short range communication are Inductive Implants, Medical Device Radiocommunication Service (MICS), Wi-fi, Bluetooth, & ZigBee (902-928, 2400-2483.5, 5725-5780 MHz), Ultra-Wideband, Medical Micropower Networks, and Medical Body Area Networks. The technologies used for the long-range communication between medical devices and physicians are Wireless Medical Telemetry Services (WMTS), and Worldwide Interoperability for Internet Access (WiMAX). Wireless Medical Telemetry Services (WMTS) shares with other medical devices with the spectrum of 14MHz ranging three defined frequency bands: 608-614 MHz, 1395-1400 MHz, and 1427-1432 MHz whereas WiMAX an IEEE 802.16 standard, operates at a speed of 70Mbps and uses frequencies around 2.5GHz in the U.S. RFID (Radio Frequency Identification) consists of tags and readers where tags emit radio waves(containing data and identity information about reader devices) to the reader devices which contains antennas which emit and receives radio signals from RFID tags.

The important risks faced in the transmission of medical devices between patient's and the physicians network is the Electromagnetic Interference. Electromagnetic inference is caused by interaction of two different signals causing modification of information and leads to vulnerable condition. Risk analysis is performed to optimize electromagnetic interference by working on the security features of information transmission. Some of the factors like selection of wireless technology, quality of service, coexistence, security, and electromagnetic interference should be taken in consideration for the efficient operation of transmission of information between medical devices and physician's network.

2.2. Threats

Exploits are the ability to take advantage of a weakness in an operating system or a sequence of commands that takes advantage of vulnerability in a system. The goal of an exploit is to cause an unattended or unprotected system to fail or to anticipate behavior and control within a system. This is a problem for medical devices because you do not want unauthorized individuals to gain access or get privileges over the devices or information stored. Recently, research has been done on the ability to gain access to and gain influence over insulin pumps and make the insulin pump inject on command. This type of exploit can be difficult to deal with because it takes advantages of glitches or bugs in the software code. It is important that medical device manufacturers develop some update procedures to deal with glitches that arise after manufacturing. These devices hold important private data about the client. A glitch in the system that allows for information to be changed within a device could set the stage for an individual to commit a murder or alter the data to make it difficult for a

patient to get treatment. One of the most likely outcomes of having wireless medical devices is that someone will develop a virus or a worm that will infect the implantable device causing it to malfunction or drain its battery. It is likely that a virus will be developed to propagate itself using the Bluetooth of a cell phone with no intention of infecting medical devices, but will cause issues with the medical devices unintentionally.

With the development of more medical devices using wireless technology, one of the issues that has to be taken into consideration is the ability for people to eavesdrop information from these devices. Information is being collected on us daily through social network websites, where we shop, how we use our phones, and what we buy on the Internet. The information on medical devices could include your personal information, your health status, your location, and your medical history. This information could be vital for identity theft and political advantage. Individuals eavesdropping for this type of information could use it to blackmail people of power and change public opinion of the potential political candidate. We have already seen some of this done when hackers hacked into a politician's private emails and spread private conversations around the Internet. The potential for private medical information to cause turmoil within the political structure is very likely.

Hacking of medical devices could create a backdoor into hospital networks. Medical information is just as valuable, if not more, then financial and other personal data. There have been medical network breaches, but much of the information surrounding how the attacks happened has not been released. Researches have been able to identify ways the vulnerabilities in these medical devices. Some medical devices are in receive-only mode, or exclusively send information instead of receiving any, but some both send and receive, which are the most vulnerable of devices; but anything connected to the internet is at risk. Infusion pumps, surgical robots, pacemakers, insulin pumps, and cochlear implants are some of the devices that are wireless capable. Some of these have already been penetrated by security researchers and others are being evaluated, as the potential is there. Many security researchers are questioning if medical device hacking will be the biggest concern in upcoming years.

