Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth

Kashif Habib, Arild Torjusen, Wolfgang Leister
Norwegian Computing Center
Oslo, Norway
Kashif.Sheikh@nr.no, Arild.Torjusen@nr.no, Wolfgang.Leister@nr.no

***Abstract*—A patient monitoring system for the Internet of Things in eHealth can be established through the integration of wireless body area network, communication infrastructure, and the hospital network. The dynamic and heterogeneous environment of the Internet of Things may facilitate the patient with mobility options. However, security-related problems may obstruct the development of such a comprehensive patient monitoring system. While assessing the security of a patient monitoring system, it is necessary to realise that it may not be enough to only look into the security related aspects of the body area network. Instead, the overall patient monitoring system should be treated as a connected and integrated eHealth system. This paper analyses the important security issues that can put the eHealth system at risk. The specific security goals and requirements, vulnerabilities, threats, and attacks are analysed and some possible security recommendations with direction for future work are discussed.**

Keywords- Internet of Things, Patient Monitoring System, eHealth System, Security.

I. INTRODUCTION

Wireless and mobile communications have played a significant role towards the development of the Internet of Things (IoT). The IoT is a network of interconnected things, such as biomedical sensors, radio frequency identification tags, actuators, and smartphones [1]. The IoT presents a concept of dynamic and heterogeneous network environment, where things communicate and exchange information in an automated or semi-automated way [2], and embed real world information into networks [3]. The communication capabilities and support for dynamic environment in the IoT can provide significant advantages to the existing healthcare system [4]. The IoT can assist the existing healthcare system by developing flexible remote Patient Monitoring System (PMS) that can benefit the patients by getting quick medical responses from the medical practitioners. However, security related issues may obstruct the development of such a comprehensive PMS.

1.1 Contribution and Organisation of This Paper

A significant contribution of this paper is the integrated security analysis of the IoT based PMS, i.e., we highlight the security related aspects in the whole eHealth system including Body Area Network (BAN), communication network, and health care enterprises. In order to analyse the security of a PMS, Section II presents the eHealth system architecture. Section III presents the security analysis of a PMS by focusing on security goals and requirements, threats, vulnerabilities, and attacks. Related work is high-lighted in Section IV. Section V provides discussion and security recommendations. Section VI concludes the paper and addresses future work.

II. EHEALTH SYSTEM ARCHITECTURE

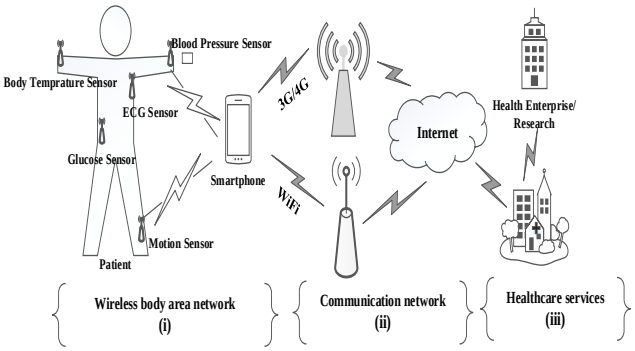

Figure 1. The IoT based patient monitoring system

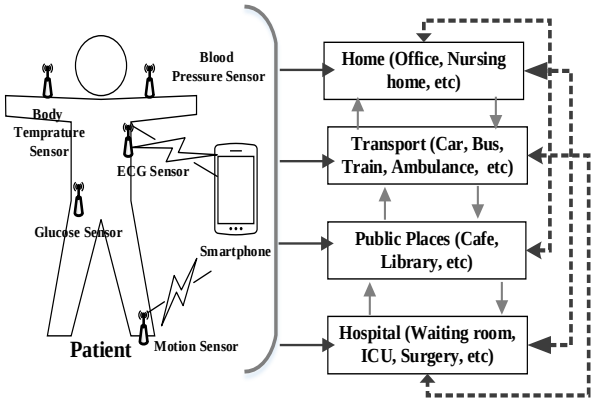

Figure 2. Schematic of the IoT in patient mobility scenarios

A PMS is comprised of three segments, i.e., (i) BAN, (ii) communication network, (iii) hospitals and health care enterprises [5]. As depicted in Figure 1, the BAN includes the actual patient, medical sensors, and the patient's smartphone. The devices in the BAN are configured by clinical staff for data collection. The patient's smartphone collects the monitored information which is then forwarded to the hospital via

 ISBN: 978-1-61208-384-1

a communication network. The communication networks including broadband network and 3G/4G network connect the BAN with a hospital network. Hospital and the healthcare enterprise evaluate the Patient's medical data and respond accordingly. The healthcare enterprise can also perform further data analysis for research purposes.

The mobility feature of the IoT in eHealth provides various possibilities of patient's locations during the monitoring sessions. As shown in Figure 2, the patient's movement in between different locations is highlighted with dotted lines. The patient monitoring sessions keep the patient connected with healthcare workers, even when the patient is outside the hospital environment.

