CHAPTER – 3

Literature Survey

In this chapter, we present a complete taxonomy and comparison of various communication security schemes proposed in literature on the basis of following security and design dimensions:

1.1. Security Dimensions

1. Key Management Provision: Whether the given scheme involves generation, distribution, and (periodic) replacement of keys used for securing the telemetry message to and fro the IMD.
2. Authentication Provision: Whether the given scheme verifies the identity of communicating devices and also that a message originates from the verifiable authenticated entity.
3. Message Integrity Provision: Whether the given scheme confirms that a message has been received correctly without unauthorized modification.
4. Confidentiality Provision: Whether the given scheme prevents disclosure of telemetry message to unauthorized entities.
5. Availability Provision: Whether the given scheme protects the IMD to ensure its availability and accessibility by authorized entities.
6. Access Control Provision: Whether the given scheme has the ability to limit and control the access to IMD and its application via a wireless communication link.
7. Non-repudiation: Whether the given scheme prevents communicating entity from denying transmission of a message or command.
8. Replay Attack Resilience: Whether the given scheme ensures message freshness to avoid a replay of stale packets.
9. Privacy Provision: Whether the given scheme satisfy privacy goals like IMD existence privacy; IMD type privacy; Specific IMD-Identification privacy; Measurement and log privacy; Bearer privacy and Tracking Privacy as explained in [16].

3.2 Design Dimensions

1. Protection Type: Whether the given scheme provides Detection of the attacks or Prevention from security attacks or both.
2. Target Device: Whether the given Scheme is applicable to all IMDs or to a specific type of IMD.
3. Invasiveness: Does the scheme require any modification in existing IMDs? If yes, is it a software modification (S/W) or a hardware modification (H/W) or both (BOTH).
4. Core Mechanism: What is the core mechanism on which this scheme is based on?
5. Access Pattern: Does the scheme secure communication during regular access (RA) or emergency access (EA) or in both the cases (BOTH)?
6. Energy Source: From where is the power required to do security related processing derived?
7. Flexibility: Does the scheme provide flexibility to change encryption algorithm and cipher if their security is compromised or a better one is available?
8. Applicability: Is the scheme applicable for IMD and external device communication (IMD↔ED) or for IMD to IMD communication (IMD↔IMD) or both for (BOTH).

3.3 Taxonomy of Security Models proposed in Literature

As these devices are evolving, the communication security schemes pertaining to them are also emerging. We discuss the communication security schemes provided in literature. Table 1 provides a complete summary of the classification scheme designed by us.

3.3.1 Inhibiting Long Range Communication

Inhibiting Long-Range Communication is a simple way of limiting access to IMD without making use of any security services and mechanisms. Even though it puts zero expense on IMDs resources, it is only effective against radio attacks launched from a certain distance. Problem remains if an attacker can pose an attack within a small distance from patient or make a physical contact. As in reality close-range communication schemes cannot defend against security and privacy attacks, we will not consider this category in our comparison oracle. Still they are worth a mention as they can be used in conjunction with security mechanisms. The proposed schemes are as under:

3.3.1.1 Use of small-range communication channel

Here, a wireless communication channel with limited range is chosen. The popular options are:

1. Radio frequency identification (RFID) based channel : RFID based channel between medical devices and external device is proposed in [56, 57]
2. Near Field Communication (NFC) : To improve privacy, Near Field Communication (NFC) with 3G smart phones is proposed in [58]. According to [59], NFC protocols currently do not provide an appropriate privacy properties for implanted medical applications.
3. Body Coupled Communication (BCC): Body Coupled Communication (BCC) which uses the human body as the transmission medium is proposed in [28]. BCC achieves very low data rates and the external device needs to be in vicinity of human skin.
4. Inductive coupled communication: Inductive coupled communication is used in [17]. Inductive coupled communication is not secure as presence of an eavesdropper may hamper communication by detuning the data transfer [60]. Moreover, an attacker with strong enough transmitters and a high-gain antenna can eavesdrop on the wireless channel even from up to ten meters away [61],[62].