2.3. Core Idea

As medical devices gain the same interconnectivity that most our daily life gadgets has, it is apparent that patient care has never been better. As technology evolves and opens new possibilities in our everyday interactions, so does medical devices. Beneficial technologies that were applied to patient care are better embedded systems, low power micro controllers, efficient bluetooth and wifi connectivity, and higher memory management. All of this resulted in a very fast growth when it comes to the possibilities that technology offered to the health care system.

However, the real issue is that the rapid advancement only focused on what the businesses are demanding ignoring the security risks involved. Today's designers are putting so much effort creating new and more efficient systems while ignoring the security concerns that might arise. Hackers can gain access to medical devices using several techniques, such as firmware defects, absence of tamper proofing, poor software engineering, Third-Party vulnerabilities, and Network misconfiguration.

The root cause of such problems is that most medical devices were conceived before the evolution of cyber security, following an iterative design approach that builds new updates and features on top of the old code base, causing the new devices to be built upon legacy code and infrastructure prone to errors and vulnerabilities.

2.4. Potential Vulnerabilities

As with any smart device connected to the internet, there is always a privacy concern. Not all medical devices are the same, and there is a wide variety of different flaws found across them, however we can agree that the most prominent vulnerabilities can be found in the form on code defects, poor tamper prevention algorithms, incomplete software engineering and testing, third-party flaws, and network misconfiguration.

Code or firmware defects are one of the most popular forms that hackers can take advantage of. Often software developers focus on providing the required functionalities while ignoring the security implications of their actions. One example is SQL injection, where a malicious user can enter a sequence of code in input forms to gain access to database protected information, or execute code commands that would alter the output. Another example is known as overflow error. Overflow occurs when the software is not protected against overflowing memory, this happens when a variable or memory locations is fed a set of data that exceeds the allowed allocation, making it easy to override the adjacent memory cells and even run a malicious code.

Poor tamper prevention algorithms are also widely common, this can be a very time-consuming process, and the developer needs to be aware of most if not all the possible outcomes of the software operation, therefore the system can easily detect an anomaly when an illogical value for example is introduced in the system. Hackers usually try to take advantage of poorly written systems by altering results or inputs data that won't be possible in a normal usage. Therefore, it is crucial to have a watchdog process to continuously monitor sensitive variables and data and make sure that they are within the acceptable range of operation.

Software engineering is another area where security is not really the main focus. A recent study has shown that a popular medical interface MD Link had a major vulnerability in its login system. All the passwords were stored locally in the hard drive, in plain

text without any sort of encryption. What's even more disturbing is that the software had a well-known back-door to have full access in case the operator forgot the password. It has a hardcoded admin password to reset the device, and all the information on how to use it was on the instruction manual. All it takes a malicious user is to get hold of the manual to gain full access to the software.

Therefore, it is necessary to make sure that the software design an engineering takes full measures against vulnerabilities.

2.5. Cryptographic Algorithms

Encryption is the process of encoding a message or information which is designed in such a way that only the authorized parties can access the information. There are two types of cryptography involved in encrypting and decrypting the information namely symmetric and asymmetric cryptography. Among the two types, asymmetric cryptography (public key cryptography) is considered as efficient method since it involves both public and private key for encoding and decoding of information fulfilling the two essential security parameters namely authentication and confidentiality. Asymmetric algorithms use receiver's public key for encryption which is authenticated to corresponding receiver with the help of recipient's private keys. Another form of public key cryptography is formation of digital signature where digital signature is formed with receiver's private keys which can be authenticated with corresponding receiver with their public keys.

RSA(Rivest–Shamir–Adleman) Algorithm is first practical public key cryptography used to encrypt the messages with receiver's public keys and decrypted at the receiver end with their private keys. The operation of RSA algorithm involves four steps namely key distribution, key generation, encryption, and decryption. The process of key generation involves with the assumption of two random prime numbers p and q, computing key length (n=modulus of public and private keys) for both public and private keys where n=p*q, followed by computing value e from carmicheal's totient function and finally calculating the private keys at the receiver end. Key distribution process occurs by encryption of information with receiver's public keys and decrypted at the receiver end with their private keys. In encryption process, cipher text is computed with message m and public keys e with the formula where the original message is recovered with the computation of cipher text with the private keys.

