Multidisciplinary Review Journal

Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 1, 2020

Review Article

SECURITY ISSUE IN IMPLANTABLE MEDICAL DEVICE: A COMPREHENSIVE SURVEY

Ajina Mohamed Ameer[1]*, Dr.M Victor Jose[2]

[1]Research Scholar, Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Thuckalay
[2]Associate Professor, Department of Computer Application,Noorul Islam Centre for Higher Education, Kumaracoil, Thuckalay
Corresponding Email: ajina1984@gmail.com

Received: 15.11.2019 ***Revised: 11.12.2019*** ***Accepted: 16.01.2020***

Abstract
Bioengineering is an area where new technology appear to be more suitable for effective disease treatments. Implantable Medical Device (IMD) have more , communications capability and decesions making abilities . different research work in computer security fields identify serious securities and privacy risk in IMD that which compromises implants and even patients health . Sensor for monitoring have l vital sign like heart rates,electrocardiogram reading, respiration rates, blood pressures, temperatures, blood glucose level and neural system activities can be analysed currently . These technologies can monitor patient depending on disease or based on situations. The technologies differ from sensor attached to body to good sensors to environments and new breakthrough show different monitorings which needs only patients to be within few meters from sensors.This articles survey goals of main securities for IMD of next generation and analyze the main relevant protection mechanism.

Keywords: Mobile health,Remote patient monitoring,Sensor, Implantable medical device, Wireless sensor network.

DOI: http://dx.doi.org/10.31838/jcr.07.01.92

INTRODUCTION

The wireless communication capability in modern Implantable Medical Device are major sources of security risk, particularly when the patients are in open environment. the implants become no longer ‘‘invisible’’, as presence of implant can be remotely found[ ]. Also, it facilitate accessess for transmitted datas by eavesdropper who listens to channels simply [44]. This results in majority of privacy breach, as IMD stores sensitive informations like diagnosed condition, vital signal, therapy, and different personal datas (example name, birth dates, and other medicinally identifier . communication channels which is vulnerable also makeit simpler to attack implants in way similar to those against common computing device[ ], that is , by altering,forging, or replying previous noted message[ ]. This potentially allows an adversary for monitoring and modifying implants without being closer to victims. Implantable Cardioverter Defibrillators replaced by yet other one without WiFi While there are still non known real-worlds processes, different attack on IMD succeedingly are shown in labs. These attack show how adversary can change or renew therapy on ICD with wireless connectivities, and that which induce shock States for patients. Other attack depletes batteries and render devices inoperativeness, which shows that patient must go through surgery for having IMD changed. Moreover, in cardiac implant case, they has switch that which can turn off by applying magnetic fields[ ]. This mechanisms motivated by shield ICD needs for electromagnetic field, for instance when patients done cardiac surgeries by electronic equipment [ ]. Anyhow tthis can be attacked,since activation of primitive mechanisms dont need such authentications. The IMD vulnerability exploitation by any attack can have any negetive medical effect for patients. That type of impacts termed as ‘‘adverse event’’.

Basic element of remote monitoring systems are data processing systems, datas acquisition systems, end-terminals at hospitals and communication networks. Datas acquisition systems have varying sensor or device with embedded sensor with datas transmissions ability wirelessly. With technological improvement, senor can not be medical sensor alone ; it can be camera or smart phone. This is du,e to researches look into contactless method where device cannot contact with patients [ ]. common forms of these sensor used in with-contact method are wireless sensors network.These can be in turn divided as , body area network or personal area network and wireless body area network . Datas processing systems have system with datas transmitting and receiving ability and processing units/circuits terminal at hospital sides can be either computers (or a databases) , dedicated devices or Smartphones . communication networks connect datas acquisition systems to datas processing systems and further transmit detected datas and conclusion to healthcare professionals who in contact with system by communication networks. Based on situations complexity, the patients either prompte admitting to hospital do some first-aids/ caution step and /takes some medication. The remote health monitoring system, their technology, capability and action availabilities differ to large extend.

Moreover, securities measure supporte on each IMDs and security assessments result can be public. Prudent engineeringa practice known in safeties and security's domain should be followed in IMDs designs. If hard-wares error are found, ofently we do replace the implants, with risk associated link to surgeries. One of failure reson when monitoring patients is precise malfunctioning of devices itself. These failure are termed as ‘‘recall’’ or ‘‘advisory’, and it is known that that they affects about 2.6 Percentage of patient carrying implants. Further more,the softwares on devices should support functionality needed to show the medical and operating task for which it was made[34,72,114].