3.3.1.2.Enforcing Proximity

These schemes allow external device to access IMD only if it is in close proximity.

1. **Ultrasonic distance-bounding**: An access control scheme based on ultrasonic distance-bounding is proposed in [29]. In this scheme, IMD grants access to only those devices that are close enough. IMD can operate in two different modes, in normal mode remote monitoring can be performed if reader is in possession of a shared key. During an emergency or for device reconfiguration, reader just needs to be within certain security range. Secret key is shared by Diffie-Hellman key exchange. Ultrasonic distance bounding requires RF shielding, moreover it is vulnerable to RF wormhole and distance-hijacking attacks as mentioned in [63]. This scheme also suffers from drawbacks like authentication using pre-shared keys which cannot be renewed, battery depletion attack by performing continuous authentication attempts and need for hardware modification in IMD.

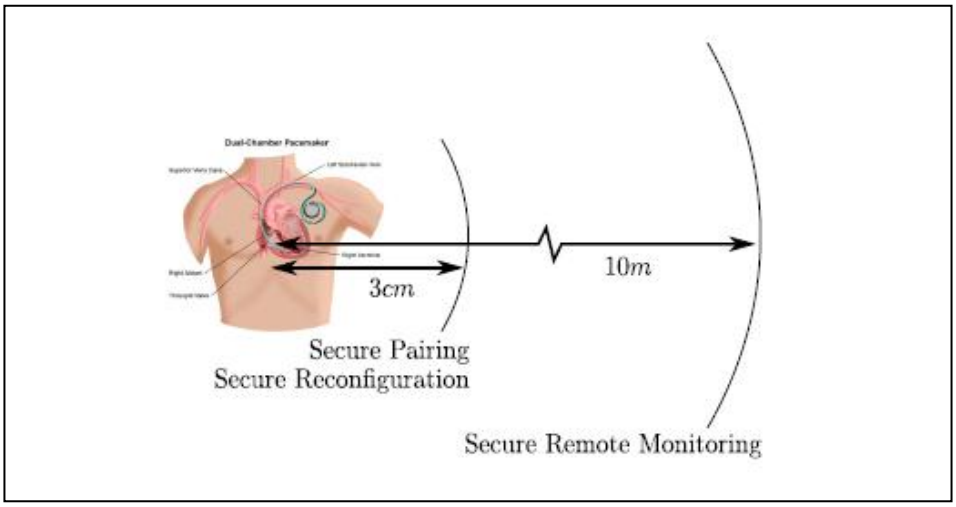

FIGURE 3.1Allowing reconfiguration from smaller distance and remote monitoring from longer distance [29]

2. **Location based service (LBS):** In order to prevent replay attacks, collusion attacks, and distance spoofing attacks, another scheme [64] is proposed based on the use of multiple location based service (LBS) devices by utilizing Bluetooth. Access is granted if the reader is located within a trusted area. The medical personnel's reader sends a broadcast message to nearby LBS devices which sends their partial key and signature to the medical personnel's reader. These keys are used by the reader to access nearby patient's medical data. Installation of LBS devices is a costly affair and key exchange between LBS devices and IMD is not explained. This scheme gives rise to a new vulnerability if one or more LBS devices are compromised.

3.3.2 Using Cryptography

As closed range schemes were incapable of addressing most of the challenges, as a matter of fact cryptography appeared as the most eligible approach. Cryptography can be classified as symmetric and asymmetric. Symmetric ciphers on one hand are considered to have lower computational complexity, power and energy requirements compared to asymmetric ones but on the other hand require each communicating party to access a unique key for maintaining communication confidentiality. Asymmetric systems feature simpler key management by investing more resources. Moreover use of cryptography prevents medical staff from accessing the patient's health data in case of an emergency if they do not have

credentials. Hence encryption scheme should be chosen considering the nature of the data, required security level and device constraints. As cryptography is a mere building block and needs to be complimented with a secure communication protocol, therefore we will not consider this category in our comparison oracle.