Two distinct prime numbers = p, q

n = p*q, where n=key length of p and q

$\lambda(n) = lcm(\lambda(p), \lambda(q)) = lcm(p-1, q-1)$ where λ is carmicheal's totient function

choosing integer e from $1 < e < \lambda(n)$ and $gcd(e, \lambda(n)) = 1$

$d = e^{-1} \bmod(\lambda(n))$, where d = modular multiplicative inverse of e modulo($\lambda(n)$)

cipher text produced during encryption at the sender is,

$cipher\_text = message^e \bmod(n)$, where message = padded plaintext M

Decrypted message produced during decryption at the receiver is,

$Cipher\_text^d = (m^e)^d = m \bmod(n)$

The Diffie-Hellman Key exchange protocol achieves forward secrecy generating new key pairs for each session and discarding at the end of each session. This protocol is widely used due to its fast generation of common shared secret keys. The operation of the protocol involves with the computation of commonly shared secret key s at both sender and receiver. Initially two integers, multiplicative group of integers modulo p and primitive root modulo g are taken and message sent part from both sender as well as receiver with the help of secret integers sender and receiver. Finally, shared secret key to both sender and receiver is computed with the above formula:

p = multiplicative group of integers modulo

g = primitive root modulo of p

Sender sends the message to the receiver is:

$A = g^a \bmod p$, where a is sender's secret integer

Also, receiver sends the message to the sender is:

$B = g^b \bmod p$, where b is receiver's secret integer

Global shared secret key (S) computed at the sender and receiver as given below:

$S_{sender} = B^a \bmod p$

$S_{receiver} = A^b \bmod p$

2.6. Bluetooth Technology in Wireless Security

Bluetooth is the open wireless technology standard for exchanging data over short distances from fixed and mobile devices, creating personal devices. It is operated under Industrial, Scientific, and Medical band (ISM) at the frequency of (2.4-2.485 GHz). Bluetooth technology is a packet-based protocol based on master-slave architecture involving various types of networks such as ad-hoc network (connecting multiple type of devices), piconet (small cluster of devices where master device deciding the frequency of the channel), and scatter nets (large network formed with 10 piconets). Frequency-hopping spread spectrum is used as data transmission mechanism and gaussian frequency-shift keying modulation scheme involved for the Bluetooth technology. The data to be transmitted is divided into packets and send each packet into one of 79 designated Bluetooth channels (40 channels each of bandwidth

2MHz for Bluetooth low energy with adaptive frequency hopping) where each channel has 1MHz. The main features of Bluetooth wireless technology standard are low cost, low power, and robustness.

Bluetooth standard uses various protocols for exchange of data from patients to physician network. Bluetooth protocol stack containing various protocols are listed under the two categories controller stack (implemented at the lower levels of OSI layer) and host stack (implemented at the higher levels of OSI layer). Host stack contains various protocols such as L2CAP, BNEP, RFCOMM, SDP, etc. Logic Link Control and Adaptation Control (L2CAP) transmits data packets to either the Host Controller Interface (HCI) or to the ACL/ASB/PSB link. Bluetooth Network Encapsulation protocol (BNEP) is similar to L2CAP used for personal area networking (PAN) profile. Radio Frequency Communication (RFCOMM) is a cable replacement protocol providing serial line interface to all the applications. Service Discovery Protocol (SDP) helps to discover the services offered by the devices to the users.

The main security threats involved in Bluetooth standard during the information of sensitive information in the medical devices are denial of service (making device unusable and draining the battery of connected devices), fuzzing attacks (sending malicious messages to the Bluetooth centric devices leads to modification and destruction of information), blue jacking (causing harm to devices as well as patients by bypassing information and received by the user which is not intended to it), disclosure threat (violation of confidentiality), and integrity threat (unauthorized changes of information during transmission).

