IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 3 - V7I3-2210)
Available online at: https://www.ijariit.com

A Study to Investigate the security issues in IMD

Sahana
sahanab@rvce.edu.in
RV College of Engineering, Bengaluru, Karnataka

Sindhu Rajendran
sindhur@rvce.edu.in
RV College of Engineering, Bengaluru, Karnataka

Vibha Narayan R.
rvibhanarayan.ec18@rvce.edu.in
RV College of Engineering, Bengaluru, Karnataka

Rahul Pinny
rahulpinny.ec18@rvce.edu.in
RV College of Engineering, Bengaluru, Karnataka

ABSTRACT

With the ever-growing rise in smart devices and their applications in most of the sectors, there is a need for security as the information is transmitted using wireless medium of transmission. One of the most profound health care devices are the implantable medical devices used for monitoring and control of vital organs such as neural systems, heart and cochlear implants. Although IMDs provide quick and cost-effective diagnostic features to the patients there exist some design constraints and software threats which need attention. There is a chance of leakage of confidential data pertaining to the person with IMD by attackers , thereby manipulating the parameters of the devices causing the patient's life to be at high risk. In our paper, the different types of IMDs and their constraints are addressed. As the emphasis is on the security aspects of these devices, their requirements , the attack vectors, the type of attacks encountered and the protection mechanisms implemented till date are also discussed.

***Keywords* — IMD, Security, Attack Vector, Encryption**

1. INTRODUCTION

Medical devices are articles that are used in the diagnosis or prognosis of diseases or any other conditions, or in the cure, diminution, treatment, or prevention of disease in animals and humans. They form the essentials of modern medicine as they help in automation of the patient's monitoring system. Implantable Medical Devices (IMDs) are electronic devices which are implanted in the body to monitor the state or improve the functioning of some body part, treat a medical condition, or just to provide the patient with a capability that he lost due to medical conditions or ailments or did not possess before. Some of the available IMD's in the market are insulin pump, pacemaker, ICD (implantable cardioverter defibrillator), neurostimulators, accelerometer, gastric electric simulator, syringe infusion pump, biosensors, drug delivery systems. The IMDs can be classified as software only, hardware only or both. Most of the IMDs available use both hardware and software. These devices can be stand alone or can be connected to a network. Networking capabilities added to the IMDs is a great advantage, it helps in continuous monitoring, treating and remote diagnosis[1].

Recent technologies are continuously trying to integrate medical devices and healthcare with wireless communication. This helps in timely medical treatment and response to the patients by overcoming temporal, organizational and geographical barriers. Live feed of the status of the implantable device is available to the patients as well as a distant personal doctor. The communication channel being wireless can be accessed by everyone. The data flow in this channel is susceptible to attacks for not only determining its presence but can also access the logs of the IMD. To overcome this issue of privacy, certain encryption mechanisms like access control schemes, auditing mechanisms, anomaly detection, and cryptographic mechanisms (AES, IDEA, RC5, RAS, ECC) are implemented in order to secure the flow of data.[2]

India's market stands in the top 20th position for medical devices worldwide, with a rate at Rs. 77539 crore (US $ 11 billion) in 2020. In the last decade, about 1.5 million medical devices were affected by security breaches due to vulnerabilities. With the rising rate at which the medical industry is shifting towards wireless technology, they are more prone to cyber-attacks in the near future. The major reason for the cyber-attacks is the software present in the medical devices.

These kinds of medical innovations in general present a mixed blessing. On one hand, they have enhanced the quality of healthcare services while on the other hand, these devices collect and exchange personal health data. Healthcare becomes a week and targeted spot for hackers to exploit this huge abundance of data available.[6] Recent studies have demonstrated successful attacks on IMDs that can not only compromise the confidentiality of medical data but may even set off malicious actions in the IMD which can potentially harm a patient and may even be fatal in some cases. In the following sections we discuss the constraints faced by the implantable medical devices, security requirement for a seamless communication, attack vectors, different types of attacks and majorly the protection mechanisms to overcome the security breaches.

2. IMD - CONSTRAINTS

A revolutionary approach for communication between a medical device bearer and programmer is shown by the new age IMDs, but on the other hand, they also have many constraints. These constraints can be broadly classified as communication level and physical level[2]:

2.1 Physical Level Constraints

- Initialization: While placing the IMD for the first time inside the body, maximum care should be taken.
- Size: There is always a tradeoff between efficiency and size. IMDs are rejected by the body due to their large size.
- Battery: IMDs are built using non rechargeable batteries, which limits its life only up to 8-12 years. High processing algorithms drain the battery easily.
- Computation: Real-time high-speed data processing is much necessary in IMDs in order to process information.
- Memory: Small size with large memory capacity is required in order to store past, present and future audit records, especially under Denial of service (DoS) attack, the attacker attacks the memory.

2.2 Communication Level Constraints

- Radiation and power: The communication transmission causes high amounts of power and radiation which could be detrimental to the patient's health.
- Security: Many addressing techniques rely on the fact that an authorized person has a stronger wireless channel when compared to that of an unauthorized person.
- Wireless channel: Many traditional techniques do not work efficiently inside the body due the fading in transmission of signal, due to the low transmission power of devices

3. IMDS SECURITY REQUIREMENTS

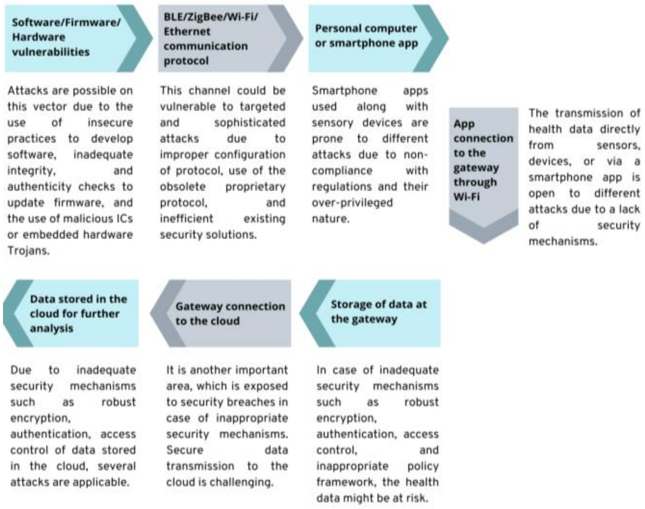
Table 1 describes the security requirements for IMDs, the points considered here are non-repudiation, confidentiality, integrity, authentication, accountability, availability, robustness, freshness, access control and authorization[6],[3].