3.3.2.1 Using Symmetric Cryptography

In [28] Rolling Code Cryptography is proposed for encryption of telemetry data between IMD and external device. Authors in [65] propose a lightweight security protocol for ultra-low power ASIC Implementation to provide authentication, confidentiality and integrity that gives low-energy computation. But the secret key shared between IMD and base station is hard coded and cannot be renewed if compromised. Also it does not guarantee availability and is prone to DOS (Denial of Service) attacks. Hardware implementations of Hummingbird which is a combination of block and stream cipher is proposed in [66] and [67]. In [68] block cipher based security protocol based on Advanced Encryption Standard (AES) algorithm. The protocol works in stream mode for basic security and in session mode for strong security and uses role-based user authorization scheme. In [69] symmetric block ciphers are evaluated for average and peak power consumption, total energy budget, encryption rate and efficiency, program-code size and security level. According to them MISTY1[70] is superior as far as power consumption factor is considered.

3.3.2.2 Using Asymmetric Cryptography

Certificate-based approaches [59] require the IMD reader to be able to access the Internet for certificate verification, and presence of a global certifying authority (CA) is needed to maintain public key certificates. A reader may not always have online access, also it is costly to maintain and track Global Certification Authority for every IMD and such support may not be available all the time. The authors of [71] suggest use of elliptic-curve cryptography (ECC) algorithm to set up symmetric keys between sensor nodes and the base station. However, it is computation-inefficient and vulnerable to DoS attacks and thus unsuitable for IMDs.

3.3.3 Key Distribution and Management

Symmetric key cryptography is favorable in all aspects as explained above but the challenge it poses is of secret key exchange, management and renewal. Therefore literature of work in this area for Implantable Medical Devices is also worth a mention. To address the challenge of key distribution, initially a universal key was proposed to be preloaded in devices of the same model known to manufacturer and patient's doctor. It is it easy for an attacker to discover the secret key of a particular model as they devices can be bought online also. Therefore, secret keys specific to a patient's device were proposed. Such schemes are discussed below.

3.3.3.1 Putting Patient in the Loop

In [72], medical staff is allowed to access an IMD using an access token which can be a USB stick or bracelet configured with secret key, for secure data download and programming. These access tokens need to be protected from theft, if lost or stolen or forgotten, it creates a safety problem by rendering the IMD inaccessible. Moreover, keys in IMD are not reconfigurable once leaked. Authors in [73] propose password to be tattooed as ultraviolet-ink micro pigmentation which is invisible under normal light. Devices that interact with IMD must be equipped with reading mechanism to interpret the tattoo and an input mechanism for key entry. This technique itself mentions the risk of infection for patients from micro pigmentation and the risk that a tattoo could be rendered unreadable when needed. Moreover keys cannot be reconfigured in IMD one disclosed. As these solutions are naïve, therefore we will not consider this category in our comparison oracle.

3.3.3.2 Use of Patient Biometrics

In [74] author demonstrates possibility of using biometrics, specifically the inter-pulse interval (IPI), as a shared secret to securely share encryption keys among sensor nodes on the same body. In [75] author proposed use of Biometrics derived from patient body to secure the keying material for a network of implanted biosensors. Fuzzy commitment scheme with error correcting codes was used for error correction in different biometric readings taken independently. In [76] authors propose an algorithm for Physiological Value-based key-agreement, called OPFKA, that can also reduce the storage costs associated with fuzzy vaults. Emergency Access is provided in [77] by utilizing a patient's biometric information (iris recognition) to perform authentication. These schemes based on

biometrics lacks a rigorous security analysis as shown in [53] and also lacks possibility of utilization for a wide range of IMDs. The reader/programmer device needs to be brought sufficiently closer to the patient for biometric exchange to take place which is not a feasible solution for remote monitoring.