Various possibilities of how the information can be prone to get vulnerable when transmission of information through Bluetooth wireless technology standard can be referred from the author [13]

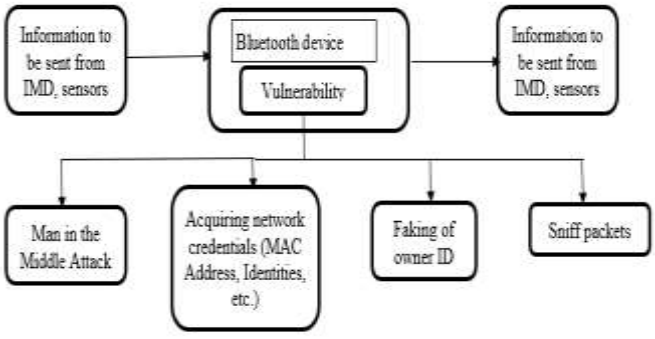

Figure 1: Ways/Methods in which the information can be prone to vulnerable when transmission through Bluetooth technology standard

2.7. AI and Wireless Security

The main focus nowadays revolves around artificial intelligence, mainly deep learning algorithms, genetic algorithms and neural networks. AI has been seeing a huge exponential growth this past few years as computer processing power increased and a higher level of parallelism is possible. Many technologies have started using Ai in real world applications such as Tesla, with its auto-piloting abilities, making use of image recognition, sensor networks, and user feedback. Google and Microsoft are also investing a huge portion of their resources developing Ai. Many have started to realize the extreme potential of machine learning, and how it might be the next ultimate weapon if developed in the right direction.

Artificial intelligence is not really a new technology, it has been around many years ago, but due to the lack of capable hardware, it was never a point of interest until recently. Deep learning and neural network algorithms tend to mimic real life biological structure, such as the nervous system, the genetic evolution, and the role of the brain in processing the collected data.

A neural network algorithm works similarly by running several layers of abstraction, each connected to the other by an output/input relationship. As data is fed to the system, those networks will react to it and adjust accordingly to perform a specific task.

AI is a great technology to have, it solves several complicated problems, can accurately predict events, and helps achieve a higher level in image processing, speech, and facial recognition.

However, with great power comes great responsibility. As powerful and useful as it seems, artificial intelligence is a major security threat, especially in the cybersecurity domain. Since it has the ability to reduce complicated brute force methods into a simpler predictive way, it can be easily used to decrypt network keys for example, guess passwords, and even find vulnerabilities in a given system.

Likely AI is also being used to increase networks security, using genetic algorithms for example.

2.8. Applying AI to Increase Network Security

As discussed above, there are so many benefits of using AI in our daily life routines, especially when it comes to security.

AI can help secure communication networks by implementing a genetic algorithm to dynamically evolve a set of rules for packet filtering.

In a traditional setup, devices are connected to a router, and behind a firewall that has a fixed set of rules to protect the network. For example :

if (Address IP == bad) => block connection

or

if (incoming connection on Port 111) => Deny

Using a genetic algorithm, we should be able to continuously evolve those rules to make it more efficient, reduce false positives, and create new rules for undetected vulnerabilities.

A genetic algorithm works by creating a random initial population of potential candidate solution, evaluates it using a fitness function, selects the best candidates, apply crossover and mutation to its DNA and then generate a new evolved population. Those steps are repeated until a satisfactory solution was found that satisfies the fitness function. On each iteration the result is corrected using crossover and mutation following a pseudo-random pattern that depends on the previous level of success.