Table 1: Security Requirements of an IMD

Requirements	Description
Confidentiality	The information which is being transmitted to and from the IMD should be guarded from the illegal users.
Integrity	The information which is being transmitted to and from the IMD and which is processed should be secured and have a strong encryption mechanism, through which data can be preserved by getting corrupted or altered.
Availability	The main aim of introducing an IMD inside the body is to have smooth-running and remote access of a patient to a doctor. The patient and the doctor should be able to perform operations on the IMD, as and when required.
Access control	Unauthorized or illegitimate persons should be denied access by the IMD
Authentication	The device access should be limited by the authorized person, in order to avoid device fidelity and deliberate disturbance. Permission to make adjustments to the IMD is also specified by the doctor.
Authorization	The act of giving permission and access rights to the patient which can depend on the type of IMD and the authorization role.
Accountability	Act of being explained or justifiable. A review log is kept by the IMD regarding previous potential breakdowns.
Freshness	The operations that are performed must be non-redundant and fresh. The attacker can unambiguously send similar operations through the device memory while maintaining adverse DoS attacks and adverse logs.
Robustness	Capability to handle abnormal circumstances and emergency situations.
Non-repudiation	A few of the IMDs in the market have a built-in log system in them. All the operation and functioning details are saved by the IMD in these logs. The adversary can access these log files, and delete them in order to erase their traces. But during this the patient does not get notified.

4. ATTACK VECTORS

With reference to a network model, it can be observed that IMDs are open to security attacks at different levels. Fig. 1 describes the attack vectors in seven different stages[1]:



Software/Firmware/ Hardware vulnerabilities

Attacks are possible on this vector due to the use of insecure practices to develop software, inadequate integrity, and authenticity checks to update firmware, and the use of malicious ICs or embedded hardware Trojans.

BLE/ZigBee/Wi-Fi/ Ethernet communication protocol

This channel could be vulnerable to targeted and sophisticated attacks due to improper configuration of protocol, use of the obsolete proprietary protocol, and inefficient existing security solutions.

Personal computer or smartphone app

Smartphone apps used along with sensory devices are prone to different attacks due to non-compliance with regulations and their over-privileged nature.

App connection to the gateway through Wi-Fi

The transmission of health data directly from sensors, devices, or via a smartphone app is open to different attacks due to a lack of security mechanisms.

Storage of data at the gateway

In case of inadequate security mechanisms such as robust encryption, authentication, access control, and inappropriate policy framework, the health data might be at risk.

Gateway connection to the cloud

It is another important area, which is exposed to security breaches in case of inappropriate security mechanisms. Secure data transmission to the cloud is challenging.

Data stored in the cloud for further analysis

Due to inadequate security mechanisms such as robust encryption, authentication, access control of data stored in the cloud, several attacks are applicable.

Fig. 1. Seven stages of attack vectors in IMDs

5. ATTACKS IN IMDS

Based on the adversary's perspective, attacks are classified as active and passive adversaries[3]. Passive adversaries are those who just listen to the channel of communication without modifying the messages or the data, between the IMD and the authorized personnel. They are just trying to gain information about the presence of IMD and its type, basic information about the device (model, serial number) and the personal details of the patient carrying it. Active adversaries are those who are capable of listening, modifying and sending data/commands between IMD and the authorized personnel. They are also capable of blocking the messages, in order to restrict them from reaching the IMD[7]. They can attack the IMD at any of the seven stages of active vectors discussed in section 1V.

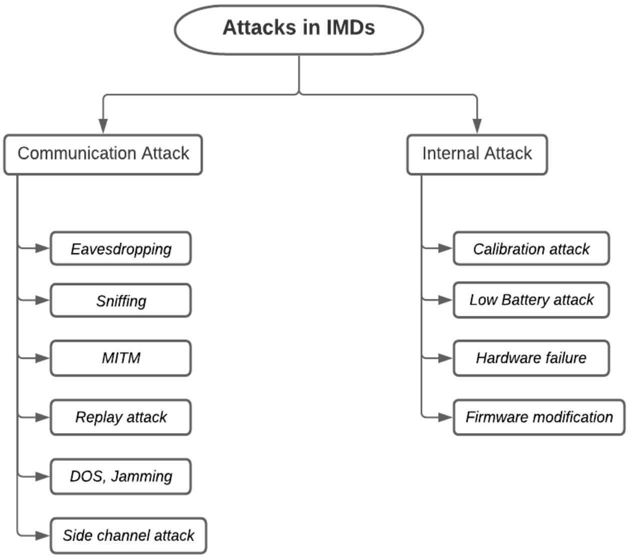


Fig. 2. Flowchart on classification of attacks in IMDs

The attacks on IMDs can be majorly classified into two groups, that is internal attacks and communication attacks. The two types are further classified into many types and are described below[2].

5.1 Internals Attacks

- Calibration attack: The attacker here mainly focuses on altering the collected data and this leads to mis-diagonis of the patient.
- Low Battery attack: This attack can happen when the processor in the IMD utilizes most of the power while transmitting, receiving and processing information. Attackers tend to add high power computing tasks into the device with an intention to drain out the battery of the IMD.
- Firmware modification attack: The attacker/adversary attempts to change the saved program in the memory, which is responsible for the functioning of the hardware. Firmware updation is an essential requirement in the recent IMD technology. Attackers exploit this feature by modifying the program. In case of a diabetic patient, the attacker/adversary can oversupply the quantity of insulin as described in[8].
- Hardware and inter-connection failure: these can be occurred by factors like natural disasters. Third party business partners who are malicious and negligent.