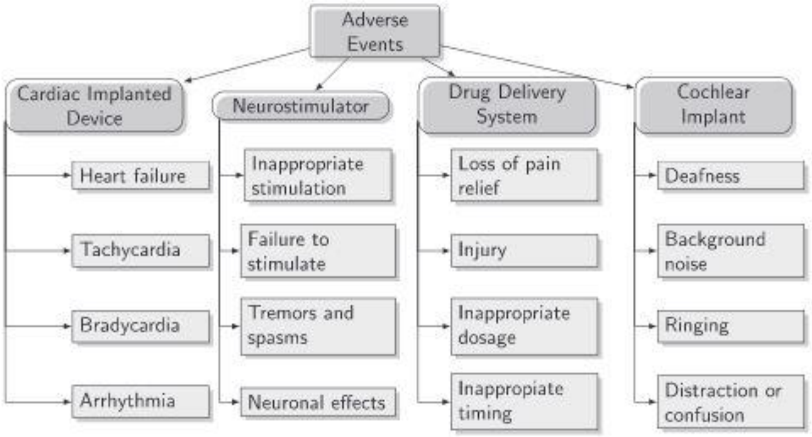

Fig. 1.Adverse event for 4representative IMD types.

IMD s often define as electronic devices that is permanently/ semipermanently implante on patients with aim of treating medical conditions, improving functionality of some body parts, or givig users ability that they didn't had before[ ]. These device are oftenly implanted two- three centimeters under patient's skins and connecte to organs need treatments . Cardiac implant are possibly most known examples of IMD, but many other are incrementally used for dealing with various medical condition effectively compared to traditional method. The most common type includes: Cardiac implant device. These include device like Implantable Cardioverter Defibrillator and Pacemaker. They treat cardiac condition by heart activities monitorings and electrical impulse application of suitable intensities and location to make heart pump at desired speeds[ ]. New model are with pressures sensor which can actively monitor that leads to heart failures. This allow to alerts patients or medical

personnels if pressure increments in ventricles is noted, as this represent a hazardious conditions for patients. Cardiac implant equip with accelerometer for mesuring patient physical activities levels. This sets as input parameters for IMD controllers, which allows for adjusting cardiac stimulations frequencies to one suiting each moments.

In Recent days FDA publish guidelines for industry on designs, testings, and uses of wireless medicine device[ ]. As stated, security of wireless signals and datas is importantly an issue inorder to preserve accessess to patients datas and hospitals network, and for preventing communication which are not authorized with medical device like IMD or Programmer. Wireless medical device should use crypto-graphic technique (that is ., authentications, encryption,and secure keystorages) for protecting communication and access. The security levels decided by threats, and it's probabilities, to which devices are exposed, and operating environments and consequence on patients in case of asecurity incidents. For designing of secure solution, FDA suggest wireless medical device include security measure for protecting communication and access but also including software protection. Nowadays, FDA is presently working on design of recommendations for managements of cybersecurities in medical device[ ].

System models and usage scenario

Fig.2 represents main entity in system and show possible communication interaction between these device. The IMDs communicates with Programmer, which can be any entities/devices authorize for interacting with implants .In normal operations, the programmers have to initiate communications with IMD s. Since radio channels is share communication mediums, programmer will hear to channels till it detects that is non busy for establishing communications. The aim of this communication is requesting datas (example,ECG signal or insulin level) or send command (example treatment modification). In case of secure solution, IMDs and Programmers are authenticated and sensitive datas is passed encrypt on . IMDs must operate under 2 varying mode: normal and emergencies. One main aim is for finding a sensible trade-off between these 2 situation. Security's in normal operations modes. The patient control what entity can have interaction with IMD s. In this cases, it is the necessity for implementing a strong accessess control mechanisms and cryptographic protocol in communications link to malicious and unauthorize accesses. The IMD s should neglect indiscriminated data request or devices.