3.3.3.3 Use of Physical Layer Approaches

1. **Telemetry Data obfuscation:** In [78] instead of using cryptography, author uses a low cost multilevel key-based scrambling algorithm. It is stated that biological signals are bursty in nature and can be obfuscated to provide security. Two levels of encoding are performed. First part of key is used to determine the order of scrambling and second key is used change the order for each packet. By storing only the required permutations for a key, hardware overhead is minimized. This scheme requires strenuous security analysis.
2. **Physical Layer Approach:** Authors in[79] use Reciprocal Carrier-Phase Quantization for refreshing symmetric encryption keys in IMDs. They claim reciprocal quantization of the phase between local oscillators can be used without consuming IMD resources for key exchange. This can be further coupled with symmetric encryption for secure communication.

3.3.4 Using Trusted External Device

On one side when encryption and key exchange schemes were proposed, IMD resource constraint was still posing a challenge. To preserve IMD's resources (battery power), authentication of incoming requests was proposed to be offloaded to a trusted external device, which, unlike IMDs, can be easily recharged. This approach had potentials to even protect the IMD against battery-draining attacks. Therefore different schemes based on this avenue were proposed which can be classified as Invasive meaning one that require design or software changes in the current IMDs and Non-Invasive meaning the scheme can directly work with existing IMDs without any modifications. While non-invasive schemes provide great advantage for existing IMDs; invasive schemes are more robust.

3.3.4.1 Invasive Approaches

1. **Communication Cloaker:** A removable external device is proposed in [80] that provides fail-open defensive countermeasure. It controls access to the IMD by making it invisible to all unauthorized devices. It encrypts all communications to

and from the IMD and checks them for authenticity and integrity. It provides fail open access during emergency when removed and shifts power-intensive computation to the cloaker reduces battery consumption. Being chargeable, it can protect against battery draining attacks but no implementation is shown.

2. **WISPer:** Zero-power defenses [14] which means security at no cost to the IMD battery have been proposed for IMDs, in which the induced RF energy is harvested for notification, authentication, and key exchange. It uses RFID-style remote powering until the authentication process is completed, and then more general access to the implanted device and battery are enabled. External device (battery less proxy) is used by medical staff to negotiate a temporary key with the IMD through the patient's body by acoustic signaling to access the IMD. Zero-power notification harvests induced RF energy to wirelessly power a piezo-element that audibly alerts the patient of security-sensitive events at no cost to the battery. Zero-power authentication uses symmetric cryptographic techniques to prevent unauthorized access; it aims to protect against adversaries. Sensible key exchange combines techniques from both zero-power notification and zero-power authentication for vibration-based key exchange that a patient can sense. This scheme is susceptible to attacks on privacy and eavesdropping during key exchange.
3. ***Heart-to-heart (H2H) Authentication:*** Authors in [81] designed a security scheme which uses ECG (heartbeat data). Their scheme performs a cryptographic device pairing protocol that uses Physiological Values randomness to protect against attacks by active adversaries. It requires the IMD and external device to measure the PV simultaneously which requires physical proximity and therefore is not useful during remote monitoring. Moreover, they assume a Transport Layer Security (TLS) channel established between IMD and external device. TLS protocol is resource intensive therefore not advisable to be implemented in IMD.