5.2 Communication Attacks

- Eavesdropping: Interception of real time users by attackers or unauthorized entities. This attack becomes an entry point for many other attacks. Reverse engineering communication protocol is exploited by eavesdropping. Due to the lack of encryption mechanisms, the attacker can block the packets.[9]
- Sniffing: In case of IMDs the secret key from the accelerometer or pacemaker can be sniffed from the signal. Software and hardware sniffers are accustomed to analyze the load by making use of MAC addresses.
- MITM: Such an attack occurs when an attacker seizes the transmissions between two authorized entities, and is applicable in every medical device.[10] describes MITM and proxy attacks on insulin pumps by exploiting the encryption techniques through the universal software radio peripheral.
- Replay attack: In this type of attack the adversary obtains a few of the valid packets in order to corrupt the transmission. Authentication, encryption mechanisms are exploited in the IMD by the replay attack[11].
- DOS, Jamming and Resource depletion: Draining the resource rapidly of the device is associated with this. Due to the battery constraint of these miniature devices, their resources can be drained easily by these attacks.
- Side channel attack: This type of attack is done by the adversary in order to gain sensitive information. They analyse the power consumed by electromagnetic (EM) radiation many times in order to get the secured information. After gaining the secret information, they can get absolute access to the device.

6. PROTECTION MECHANISMS

This section describes the different types of protection mechanisms available in order to protect the IMDs. Most of the proposals here give importance to the constraints and attacks discussed in the above sections. The majority are preventive measures, although a few mechanisms also discuss the error correction methods. Classification of the protection mechanisms is described in the Fig. 3

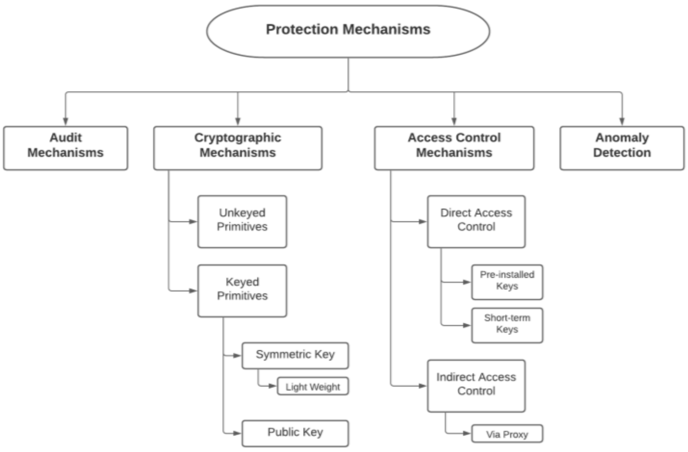


Fig. 3: Flowchart representation of classification of protection mechanisms

6.1 Audit Mechanisms

A simplest security system which collects the patient's status and keeps track of the registered or unregistered users trying to access the IMD's. The logs provide data for patient care and also helps in reconditioning patients treatment if conveyed through IMD. This helps in fighting against the non-repudiation, but doesn't prevent from getting attacked. This can be overcome by carrying out some suitable mechanisms that detect as well as prevent them from happening at top priority. The major difficulty faced in this mechanism is the limited memory accessibility in the IMD. In the case of ICD, the memory is of 1 MB out of it 75% is used for medical functions and the remaining few kilobytes are used for recording incidents. By increasing the memory capacity, the size of IMD increases which is against the requirement. Therefore, a possible solution for this is to move the memory and complex computation part to an external proxy ,which keeps a log of events, without any restrictions for its working. “RFID Guardian” [12] is one such external device which gathers and examines evidence of all the events that occurred in a fixed range. But this becomes problematic when the attacker gets the access of the RFID Guardian. MedMon [13] is a similar one which keeps a check on snooping and all communication occurring with the IMD. Other solutions include superimposing the past non relevant data, raising an alarm to alert the patient or a drastic one which simply blocks the communication channel during attacks[14].

6.2 Cryptographic Mechanisms

The process of securing the data and the communication channel through codes and providing access to those who are intended to access it. In view of IMD, the data in the IMD and the communication between the IMD and the external device or a patient himself or a doctor is to be protected from external attackers and also handle the access to the IMD. Cryptographic solution can be used to provide a confidential communication channel between the IMDs and the authorized personnel. Based on the cryptographic primitives, the cryptography-based security is divided as below[15]:

6.2.1 Unkeyed Primitives: The cryptography algorithm that doesn't use any key such as hash function but provides integrity to the data. It is a one way permutation which means input cannot be predicted from the output obtained.Here, the large data is converted to a fixed length hash value or digest.The common hash functions used in cryptography are Message Digest(MD) and Secure Hash Algorithm(SHA)[16].The communication cost is higher and is insufficient to detect the modification in the data[17].

6.2.2. Keyed Primitives: The cryptography tool that uses keys to secure the data and communication channel.

6.2.3 Symmetric Key Primitives: A common secret key,like symmetric key ciphers or message authentication codes or pseudo random sequence or identification primitives, is shared between two trusted systems. Based on the data bits grouping, symmetric cryptographic is divided into stream cipher and block cipher.The former encrypts individual bits with key and the latter being secure and faster, encrypts a block of bits with the same key[18].This scheme(especially stream cipher found in Media Access Control) works perfectly on resource constrained devices thereby used in most of the present generation IMD but suffer from key distribution which are essential to procure access to the device by authorised personnel and to encrypt transmissions[19].Few techniques involve key updating mechanisms based on hash chain scheme[20]. Based on the IMD type, working environment and the relation between the other entities different keys can be used from different sources. The keys can be pre loaded in the authorised devices which have a lasting relation with the IMD and can later be updated during the first communication session.The keys must be protected, be accessed only by trusted entities and are used to enhance various cryptographic tokens used in negotiation between different entities. The other way is to store the cryptographic keys required by IMD in an exterior smart wearable device such as a smart bracelet.This is a risky process as losing the device makes the IMD inaccessible or provide accessibility to the unauthorised devices or users[21]. The energy efficient and common algorithm used in medical devices is Advanced Encryption Standard(AES)[18] ,a repetitive block cipher procedure which depends on the substitution and permutation network structure.Authors suggest getting an invisible tattoo of the key using ultraviolet pigmentation so that it helps the medical personnel in an emergency thereby providing access to IMD[22].But there is a possibility of the attacker reading this key when he is in physical access to the patient.A innovative cryptography procedure with contended military grade security level that incorporate a one time pad cipher with a innovative key distribution and validation measure. The lightweight cipher can be used in providing hardware efficiency[23].