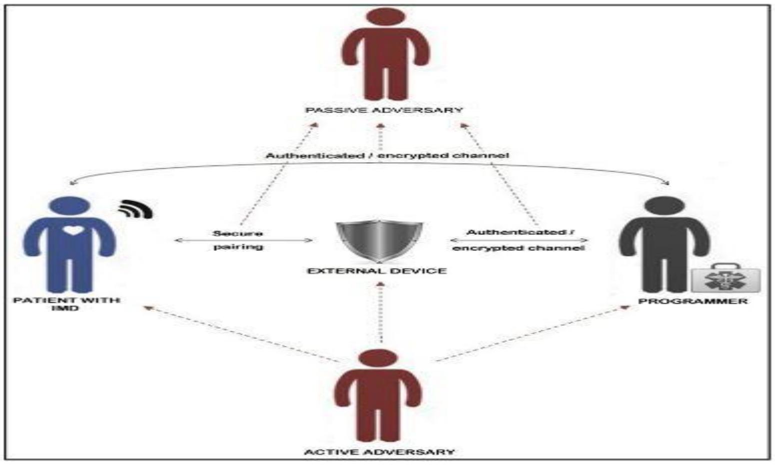

Fig. 2.Typical usages of scenarios for IMDs

In the secure solution case , the IMD s and Programmers are authorized and sensitive datas are passed with encryption on channels. Apart from direct communications between IMD s and Programmers, idea of external devices uses (example cloakers, Shields, IMD Guards, etc.), which act as proxy's. In this cases, rather establishing direct connections with Programmers, the IMDs delegates this tasks for external devices that authenticates Programmers, initially there is secure pairings between IMD s and external devices. Once Programmer is authorized, this can communicates with IMDs using encryption on channels by external devices. In emergency modes, the IMD s have to give answers even if authentications fails and, in some case, the medical personnel's should disable the devices . As patients generally will move about varying location and can visit different hospitalsl and doctors , IMD always will not communicate with same, known devices. Also, the entities authorized for communicating with implants may differ[ ].

An emergency solution that gives needed safeties for patients is to force IMDs for disregarding and authorizing mechanism and to process all incoming command. Any requesters then become authorized user, possibly with full privilege. This is not accomplishable if securities protocol and strong accessess control mechanism are not deactivated, which can make fully exposed to attacker's.

Heart and blood based disease's monitoring system

Heart based monitoring system are common types of monitor system. The reasons for this can be that vital sign with heart can be related to different illness which reveal many hidden illness. chronic heart failures, Cardiac arrhythmias, blood clot,stroke, and higher blood pressures are some of common illness in this categories. The possibilities for measuring heart rates,ECGs, blood pressures,respiration rate, oxygen volumes in blood and arrhythmias detections . Different technology like ECG monitoring or textile-linked wearable system are used for getting the datas. Although these essential datas can be collected, there is more spaces to improve system accuracy . Different application that use Smartphones in different aspect of cardiologies like remote patient monitoring and user guidance application for cardiac disease prevention are studyed.[ ].

Challenges

This monitoring system is common as heart based illness, are causes of mortalities in world. Also, goodl sign monitoring systems often give overall result with respiration and heart related measurement. Main challenge in this area is to get clean signals from patients. Contact-based method uses method such as ECGs and photoplethysmographic method uses light incidenting on small vein close to skin surfaces and evidence shows that it is very useful. breathing abnormality and respiratory system probkems detections challenges the monitoring system since these system have breathing sound detections.

Contact-based method

'telemonitoring systems' use software and hardware device for monitoring different heart-based illnesses. Software application runs on android platforms. heart rates variability and ECG detections methods based on Autonomous Nervous System. Cardiovascular disease are monitored by off-the-shelf sensors set. ECGs and Blood pressure monitoring systems have algorithms based on 5 state where mobile devices can be of varying state which depends on charge levels [ ]. this has energies optimizations feature where even datas storages will be done with energies saving. Another system measure personalheart rates, ECGs, pulse oximetries, pH levels of blood and temperatures using a series of sensor. This system can measure ECG,air flows in lung, body temperatures,galvanic skin responses and oxygen saturation level. Although full fall detection systems, for aiding the decesion, it gather accelerometer reading and vital sign like SpO2,ECGs, temperatures, heart rates ,heart rate variabilities .Developing applications for real-time monitorings of patient with coronary artery and heart disease. It's categorising method is eighty five percent correct while detection work is zen %. It work in 3 modes (, sports, drive and rest), and have ten -fold algorithms depending on support vector machine for aiding decisions making. Use of telemedicines scenarios, where 2 paramedic within ambulance communicates to 'tele-EMS physicians' in 'teleconsultation centres' in remote locations, it is analysed that simple web applications and devices interface are best than special network using protocol and off-the-shelf device in emergency telemedicine system, since the former dont put any constraint on user and developers.