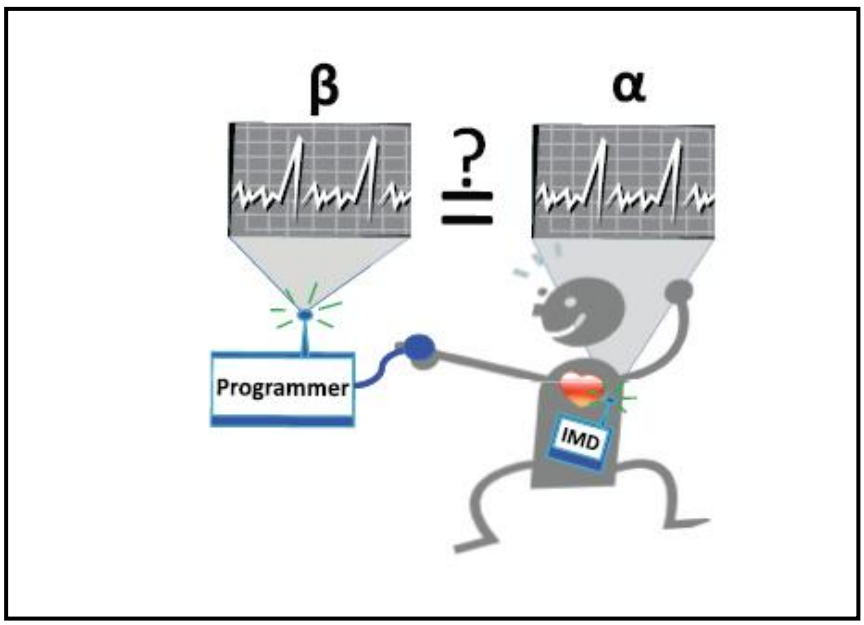

FIGURE 3.2 ECG readings taken simultaneously by IMD and external device is matched to allow access [81]

1. **SISC *for Secure Implants:*** In [82], a new implant system architecture is proposed where security and main-implant functionality are made completely decoupled by running the tasks onto two separate cores. The security core is powered by RF-harvested energy for it to perform external-reader authentication without fearing about Denial-of-Service (DoS) attack against battery. Authentication is performed without drawing energy from implant's battery by harvesting energy from requesting entity. The low-power security processor that executes the communication protocol is called Smart-Implant Security Core (SISC) and is designed to work independently from the primary implant module. It provides mutual authentication between IMD and external reader. It relies on offline key distribution and on fail open access in case of emergency.
2. ***Powerless Mutual Authentication:*** In [4] RF- energy harvesting is used to mitigate battery constraint and biometric key extracted from ECG signals is used for mutual authentication in regular and emergency access. It also protects the ICD against clogging attacks.
3. ***Trust Based Security:*** To meet the requirements on low computational complexity, N-th degree truncated polynomial ring (NTRU)-based encryption/decryption is used to secure IMD–sensor and sensor–sensor communications in [83]. This scheme is based on direct/indirect trust relationship among sensors.

3.3.4.2 Non-Invasive Approaches

1. **Shield**: Uses physical layer mechanism for secure communication with IMD and cryptographic channel to communicate with external devices. It deals with passive as well as active attacks. It works as a personal gateway which acts as a jammer-cum-receiver and jams the messages to make them and unauthorized commands IMDs preventing others from decoding them while itself being able to decode them [84]. It then encrypts the IMD message and sends it to the legitimate programmer. All commands must be encrypted and sent to the shield first, which is then relayed to the IMD. Being non-invasive for IMDs, it requires changes in all programmers. Here, confidentiality is not warranted for data exchange between shield and IMD. It is not effective for radio technology due to potential legal issues with jamming.

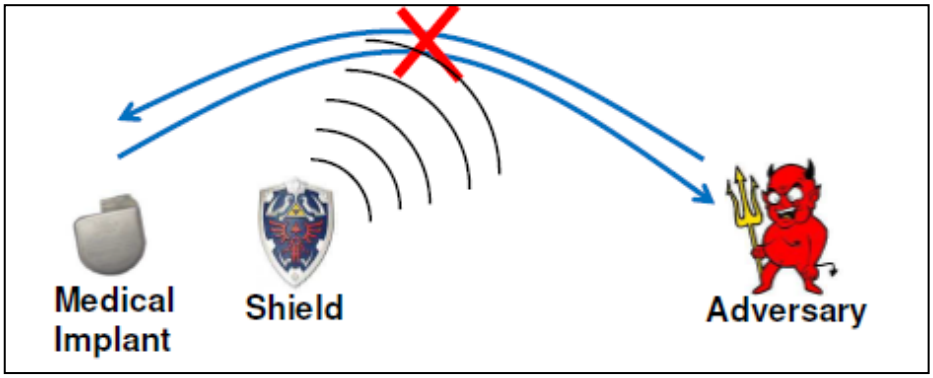

FIGURE 3.3 Shield Jamming Unauthorized Communication [84]