6.3 Lightweight Cryptography

The algorithm is used in resource constrained devices, like IMD, medical sensors or RFID tags, where the data is grouped either in streams or blocks but having no compromise in the security[24],[25]. The algorithm is chosen in such a way that it is compact, high speed, low power consumption and immediate connection requirement considering the patient's health and life while having no compromise in providing necessary requirements for security[26].Choosing an algorithm that fulfills all the needs is a big problem as the IMDs have limited power, memory constraints and require a faster execution/action towards the inputs/ threats/ emergency and concerning the life of the patient. A faster compact crypto algorithm reduces power losses, memory usage and increases battery life time[27].Table 2 [24]-[33] describe different symmetric lightweight cryptographic algorithms based on the Advanced Encryption Standards(AES) concerning the IMD.

Table 2: Different Symmetric Lightweight Cryptographic Algorithms

Types	Description
Advanced Encryption Standard (AES)	A block cipher with substitution and permutation network structure. A 4*4 matrix representation of 128 bits. Operations applied to cipher text: Substitute bytes, row shifting, columns mixing and add round key. Shifting operation increases the speed of the algorithm.
Camellia	A feistel cipher with similar capabilities as AES. A block cipher of 128-bit data and variable key size which is implemented on software and hardware. Software implementation is faster and recommended. Security based on the fact that no linear or differential attacks exceeding 128-bits is reported successful.
International Data Encryption Algorithm (IDEA)	Software implemented commercial architecture uses block cipher design to replace Data encryption standards(DES) by enlarging the size of the key. Consists of simple arithmetic operations like addition, multiplication and XOR. Doesn't use S box or lookup table
Light Encryption Devices(LED)	Much hardware oriented lightweight block cipher an extension of AES based cipher. Part of master key replacing the round key and having no strong dependence on key scheduling.

Rabbit	Efficient stream cipher firm for software implementation. Revolve around bitwise operation like shifting, XOR and concatenation resulting in faster performance. For every repetition pseudo random bit of size equal to size of the input key is produced.
RC5	A block cipher with variable and self-chosen block size, key size and number of rounds. Depends on operations like XOR, cyclic shift and modular addition. Faster execution obtained from minimum memory. Differential cryptanalysis is ignored assuming it requires a complete codebook to retrieve answers.
Salsa20	Software oriented stream cipher, similar to IDEA and arithmetic operation based on AES. Use of merging expansion operations with hash functions used to constitute key streams.
SIMON	A feistel block cipher ,developed especially for hardware but efficient in software too, with operations like a simple round function of bitwise (AND, OR) and left circular shifts to secure sensitive data.
SPECK	A feistel cipher structure similar to the SIMON and Camellia cryptography is used in SPECK. Both SPECK and SIMON are considered families of multi block ciphers. They contain 10 blocks of different keys. It performs a bitwise operation for every crucial direction, bitwise XOR and modular addition operations.

6.4 Public Key Primitives

Two different keys, public key ciphers and signatures, among them one is public to trusted devices and other one is kept secret. It uses mathematical operations like factorization or discrete logarithm which makes it impossible in computing the keys and advantage being it doesn't require any secure channel for communication[34]. The most commonly used algorithms are Rivest-Shamir-Adleman(RAS) and Elliptic Curve Cryptography(ECC)[28]. The former depends on the result of two random prime numbers used to build its security on complexity of factorization and the latter being the most efficient technique than the former depends on discrete logarithm found from an elliptic curve element. But both the techniques work slowly and against the requirement in IMD and for faster computation it requires higher RAM. The complex circuit and high message exchanging during communication leads to higher power and resource consumption thereby reducing the reliability[35]-[40].The solution to overcome this complication is to use an external proxy device which handles heavy computation for public key cryptographic tool prior to gaining the access of IMD. Damage or misplacement of the external devices makes the IMD in accessible.

6.5 Access Control Mechanisms

Depending on the architecture, key type, channel and logic control, the classifications is shown in the below Fig. 4

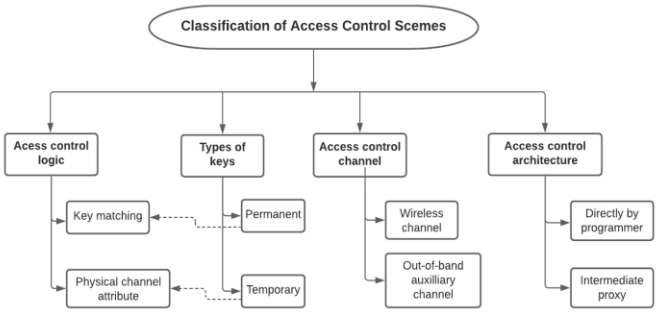


Fig. 4.Flowchart on classification of access control schemes

6.5.1 Direct Access Control - Pre installed Keys: One of the measures proposed in [41] concludes a common master key(nonrealistic) K_M for all commercial programmers.The IMD I with a unique specific key K computed as cryptographic function(K_M , I) is accessed by the programmer on the demand of its name I and a nonce N and returns R = RC5(K, N) and verify the response it received from the authorized personnel. In rolling code based authentication measures,entry is granted only if the difference between the sequence numbers encoded by an encryption key of the insulin pump and the authorised personnel is within a certain range[42]. The concept of adding an additional triggering circuit, designed using the passive RFID technology that harvests energy from the incoming signal to perform a lightweight validation of the wake-up authentication code,before the master circuit of the IMD was proposed by Liu et al. [43] . Only on the validation of wake-up code,the mater circuit will be woken up, thereby preventing resource depletion attack.In this case key is pre installed else the key is obtained just prior to accessing by using the patients physical characteristics(like height, iris, fingerprints) or an item possessed by him.Patient's biometric data were pre loaded in IMD by HEi et al.[44] which includes two level verification.The first verifies the type of biometric features and the second verifies more precisely using iris data. However, the cancellation process of the key is too hard to implement based on the count of medical units to be notified. The IMD is exposed to baleful attacks if the personnel is hacked or stolen by an adversary and this can be overcomed by using a temporary key.