Kostenko, Frolov suggest the following model in choosing the probabilities of the mutation and crossover where N is the number of optimized parameters and P the population size.

$$M_{mut} = (m_{i,j}^{mut})_{i=1,j=1}^{N,P}, \quad M_{cr} = (m_{i,j}^{cr})_{i=1,j=1}^{N,P}.$$

A simple logic flow of algorithm is as follow:

Figure 2: Flow chart of the simple genetic algorithm which correlates with the extraction of clear information, removing malfunctioned signals/information from the transmitted information

An example of Cross over is usually done by splitting a portion of Data 1 and Data 2, and mixing it's DNA as the following

Data 1 : 010111 | 01011011

Data 2: 110101 | 01100101

Result : 010111 01100101

Mutation is simply inducing a binary change randomly in order to create a variation and possibly evolve the candidates into a better solution.

Data: 10010101101011

After mutation: 10010101001010

The newest generation replaces the old one, and the process is repeated again.

This will create a dynamic set of network rules that always tries to evolve to a better optimized and secure version instead of relying on fixed firewall instructions.

3. FUTURE DIRECTIONS

This paper could take to the further advanced level of research in certain areas which are mentioned as below:

- How well security parameter (Advanced techniques of encryption & decryption (public key cryptography), digital signature, routing protocols) is enhanced from transmission of sensitive information from patient's network to the physician's network.
- Making the transmission to be bidirectional and testing the implementation techniques with various network standards.
- Finding the efficient method to treat the diseases/unusual effect of a patient in a remote location
- Designed as a defense/detective mechanism by police officers to find out hackers creating threats in medical devices as well as to patients
- Using of communication system in conjunction with packet analyzer to detect the vulnerabilities present in the security system.

4. RESULTS

In this paper, the motives for the cause of security attack is identified. Security attacks can be minimized by limited access to the device to an extent and ensuring/enforcing proper user

authentication, session termination/timed sessions, use of strong passwords, physical security measures (e.g. locks) and efficient cryptography mechanisms [15]. Software content gains quality of trust by restricting updates to authenticated users and proper encryption methods implemented at both physicians and patient network. In this paper, the architecture can be proposed which helps to improve security in the communication system involved with patients and physicians.

An algorithm can be designed for the secured communication system involved with patients and the physicians. This algorithm involved with sensing the vital/essential signs required to be transferred to physicians are then transmitted through the open wireless technology standard. After checking with the attributes of the security parameters and content of the encrypted message, check for the threat detection. If the vulnerability state is detected, the system raises notification and interrupts the information to be sent to the desired recipient else the information is sent to second level of threat detection. Second level of threat detection consists of detecting the credentials of the wireless device as well as sender's device with the individual and global profile identifying the fake device (hacker's) identity. After the second level threat detection, if the threat is detected, the system raises notification and interrupts the information to be sent to the desired recipient else the information is sent to third level of threat detection. Third level threat detection consists of detecting the malicious/hiding signals present in the information with the help of electronic devices. After the second level threat detection, if the threat is detected, the system raises notification and interrupts the information to be sent to the desired recipient else the information could be transmitted to intended/desired recipient.