5G mobile system can enhance full monitoring with systems. System architectures for sensing cardiac datas for wheelchair users, Photoplethysmography imagings using Oxicam and false alarm reductions systems are some analysis made recently [ ].

use of piezoelectric senior for heart-related medical reading and seismo cardiograms are noted and similarly HeartCycles use textile-based sensor, Bayesian algorithms are used for findingabnormalities of heart rates. Improved Fourier Interpolation methods are used in capacitive electrocardiographic and heart rates monitoring systems. This have been verified with various clothes thickness [ ].

Table 1 summary if the technology

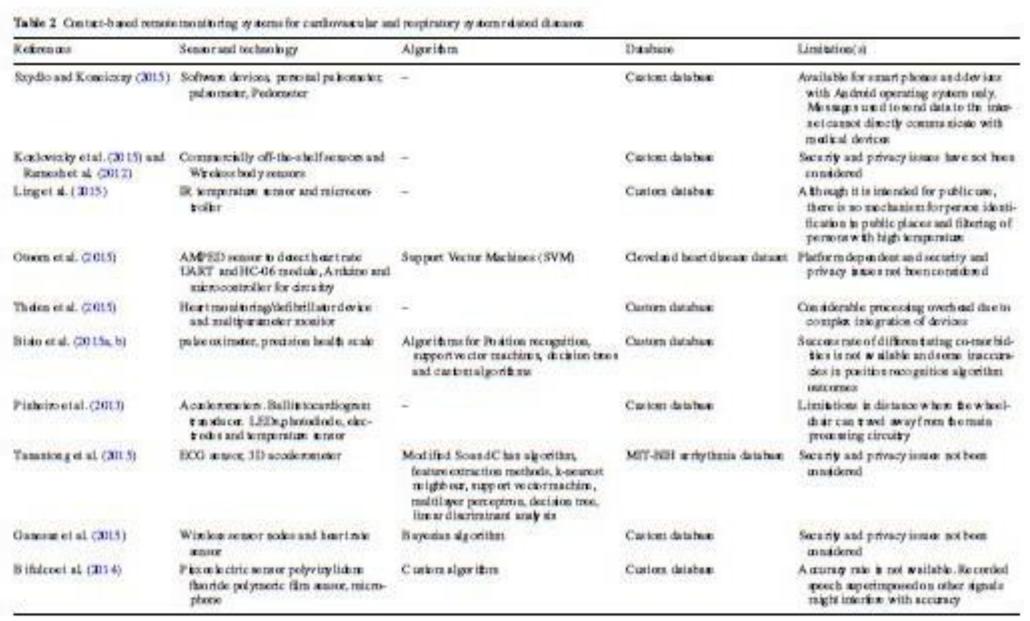

Table 2 Contact-based remote monitoring systems for cardiovascular and respiratory system related diseases

References	Sensor and technology	Algorithm	Database	Limitation(s)
Szydlo and Konieczny (2015)	Software devices, personal pulsometer, pulsometer, Pedometer	–	Custom database	Available for smart phones and devices with Android operating system only. Messages used to send data to the internet cannot directly communicate with medical devices
Kozlovszky et al. (2015) and Ramesh et al. (2012)	Commercially off-the-shelf sensors and Wireless body sensors	–	Custom database	Security and privacy issues have not been considered
Ling et al. (2015)	IR temperature sensor and microcontroller	–	Custom database	Although it is intended for public use, there is no mechanism for person identification in public places and filtering of persons with high temperature
Otoom et al. (2015)	AMPED sensor to detect heart rate UART and HC-06 module, Arduino and microcontroller for circuitry	Support Vector Machines (SVM)	Cleveland heart disease dataset	Platform dependent and security and privacy issues not been considered
Thelen et al. (2015)	Heart monitoring/defibrillator device and multiparameter monitor	–	Custom database	Considerable processing overhead due to complex integration of devices
Bisio et al. (2015a, b)	pulse oximeter, precision health scale	Algorithms for Position recognition, support vector machines, decision trees and customal algorithms	Custom database	Success rate of differentiating co-morbidities is not available and some inaccuracies in position recognition algorithm outcomes
Pinheiro et al. (2013)	Accelerometers, Ballistocardiogram transducer, LEDs, photodiode, electrodes and temperature sensor	–	Custom database	Limitations in distance where the wheelchair can travel away from the main processing circuitry
Tamaniong et al. (2015)	ECG sensor, 3D accelerometer	Modified So and Chan algorithm, feature extraction methods, k-nearest neighbour, support vector machine, multilayer perceptron, decision tree, linear discriminant analysis	MIT-BIH arrhythmia database	Security and privacy issues not been considered
Gaman et al. (2015)	Wireless sensor nodes and heart rate sensor	Bayesian algorithm	Custom database	Security and privacy issues not been considered
Bifulco et al. (2014)	Piezoelectric sensor polyvinylidene fluoride polymeric film sensor, microphone	Custom algorithm	Custom database	Accuracy rate is not available. Recorded speech superimposed on other signals might interfere with accuracy