6.5.2 Direct Access Control - Short term Keys: The IMD and the programmers are required to take out certain attributes from the common source simultaneously and produce the temporary keys based on these similar attributes, while the other category requires only one device to create the key and distribute it to the other device. The authenticity of the temporary key based access control depends on the security of the cryptographic key generation using numerous proximity based methods and distribution procedures.

- Biometric: The physical characteristics of humans like iris, fingerprint which can be used to identify oneself. Use the pseudo-random number extracted from the biometric peculiarities for the encoding and decoding of the temporary key during communication[45]. Hu et al. proposed the ordered-physiological-feature-based key agreement (OPFKA) [46] leverages the fact that the generated features are ordered and known only to the corresponding sensor itself, and employs simple noisy data as scrap points to provide escalated security. The use of physiological parameters like the electrocardiogram (EKG or ECG) to secure the transmission in body area networks (BANs) and to generate temporary key[47]. ECG based key with cryptography protocol guarantees access control in IMD.

The communication between the reader and the IMD is controlled by the IMD Guard which is similar to that of the RFIC Guardian and whose absences make the IMD accessible easily[48]. ECG signal has two prime advantages, first; a reasonably high level of randomness that the attackers cannot predict[49] and Second; ECG signal is measured in high precision only if the device is in physical correspondence with the patient[50],[51].The biometric techniques can be applied easily than the protocols based on shared key and prevent disclosure of key to the attacker. But this approach has drawbacks like the physical presence of the person which couldn't be possible in emergency situations and other being the perfectness in the biometric features obtained. The error in the features gathered must be within an acceptable range and be able to be corrected[52]-[54].

- Distance Based: In this the person within a particular range of communication is assumed to be a reader rather than adversary who holds the required credentials for accessing or a legitimate reader without credentials in emergency situations[48].A distance-bounding protocol based on ultrasonic sound waves. The protocol permits the IMD to compute the distance between programmer and IMD since an adversary at a large distance will not be able to propagate faster than the rate of ultrasonic sound, regardless of the category of transceiver or antenna being used. An accuracy of 97-100% is obtained for an attack initiated from a distance of 5 - 6 feet[55].Some other technique which utilizes the near field communication (NFC) to execute device pairing, which makes way for key exchange between an IMD and the programmer in short communication scope (less than 6cm). A round trip time is measured to get rid of relay attacks. The major drawbacks, firstly being presence of adversary within the fixed range or the patient himself and secondly, by fooling the IMD about the location of adversary within the permitted range when he is far apart from the range.[56],[57]
- Body-coupled communication: The communication range is limited very close to proximity of the human body, which increases the difficulty for the adversary to intrude the communication[42]. Power consumption is low as the signals are sent only for a limited range besides through free space. IMD implanted with a magnetic sensor which turns on only after detecting the magnetic field generated by the near programmer and then the key for communication is shared by the IMD for that session. Unfortunately, it is doubtful about safety while using magnetic fields[58].
- Vibration based transmission channel comprises virtually short-range, requiring uninterrupted physical contact, and extremely user-perceptible. An audio channel based key exchange method, in which the IMD creates a random value to be used as a session key and transmits it as a modulated sound wave[41].

6.5.3 Indirect Access Control using a Proxy: A wearable device or a smartphone which has more capability and the ability to perform calculations than the IMD acts as a proxy. The IMD and the proxy communicate through a protected, lightweight symmetric encryption that can be regarded as safe and the proxy device handles the access control. Proxy device usage increases the vulnerability surface as well.

- Jamming based Scheme: proper use of radio interferences or signals can help in protecting the confidentiality of the sensitive communications of the IMDs. Cloaker, an external device proposed by Denning et al. [59], whose presence in the vicinity, the IMD simply ignores other incoming signals. Proxy can be preloaded with the asymmetric keys on approval of external personnel. After successful validation, communication takes place through the proxy for maintaining the log for later forensic and analysis purpose. During emergency the proxy is placed out of communication range thereby providing open access to IMD under patient's notice. IMD Guard which contacts the exterior wearable device Guardian was proposed in [60]. On the existence of the Guardian, the IMD Guard stops periodic broadcasting of messages and is resistant to spoofing attacks by sending two portions of challenges divided by a constant time T. Based on the first portion messages the IMD interprets that it is spoofed and enter into emergency mode. Gollakota et al. [61] proposed a unique full duplex radio architecture with two antennas(one as receiver and other as jammer) focusing on the confidentiality of the IMDs' communication without any mitigation to the IMDs. Continuous monitoring of IMD's signals by antennas and jams its messages. The jamming scheme had a drawback which was demonstrated experimentally and analytically by Tippenhauer et al. [66] using a MIMO based attack that recovers the communication protected by jamming.
- Gateway based scheme: Body Double, a keyless based scheme, proposed by Zheng et al. [62] used in IMDs in emergency situations. The adversary is spoofed to communicate with the gate ,pretending to be wireless and is embedded with a exterior authentication proxy, rather than IMD. The gateway jams the request on failure of authentication and turning off or removing the gateway makes the IMD completely accessible at emergency situations.
- Mobile device-based Scheme: Use of built-in sensors in the proxy mobile device for assisting in the temporary key generation/distribution. Temporary key generation majorly based on the persons walking characteristics filtered by the obtained accelerometer signals was designed in Walkie-Talkie proposed by Xu et al[63]. Zhang et al. propose SBVLC [64] ,a key recovery technique where the authorized personnel present a barcode which contains the temporary key to the proxy which is obtained by scanning and decoding the barcode by a proxy and vice versa. Li et al. [65] proposed the use of a Visible Light Communication (VLC) where the key is encoded and transferred through a light sensor present in the proxy as a beam of rays with controlled intensity in the visible region thereby providing security and access to the authorized user in the vicinity and also helpful in emergencies as there is no requirement of human presence.