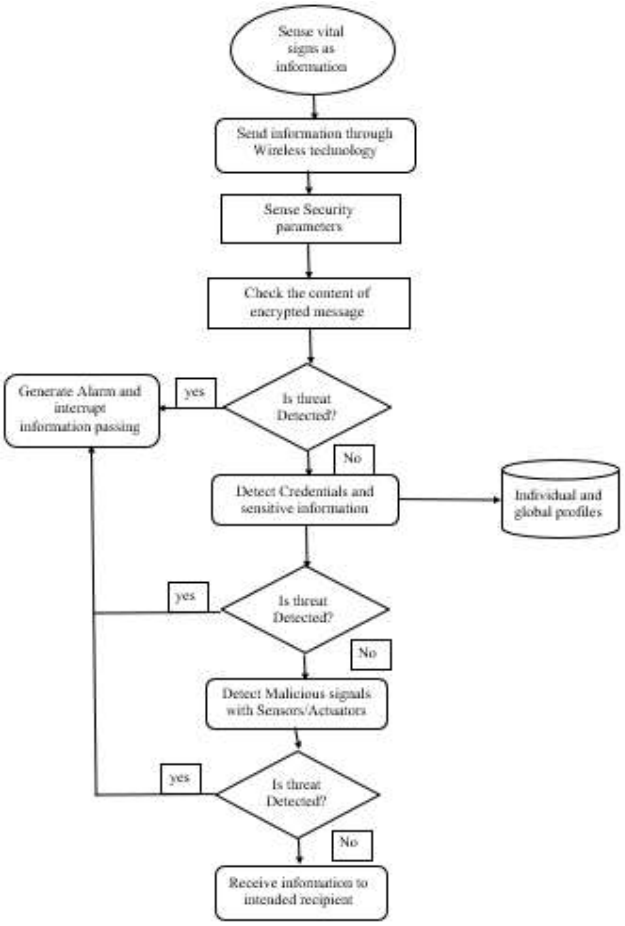

Figure 3: Proposed three-layered security architecture intended to establish security between patients and physician network through open wireless technology standard

5. CONCLUSION

In this paper, the evolution of the security attacks of the medical devices, and reason for the attacks in the medical device network system is identified. Various threats formed as result of the compromise of information is shown. Choice of wireless technology standard proves to be the best way for efficient transmission of information from patients to the physician/hospital network which is selected upon the set of selective criteria. Improper software engineering practices, poor tamper prevention algorithms, code/firmware defects, etc. are shown to be crucial reasons for the information prone to attain vulnerable condition. The basic vulnerable mechanism Three-level layered algorithm centered for secure transmission of information from patients to the physicians/hospital network helps to retain the security parameters and minimize the vulnerability involved in the network. Proposed results and future directions towards better prevention of security attack and proper message is received to the physicians.

6. REFERENCES

[1] Kobes, Shelby David, **Security implications of implantable medical devices, Graduate Theses and Dissertations**. 13683, 2014.

[2] Mandeep Khera. **Think Like a Hacker**, Journal of Diabetes Science and Technology. Vol 11, Issue 2, pp. 207 – 212, 2016.

[3] Pedro Peris-Lopez and Jaun E.Tapiador. **Security and privacy issues in implantable medical devices: A comprehensive survey**, Journal of Biomedical Informatics. Volume 55, Pages 272-289, June 2015.

[4] Patricia AH Williams and Andrew J Woodward. **Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem**, Med Devices (Auckl). 8: Pages 305–316, 2015.

[5] Articles on the compromise of former US Vice President Dick Cheney's pacemaker

[6] Article on compromise of insulin pump, **Black Hat: Lethal Hack and wireless attack on insulin pumps to kill people** from computer world.

[7] **Wireless Medical Technologies: Navigating Government Regulation in the New Medical Age**, Updated November 2013, Fish & Richardson Regulatory and Government Affairs group.

[8] Description of Wireless Medical Devices by the U.S. Department of Health and Human Services, Food & Drug Administration (FDA).

[9] Wikipedia articles about public key cryptographic algorithms, RSA and Diffie-Hellman key exchange protocol.

[10] Articles from Harvard Business Review, Medical system Hacks Are Scary, but Medical Device Hacks Could Be Even Worse.

[11] Articles from INFOSEC Institute, Hackable Medical Devices.

[12] Wikipedia articles about Bluetooth wireless technology standard.

[13] TJ. O'Connor. **Violent Python – A cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers**, Syngress, imprint of Elsevier, ISBN: 978-1-59749-957-6, Pages 201-210.

[14] V.A Kostenko. **Self-learning genetic algorithm**, Journal of Computer and Systems Sciences international, volume 54, Issue 4, pp 525-539, July 2015.

[15] Chakraborty, R, Mandal, J.K. **Secure Encryption Technique (SET): A Private Key Crypto System**, in the International Journal of Multidisciplinary in Cryptology and Information Security (IJMCIS), ISSN 2320-2610, Vol.4, No.1 (January – February 2015 issue), pp.10-13, 2015.