Mesured Heart rates by use of web-camera have been proved to be accurate by conventional ECGS. Respiration rates have been found similarly by use of web cameras. Kinect versions of 2 camera have been found proven accurate by studies for measuring respirations in neonate. The use of optical proximities sensor in photoplethysmographys for getting physiological signal. blood pulse measurements system by uses of linearly polarized lights [ ]. Uses of pupillary fluctuation is another way for mesuring heart rate vulnerabilities. Segmentations of boundaries of eye pupil and remote eye tracks are beneficial here, for viewing pupil diameters change that occur with heart beats. A web-dependent interfaces for optical coherence tomographic images processing for disease diagnosis in relation to retinas. Other facial sign can be also used for deriving many datas in association with cardio-metabolic event. These requires cameras, multispectral imaging systems and 3D optical sensor. Uses of dual-wavelength imaging systems for finding blood oxygen saturations. The wireless systems monitor respiration while wearable systems detect patients coughing. Inertial measure unit are used for measuring thoracic and cavities motion for monitoring of respiration while a MEMS microphones are used for recording coughing and air sound from Chester. While these systems claime to be contactless systems for respiration monitorings. its not fully no-contractual as IMU unit are attached for chests. Only reading are wirelessly sent . Anyhow, as IMU node are low-weighted node person is free for activity thus this is advantages. The node also need lower power (3.7V) and systems can find talking and can differentiate cough. This is a promising method that use 0 crossing rates and filter for processings. It suggest more complexity in algorithm for enhancement.

CONCLUSION

Implantable Medical Device improves qualities of life of patient and, in some case,plays a vital role in preserving them live. The new generations of IMD are incrementally including more computing and communicating abilities. More recent development in contactless cameras-based method. Based on different category existing research have been shown. The reviews show that this field is making substantial impacts on society and researches communities. As technology advance, outcome are also improved. Further cooperations among researcher from manufacturing technology, bioengineerings, and computer securities are vital for guaranting both patient's privacies and safeties and securities of datas and communication. The IMDs are computer systems that are embedded in humans. This is nowaday special situations and user opinions should be taken into accounts as far as required.

REFERENCES

1. C.J. Borleffs, J. Thijssen, M.K. de Bie, J.B. van Rees, G.H. van Welsenes, L. vanErven, J.J. Bax, S.C. Cannegieter, M.J. Schalij, Recurrent implantablecardioverter-defibrillator replacement is associated with an increasing riskof pocket-related complications, Pac. Clin. Electrophysiol. 33 (8) (2010) 1013–1019.
2. Arney, K.K. Venkatasubramanian, O. Sokolsky, I. Lee, Biomedical devicesand systems security, in: Annual International Conference of the IEEEEngineering in Medicine and Biology Society, 2011, pp. 2376–2379.
3. K. Daniluk, E. Niewiadomska-Szynkiewicz, Energy-efficient security inimplantable medical devices, in: Federated

Conference on ComputerScience and Information Systems (FedCSIS), 2012, pp. 773–778.