6.6 Anomaly Detection

A peculiar type of memory-based mechanism that tries to spontaneously detect resource depletion or unofficial access based on the periodic patterns, such as physiological modifications or access patterns like time, place or command and notify the patient about it or make the device inaccessible by turning off the communication, without disturbing the medical functionality. The adversary tries to communicate with IMD and it fails in authentication stage repeatedly and thereby draining the battery and memory, which is the excellent example for Denial of Service(DoS) and Resource Depletion(RD). Based on the constraints restricted in the IMD, the combination of pattern analysis and notification system can be used as the best possible solution within IMD. After being implemented by temporal and location correlation, it fails in achieving 100% precision as it is impossible to differentiate attacks that may occur in a normal pattern.

Support Vector Machine based classifier, proposed by Hei et al [67] which provides 90% of average detection rate against RD, used to classify normal and abnormal events in the patient's phone based on the previously trained data and deactivate classification during emergency situations(like a heart attack) while the IMD personnel still having the access to it. The IMD is accessed on the outcomes of the classification and patient's decision. Yet this poses certain drawbacks like not considering the emergency conditions which could harmful to the patient's life, use of a external device(patient's phone) and patient's responsibility when the SVM fails to classify. Based on the deviation of received signal properties ,like its strength, time of arrival, angle of arrival and others, from those expected(as recorded previously) through a wireless communication Zhang et al.[13] proposed an external security device which detects the abnormalities and alerts the patient or blocks the transmission from detecting the IMD. Use of supervised learning, to understand infusion patterns in normal patients with intake quantity, rate and time of infusion, to generate a progressive model and dynamically determine a safest range of infusion for abnormal infusion detected was presented by Hei et al.[68],[69]. MedMon, a medical safety detector, that records all the communication of the IMD and then passes it to multilayer anomaly detection system for analysis. Necessary actions, like notifying the patient(passive response),jamming the communication channel(active response) , are taken based on the detection[13].The drawback being the entire security is occupied on an exterior device but with a benefit that it can be implemented on a existing device without any tempering. In continuation to MedMon, use of exterior devices consisting of a few antennas that set up a database of authorized personnel based on their location which are determined through triangulation techniques, was proposed by Darji and Trivedi[70]. This proves effective in immobile scenarios but fails in mobile scenarios.

7. CONCLUSION

Implantable Medical Devices are playing a major role in the current healthcare industry in automating the complete treatment procedure and keeping the patient health conditions monitored. The recent IMDs have networking and communication capabilities integrated within them. These create a loophole for attackers to attack the device. There always exists a tradeoff between size ,battery life, computational power and memory. Based on the requirements of the particular IMD, these tradeoffs can be taken care of. We have discussed the different types of attacks, attackers and the stages at which the attack can take place. Based on the previous research, we have presented the different types of protection techniques, encryption mechanisms and their shortcomings in different scenarios. There is still an open door for emerging technologies

8. REFERENCES

[1] T. Yaqoob, H. Abbas and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3723-3768, Fourthquarter 2019, doi: 10.1109/COMST.2019.2914094.

[2] H. Rathore, A. Mohamed, A. Al-Ali, X. Du and M. Guizani, "A review of security challenges, attacks and resolutions for wireless medical devices," 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), 2017, pp. 1495-1501, doi: 10.1109/IWCMC.2017.7986505.

[3] Carmen Camara, Pedro Peris-Lopez and Juan E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey", in Journal of Biomedical Informatics, Volume 55, 2015, Pages 272-289, ISSN 1532-0464, doi: 10.1016/j.jbi.2015.04.007.

[4] L. Wu, X. Du, M. Guizani and A. Mohamed, "Access Control Schemes for Implantable Medical Devices: A Survey," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1272-1283, Oct. 2017, doi: 10.1109/JIOT.2017.2708042.

[5] Alassaf, Norah & Alkazemi, Basem & Gutub, Adnan. (2017). Applicable Light-Weight Cryptography to Secure Medical Data in IoT Systems. Journal of Research in Engineering and Applied Sciences (JREAS). 2. 50-58. 10.46565/jreas.2017.v02i02.002.

[6] Rathore, H., 2016. "Mapping biological systems to network systems". Springer

[7] D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S.S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, W.H. Maisel, Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses, in: Proc. of the 29th Annual IEEE Symposium on Security and Privacy, 2008, pp. 129–142.

[8] X. Hei, X. Du, S. Lin, I. Lee and O. Sokolsky, "Patient Infusion Pattern based Access Control Schemes for Wireless Insulin Pump System," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 11, pp. 3108-3121, 1 Nov. 2015, doi:10.1109/TPDS.2014.2370045.

[9] Venkatasubramanian, K.K., Gupta, S.K.S., Jetley, R.P. and Jones, P.L. "Interoperable medical devices". IEEE Pulse, 1(2), pp.16-27, 2010.

[10] N. Ellouze, M. Allouche, H. B. Ahmed, S. Rekhis, and N. Boudriga, "Security of implantable medical devices: Limits, requirements, and proposals," Security Commun. Netw., vol. 7, no. 12, pp. 2475–2491, Nov. 2013.