2. **MedMon:** Authors in [45] propose a medical security monitor (MedMon) for detection of active attacks by snooping (passive monitoring) on radio communication. It uses multi-layer anomaly detection. Physical anomalies are detected by observing received signal strength indicator (RSSI), time of arrival (TOA), differential time of arrival (DTOA), and angle of arrival (AOA). Behavioral anomalies are identified by checking with historical data and commands. On detecting malicious activity either audibly notifies the user or jams the communication. It requires to be trained to differentiate normal and malicious behavior. Like in other such systems, it may suffer from false positives and false negatives. Moreover this scheme does not protect from passive and replay attack.
3. **BodyDouble:** Authors in [85] employ a non-key based security scheme by use of external authentication proxy embedded in a gateway and paired with IMD. As in

[84] gateway transmits jamming signals to jam every incoming request to the IMD but itself receives the request and performs authentication using digital signals, for attacker it establishes a spoofed connection to thwart repeated attacks by same attacker. Here, communication is not encrypted (assumes a covert encryption channel) and authentication scheme cannot protect against identification frauds as IMD device ID and FCC ID are used for authentication.

4. **IMDGuard:** Authors in[86] secures Implantable Cardiac Devices(ICDs) by an external device that utilizes the patient's electrocardiography signals for key extraction. It is a device that would pair with an IMD and use radio jamming to defend against eavesdropping and unauthorized commands under non-emergency conditions. IMDGuard protocol is subjected to man-in-the-middle attack that reduces its effective key length as shown in [42].
5. **Statistical/Machine Learning:** Author in [37] proposes elliptic curve cryptography (ECC)-based key-management protocol to securely derive and update symmetric keys between medical sensors and collection devices. Protocol enables symmetric keys to be derived without the existence of any prior shared secrets, making it scalable to large systems. Collection device uses a two-tier authentication scheme to verify the source of incoming patient data. At the first tier, data from patient is accepted only if biometric signature matches. At the second tier, incoming physiological data is continually passed to a filter that assesses whether the data is consistent with prior data from that patient. The filter uses statistical or machine-learning techniques to learn a patient's profile and then raises an alarm if incoming data deviates from that profile. An alarm could be triggered by falsified patient data or an acute change in the patient's medical condition. This scheme does not consider the power constraint of IMD to a large extent.
6. ***PIPAC:*** Patient Infusion Pattern-based Access Control Scheme for Wireless Insulin Pump System [87]uses Smartphone to provide physical layer as well as application layer security. At physical layer Near Field Communication (NFC) based access control and at application layer it uses past glucose trends to detect anomalous insulin pump system behavior. This scheme can be used to defend against security attacks in particular (1) single acute overdose and (2) chronic overdose. It uses SVM based regression scheme and a supervised learning approach to learn normal patient infusions pattern with the dosage amount, rate, and time of infusion, which are

automatically recorded in insulin pump logs. The generated SVM based regression models are used to dynamically configure a safety infusion range for abnormal infusion identification. Abnormal infusions of bolus dosage, basal rate, and total daily insulin would send an alarm to the patient and can be deactivated during emergency to give fail open access. This scheme suffer from False Positive and False Negatives.

3.3.5 Emergency Access for IMDs

In Emergency State stringent security policies may pose a risk of inaccessibility for the IMD [80] [27] if authorized staff is unavailable threatening safety of patient. Therefore a viable solution is to disable security in case of an emergency. But this may turn out to become the weakest link for an unauthorized person to gain control of an IMD's operation or disable its therapeutic services, this may also motivate the attacker to induce false emergency. Therefore it is important to look into the solutions which work even during emergency.