4. T.P. Berger, J. DHayer, K. Marquet, M. Minier, G. Thomas, The GLUON family: alightweight hash function family based on FCSRs, in: Progress in Cryptology –AFRICACRYPT 2012, Lecture Notes in Computer Science, vol. 7374, Springer,Berlin Heidelberg, 2012, pp. 306–323.
5. M.A. Callejon, D. Naranjo-Hernandez, J. Reina-Tosina, L.M. Roa, Acomprehensive study into intrabody communication measurements, IEEETrans. Instrum. Meas. 62 (9) (2013) 2446–2455
6. M. Darji, B. Trivedi, Detection of active attacks on wireless IMDs using proxydevice and localization information, in: Security in Computing andCommunications, Communications in Computer and Information Science,vol. 467, Springer, Berlin Heidelberg, 2014, pp. 353–362.
7. FDA, Radio Frequency Wireless Technology in Medical Devices – Guidance forIndustry and Food and Drug Administration Staff, 2013.
8. K. Fu, Trustworthy medical device software, in: Public Health Effectiveness ofthe FDA 510(k) Clearance Process: Measuring Postmarket Performance andOther Select Topics: Workshop Report, 2011
9. D. He, S. Chan, S. Tang, A novel and lightweight system to secure wirelessmedical sensor networks, IEEE J. Biomed. Health Infor. 18 (1) (2014) 316–326.
10. X. Hei, X. Du, Biometric-based two-level secure access control for implantablemedical devices during emergencies, in: Proceedings IEEE INFOCOM, 2011,pp. 346–350.
11. X. Hei, X. Du, J. Wu, F. Hu, Defending resource depletion attacks onimplantable medical devices, in: Proc. of IEEE Global TelecommunicationsConference (GLOBECOM), 2010, pp. 1–5.
12. N. Henry, N. Paul, N. McFarlane, Using bowel sounds to create a forensically-aware insulin pump system, in: Workshop on Health InformationTechnologies, HealthTech, USENIX, 2013, pp. 1–10.
13. S. Hosseini-Khayat, A lightweight security protocol for ultra-low power ASICimplementation for wireless implantable medical devices, in: 5thInternational Symposium on Medical Information CommunicationTechnology (ISMICT), March 2011, pp. 6–9.
14. F. Hu, Q. Hao, M. Lukowiak, Q. Sun, K. Wilhelm, S. Radziszowski, Yao Wu,Trustworthy data collection from implantable medical devices via high-speedsecurity implementation based on ieee 1363, IEEE Trans. Inform. Technol.Biomed. 14 (6) (2010) 1397–1404.
15. F. Hu, Q. Sun, Y. Wu, M. Guo, J. Lu, J. Li, D.J. Gay, J.K. Garner, A.L. Poellnitz,Implantable medical devices: architecture and design, in: TelehealthcareComputing and Engineering: Principles and Design, first ed., 2013, pp. 359–406 (Chapter 14).
16. Magno M et al (2013) A versatile biomedical wireless sensor node with novel drysurface sensors and energy efficient power management. In: Advances in sensors and interfaces (IWASI), 2013 5th IEEE international workshop on, pp 217–22
17. Mainanwal V, Gupta M, Upadhayay SK (2015) A survey on wireless body area network: security technology and its design methodology issue. In: Innovations in information, embedded and communication systems (ICIIECS), 2015 international conference on, pp 1–5
18. Malhi K et al (2012) A zigbee-based wearable physiological parameters monitoring system. IEEE Sens J 12(3):423–430
19. Mastorakis G, Makris D (2014) Fall detection system using kinect’s infrared sensor. J Real Time Image Process 9(4):635–646.
20. Rodbard D (2016) Continuous glucose monitoring: a review of successes, challenges, and opportunities. Diabetes Technol Therapeut 18(S2), S2–3–S2–13.
21. Nadeem A et al (2015) Application specific study, analysis and classification of body area wireless sensor network applications. Comput Netw 83:363–380
22. Sawand A, Djahel S, Zhang Z, Naït-Abdesselam F (2015) Toward energy-efficient and trustworthy eHealth monitoring system. China Commun 12(1):46–65
23. Schneider RB, Biglan KM (2017) The promise of telemedicine for chronic neurological disorders: the example of Parkinson’s disease. Lancet Neurol 16(7):541–551. sSerhani MA, El Menshawy M, Benharref A (2016) SME2EM: smart mobile end-to-end monitoring architecture for life-long diseases. Comput Biol Med 68:137–154
24. Prabhakar SK, Rajaguru H (2017) Development of patient remote monitoring system for epilepsy classification. In: Goh J, Lim CT, Leo HL (eds)
25. Szydlo T, Koneiczny M (2015) Mobile devices in the open and universal system for remote patient monitoring. IFAC-PapersOnLine 48(4):296–301
26. Tanantong T, Nantajeewarawat E, Thiemjarus S (2015) False alarm reduction in bsn-based cardiac monitoring using signal quality and activity type information. Sensors 15(2): 3952.
27. Fatima, K., Mathew, S., Suhail, M., Azhar, E., Damanhouri, G., Qadri, I. Architecture of viral RNA helicases; HCV helicase as antiviral target (2018) International Journal of Pharmaceutical Research, 10 (2), pp. 31-39. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85042429638&partnerID=40&md5=844e4516225a82a049ba4ac49cbe0076
28. Nirmala, Kulandaisamy Agnes, and Marimuthu Kanchana. "Leucas aspera – A Review of its Biological activity." Systematic Reviews in Pharmacy 9.1 (2018), 41-44. Print. doi:10.5530/srp.2018.1.8