[11] Hosseini-Khayat, S., "A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices". In Medical Information and Communication Technology (ISMICT), 2011 5th International Symposium on (pp. 6-9). IEEE, 2011

[12] M.R. Rieback, B. Crispo, A.S. Tanenbaum, RFID guardian: a battery-powered mobile device for RFID privacy management, in: Information Security and Privacy, Lecture Notes in Computer Science, vol. 3574, Springer, Berlin Heidelberg, 2005, pp. 184–194.

[13] Zhang, Meng et al. "MedMon: Securing Medical Devices Through Wireless Monitoring and Anomaly Detection." IEEE Transactions on Biomedical Circuits and Systems 7 (2013): 871-881.

[14] Gupta, S. "Implantable medical devices-cyber risks and mitigation approaches". In Proceedings of the Cybersecurity in Cyber-Physical Workshop, The National Institute of Standards and Technology (NIST), US, 2012.

[15] A.J. Menezes, S.A. Vanstone, P.C.V. Oorschot, Handbook of Applied Cryptography, first ed., CRC Press, Inc., 1996

[16] L. Yehia, A Khedr, A. Darwish, Hybrid Security Techniques for Internet of Things Healthcare Applications. Advances in Internet of Things, 5(03), 2015.

[17] A. Trad, A. Bahattab, S. Othman, Performance trade-offs of encryption algorithms for Wireless Sensor Networks. IEEE World Congress on Computer Applications and Information Systems (WCCAIS), pp. 1-6, January 2014.

[18] L. Gupta, R. Jain, Security in low energy body area networks for healthcare, online, available at: http://www.cse.wustl.edu/ ~jain/cse 571-14/ftp/ban/index.html ; 2014.

[19] K. Chaudhari, M. Borole, A Survey on Various Cryptographic Algorithms for Security Enhancement.

International Journal of Computer Applications, 110(7), January 2015

[20] D. He, S. Chan, S. Tang, A novel and lightweight system to secure wireless medical sensor networks, IEEE J. Biomed. Health Infor. 18 (1) (2014) 316–326.

[21] E. Freudenthal, R. Spring, L. Estevez, Practical techniques for limiting disclosure of RF-equipped medical devices, in: IEEE Engineering in Medicine and Biology Workshop, 2007, pp. 82–85

[22] S. Schechter, Security that is Meant to be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices, 2004

[23] S. Hosseini-Khayat, A lightweight security protocol for ultra-low power ASIC implementation for wireless implantable medical devices, in: 5th International Symposium on Medical Information Communication Technology (ISMICT), March 2011, pp. 6–9.

[24] D. Dinu, Y. Le Corre, D. Khovratovich, L. Perrin, J. Großschädl, A. Biryukov, Triathlon of Lightweight Block Ciphers for the Internet of Things. IACR Cryptology ePrint Archive, 209, 2015.

[25] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, L. Uhsadel, A survey of lightweight-cryptography implementations. IEEE Design & Test of Computers, 24(6), pp. 522-533, 2007.

[26] T. Guneysu, Lightweight Cryptography for Securityand Privacy, Springer, 2016.

[27] C. Manifavas, G. Hatzivasilis, K. Fysarakis, K.Rantos, Lightweight cryptography for embedded systems - a comparative analysis, Data Privacy Management and Autonomous Spontaneous Security, Springer Berlin Heidelberg, pp. 333-349, 2014

[28] A. Gutub and F. Khan, Hybrid Crypto Hardware Utilizing Symmetric-Key & Public-Key Cryptosystems, International Conference on Advanced Computer Science Applications and Technologies (ACSAT), Palace of the Golden Horses, Kuala Lumpur, Malaysia, November 2012.

[29] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S.Moriai, J. Nakajima, T. Tokita, Camellia: A 128-bit block cipher suitable for multiple platforms - design andanalysis, International Workshop on Selected Areas in Cryptography, pp. 39-56, 2000.

[30] G. Meiser, T. Eisenbarth, K. Lemke-Rust, C. Paar, Efficient implementation of eSTREAM ciphers on 8-bit AVR microcontrollers, IEEE International Symposium on Industrial Embedded Systems, pp. 55-66, June 2008.

[31] J. Guo, T. Peyrin, A. Poschmann, M. Robshaw, 2011, The LED block cipher, International Workshop on Cryptographic Hardware an Embedded Systems,Springer Berlin Heidelberg, pp. 326-341, September 2011.

[32] M. Boesgaard, M. Vesterager, T. Christensen, E. Zenner, The stream cipher rabbit. ECRYPT Stream Cipher Project Report, 6, 2005.

[33] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, SIMON and SPECK: Block Ciphers for the Internet of Things, IACR Cryptology ePrint Archive, 2015.

[34] A. Gutub, High Speed Low Power GF(2k) Elliptic Curve Cryptography Processor Architecture, IEEE 10th Annual Technical Exchange Meeting, KFUPM, Dhahran, Saudi Arabia, March 2003.

[35] S. Rehman, M. Bilal, B. Ahmad, K Yahya, A. Ullah, O. Rehman, Comparison based analysis of different cryptographic and encryption techniques using message authentication code (mac) in wireless sensor networks (wsn). arXiv preprint arXiv:1203.3103, 2012.

[36] A. Gutub, Merging GF(p) Elliptic Curve Point Adding and Doubling on Pipelined VLSI Cryptographic ASIC Architecture, International Journal of Computer Science and Network Security (IJCSNS), 6(3A) , pp. 44 – 52, March 2006.

[37] M.H. Eldefrawy, M.K. Khan, K. Alghathbar, A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography, in: 2010 International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID), 2010, pp. 1–6.

[38] F. Furbass, J. Wolkerstorfer, ECC processor with low die size for RFID applications, in: IEEE International Symposium on Circuits and Systems, 2007, pp. 1835–1838.

[39] Y.K. Lee, K. Sakiyama, L. Batina, I. Verbauwhede, Elliptic-curve-based security processor for RFID, IEEE Trans. Comput. 57 (11) (2008) 1514–1527.

[40] K. Singh, V. Muthukkumarasamy, Authenticated key establishment protocols for a home health care system, in: 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, 2007, pp. 353–358.