1. **Biometric Based:** [77] provides biometric based two-level secure access control scheme for IMDs for use in emergency situation. The first level uses basic biometric information and second level requires iris recognition. This technique has limited use as it requires external devices to be equipped with features of biometric measurement.
2. Heart-to-heart (H2H): In [81] ICDs can be accessed in emergency by external device kept very close to patient's heart for matching of physiological values sensed by reader and ICD simultaneously.

3.4 Comparison of Security Models

In this section we discuss the merits and demerits of available security schemes. This field witnesses many state-of-art solutions for securing IMDs while considering the power management, emergency situations, and essential security properties as shown in Table 3.1. But there are certain loopholes. While none of the security scheme addresses IMD privacy and non-repudiation challenge, most of them also lack in Key Management front.

TABLE 3.1 Comparisons of Surveyed Security Models

	Proximity [29]	***IMDShield [84]***	**MedMon [45]**	**IMDGuard [86]**	**Cloaker [80]**	**H2H [81]**	**WISP [14]**
SECURITY DIMENSIONS							
Key Management	Yes	No	No	Yes	No	Yes	Yes
Authentication	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Message Integrity	No		Yes	No	Yes	Yes	No
Confidentiality	Partial	Yes	No	Yes	Yes	Yes	Yes
Availability	No	No	No	No	Yes	No	Yes
Access Control	No	No	No	No	No	No	No
Non-repudiation	No	No	No	No	No	No	No
Replay Resilience	No	No	No	No	No	Yes	No
Privacy	No	No	No	No	No	No	No
DESIGN DIMENSIONS							
Protection Type	PREV	PREV	DET	PREV	PREV	PREV	PREV
Target Device	All IMD	All IMD	All IMD	ICD	All IMD	ICD	All IMD
Invasive	Yes	No	No	Yes	Yes	Yes	Yes
Core Mechanism	Distance Bounding	Jamming	Anomaly Detection	Jamming	Secure Protocol	PV exchange and TLS	WISP
Access Pattern	Both	REG	REG	REG	REG	Both	REG
Energy Source	IMD battery	Shield Battery	External	External	External	IMD battery	Energy Harvesting
Flexibility	No	No	No	No	No	No	No
Applicability	IMD-ED	IMD-ED	IMD-ED	IMD-ED	IMD-ED	IMD-ED	IMD-ED

Most of the scheme uses a naïve technique of access control which is neither role based nor context aware. Quite a few schemes are device specific and cannot be used for all IMDs and do not address the heterogeneous nature of IMDs. These schemes secure wireless communication between an IMD and external device but fail to work for multiple IMDs implanted on a human body and internetworked with each other. The shortfalls are enumerated below:

1. Most of the schemes use pre-shared keys over a long period of time makes them vulnerable to cryptanalysis attacks.

2. Most of the schemes do not take IMD interoperability as design criteria.
3. Most of the schemes do not provision encipherment technique upgrade.
4. Above schemes do not address Privacy Issues.
5. Most of the schemes provide naïve access control which is neither role based (fine grained) nor context aware.
6. Above schemes do not provide non-repudiation.
7. Most of the schemes adopt fail-openness during emergency which leads to no security during emergency.
8. Most of the schemes are not scalable when more IMDs are added.
9. Many schemes are device specific thus not suitable for a wide range of IMDs.

3.5 Conclusion

In this chapter we have presented a complete taxonomy of security models designed in order to achieve communication security for IMDs. Our analysis shows that more emphasis has been given to securing IMD and External Device communication while paying less heed to IMD and IMD communication. We have identified several areas of future work such as need for a generalized and complete model for securing wireless communication of an IMD on a human body. Also the scheme needs to be autonomous for wide acceptability by patients who cannot afford to configure and maintain rigorous security schemes. Finally, as the IMD devices evolve to include interoperability the security scheme must evolve as well to cater to the increasing demands of security. As the external devices based approach is the most flexible and scalable option in which sophisticated security mechanism can added depending on the need of IMDs we use this model from development of a security solution.