[41] D. Halperin et al., "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in Proc. IEEE S P, Oakland, CA, USA, 2008, pp. 129–142.

[42] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in Proc. IEEE HealthCom, Columbia, MO, USA, 2011, pp. 150–156.

[43] J.-W. Liu, M. A. Ameen, and K.-S. Kwak, "Secure wake-up scheme for WBANs," IEICE Trans. Commun., vol. 93-B, no. 4, pp. 854–857, 2010.

[44] X. Hei and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," in Proc. IEEE INFOCOM, Shanghai, China, 2011, pp. 346–350.

[45] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in Proc. ICPP Workshops, Kaohsiung, Taiwan, 2003, pp. 432–439.

[46] C. Hu et al., "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in Proc. IEEE INFOCOM, Turin, Italy, 2013, pp. 2274–2282.

[47] F. Xu, Z. Qin, C.C. Tan, B. Wang, Q. Li, IMDGuard: securing implantable medical devices with the external wearable guardian, in: Proceedings IEEE INFOCOM, 2011, pp. 1862–1870.

[48] M.R. Rieback, B. Crispo, A.S. Tanenbaum, RFID guardian: a battery-powered mobile device for RFID privacy management, in: Information Security and Privacy, Lecture Notes in Computer Science, vol. 3574, Springer, Berlin Heidelberg, 2005, pp. 184–194.

[49] S.-Y. Chang, Y.-C. Hu, H. Anderson, T. Fu, and E. Y. L. Huang, "Body area network security: Robust key establishment using human body channel," in Proc. USENIX HealthSec, 2012, p. 5.

[50] M.-Z. Poh, D. J. McDuff, and R. W. Picard, "Non-contact, automated cardiac pulse measurements using video imaging and blind source separation," Opt. Exp., vol. 18, no. 10, pp. 10762–10774, 2010.

[51] F. Zhao, M. Li, Y. Qian, and J. Z. Tsien, “Remote measurements of heart and respiration rates for telemedicine,” PLoS ONE, vol. 8, no. 10, 2013, Art. no. e71384.

[52] S.-D. Bao, C.C.Y. Poon, Z. Yuan-Ting, L.-F. Shen, Using the timing information of heartbeats as an entity identifier to secure the body sensor network, IEEE Trans. Inform. Technol. Biomed. 12 (6) (2008) 772–779.

[53] S. Cherukuri, K.K. Venkatasubramanian, S.K.S. Gupta, BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body, in: Proc. of International Conference on Parallel Processing Workshops, 2003, pp. 432–439.

[54] K. Cho, D. Lee, Biometric based secure communications without pre-deployed key for biosensor implanted in body sensor networks, in: Information Security Applications, Lecture Notes in Computer Science, vol. 7115, Springer, Berlin Heidelberg, 2012, pp. 203–218

[55] T. Halevi and N. Saxena, “On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping,” in Proc. ACM CCS, Chicago, IL, USA, 2010, pp. 97–108.

[56] X. Hei, X. Du, and S. Lin, “Poster: Near field communication based access control for wireless medical devices,” in Proc. ACM MobiHoc, Philadelphia, PA, USA, 2014, pp. 423–424.

[57] B. Kim, J. Yu, and H. Kim, “In-vivo NFC: Remote monitoring of implanted medical devices with improved privacy,” in Proc. ACM SenSys, Toronto, ON, Canada, 2012, pp. 327–328

[58] S. Lee, K. Fu, T. Kohno, B. Ransford, W.H. Maisel, Clinically significant magnetic interference of implanted cardiac devices by portable headphones, Heart Rhythm 6 (10) (2009) 1432–1436.

[59] T. Denning, K. Fu, and T. Kohno, “Absence makes the heart grow fonder: New directions for implantable medical device security,” in Proc. USENIX HotSec, San Jose, CA, USA, 2008, Art. no. 5.

[60] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, “IMDGuard: Securing implantable medical devices with the external wearable guardian,” in Proc. IEEE INFOCOM, 2011, Shanghai, China, pp. 1862–1870.

[61] 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. ACM SIGCOMM, Toronto, ON, Canada, 2011, pp. 2–13.

[62] G. Zheng, G. Fang, M. A. Orgun, and R. Shankaran, “A non-key based security scheme supporting emergency treatment of wireless implants,” in Proc. IEEE ICC, Sydney, NSW, Australia, 2014, pp. 647–652.

[63] W. Xu, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, “Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication,” in Proc. ACM/IEEE IPSN, Vienna, Austria, 2016, pp. 1–12

[64] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, “SBVLC: Secure barcode-based visible light communication for smartphones,” in Proc. IEEE INFOCOM, Toronto, ON, Canada, 2014, pp. 2661–2669

[65] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, “Secure ad hoc trust initialization and key management in wireless body area networks,” ACM Trans. Sensor Netw., vol. 9, no. 2, 2013, Art. no. 18

[66] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, “On limitations of friendly jamming for confidentiality,” in Proc. IEEE S&P, Berkeley, CA, USA, 2013, pp. 160–173

[67] X. Hei, X. Du, J. Wu, and F. Hu, “Defending resource depletion attacks on implantable medical devices,” in Proc. IEEE GLOBECOM, Miami, FL, USA, 2010, pp. 1–5

[68] Kessel DO, Berridge DC, Robertson I. Infusion techniques for peripheral arterial thrombolysis. Cochrane Database Syst Rev. 2004;(1):CD000985. doi: 10.1002/14651858.CD000985.pub2. PMID: 14973961.

[69] Matan Kintzlinger, Nir Nissim, Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems, Journal of Biomedical Informatics, Volume 95, 2019, 103233, ISSN 1532-0464, https://doi.org/10.1016/j.jbi.2019.103233.

[70] M. Darji, B. Trivedi, Detection of active attacks on wireless IMDs using proxy device and localization information, in: Security in Computing and Communications, Communications in Computer and Information Science, vol. 467, Springer, Berlin Heidelberg, 2014, pp. 353–362.