III. SECURITY ANALYSIS

In the process of assessing the security of a PMS, it is essential to understand that it is not enough to only analyse the security issues at the BAN. Instead, security of the entire system including BAN, backend communication network, and hospital network should be analysed. The different segments of a PMS have several security requirements and possess vulnerabilities that can be exploited by threat agents to launch attacks against eHealth system. Quality of service (QoS), safety, and security are key aspects in the deployment of a PMS. Thus, identification of security related requirements, vulnerabilities, and threats are keys to the development of a trustworthy system. The identification of system assets, possible vulnerabilities and threats, and appropriate countermeasure can help to understand the associated system risks. The terms such as authentication, availability, confidentiality, integrity, information system, threat, vulnerability, and security requirements, are used in this paper in relation to their meanings defined by [6].

From a system point of view, transferring complete and accurate information from the patient to the hospital is always necessary. Failure to do so may cause a threat to the patient's health. People with bad intentions can send wrong data to the hospital by miss-utilising the devices. The quality of data may also vary depending upon the quality of communication links. The data from BAN is sent using public communication infrastructures to the hospital. Hence, data authentication is also very important.

Data security and patient's privacy are certainly the important challenges in the deployment of PMS. In order to highlight specific security requirements in PMS, we analyse the system as a sequence of segments, identify related security requirements, vulnerabilities, threats and attacks of each segment, and possible security solutions for identified issues.

A. Security Goals and Requirements

Successful deployment of a PMS relies upon secure transfer of the patient's vital signs to the hospital. The secure transfer requires that the PMS satisfies major security goals, requirements, and QoS requirements such as device/user authentication, authorisation, confidentiality, privacy, integrity, access control, availability, interoperability, reliability, usability, and resource efficiency. While security requirements are very important, some other factors such as incorrect use of devices, control on data disclosure, and usage also need proper attention. Table 1 provides a summary of the security goals and requirements in a PMS. The specific security requirements and security goals for all three segments are identified in the following sections.

TABLE 1. SECURITY GOALS AND REQUIREMENTS

BAN	Communication Network	Healthcare Enterprise
Data confidentiality, data integrity, data availability, data authentication.	Data confidentiality, data integrity, data reliability, data accuracy, data authentication.	Data confidentiality, data integrity, data availability, patient and data authentication, physical security, access control.

1) Body Area Network (BAN)

The communication links inside the BAN are built using wireless technologies. The security requirements and goals in such network need more attention in comparison to structured networks. Data confidentiality is required to protect data disclosure while in storage at local node or exchanged between nodes. Data confidentiality should sustain even if the nodes in the network are compromised. The leaked data may disclose the patient's disease related information. Data integrity is required to protect against modification of data not only while in transit but also when in storage. The modified data can lead the health personnel towards wrong diagnosis of the patient. Data availability is required to ensure that health personnel get timely access to the patient's data. Delayed or no access to the information may prevent the patient's treatment procedures. Data authentication is required to detect and identify any forged data sent by an adversary. It is also important to establish trust in the received data and in the overall system.

2) Communication Network

Once the patient's health status is monitored and processed inside BAN and stored in the smartphone, then data is transferred by the communication network. Data confidentiality is required to prevent information disclosure in case of interception of communication session. Data integrity is necessary to ensure that the data transferred from BAN to the hospital is unmodified. Data reliability requirement can ensure that the data from BAN to the hospital is available even in case of a link or node failure. Data accuracy is required to ensure that the data is fresh and not reordered by an adversary.

3) Hospital and Healthcare Enterprise

The patient's data are collected at the hospital for medical diagnosis and treatment. Physical security requires restricted physical access to the medical servers in the hospital containing patient's medical records. Weak physical security procedures may allow unauthorised persons to alter the data and system. Data confidentiality is required to limit the data monitoring at the PMS servers for only authorised persons. Data integrity is required to ensure that the data is secure against unauthorised modification. Data availability is required to ensure that data is available to the medical staff even in case of any system failure. Authentication mecha-

 ISBN: 978-1-61208-384-1

nism is required to not only authenticate the users in the hospital but also to ensure that data is received from the correct patient.

B. Threats, Vulnerabilities, and Attacks

BAN, communication networks, and hospital network are vulnerable to various security threats, mainly due to the inherent vulnerabilities of wireless communication. Table 2 provides a summary of threats, attacks, and vulnerabilities in a PMS. We highlight only specific vulnerabilities, threats, and attacks in different segments of a PMS.

TABLE 2. THREATS, VULNERABILITIES, AND ATTACKS

BAN		Data impairment, dropped data, data counterfeit, data disclosure, frequency jamming threat, data collision threat, compromised data routing threat (e.g. route spoofing, selective forwarding, sinkhole, Sybil, worm holes), data flooding threat, data eavesdropping threat, Denial of Service (DoS) attack [7, 8].
Comm. Network	**Wi-Fi**	Data eavesdropping, data tampering, unauthorised data access and spoofing, rogue access point, man-in-the-middle attack, DoS attack [9].
	3G/ 4G	Mobile-to-mobile attacks, patient's location and activity tracking attack, man-in-the-middle attack, data eavesdropping, scrambling attack, DoS attack [10].
Hospital		Physical security, unauthorised data access, social engineering attack, removable distribution media threat, data interception, faulty hardware, software attacks such as virus, worms, Trojans, and spyware, DoS attack [11, 12].

1) Body Area Network (BAN)

The main participant in the BAN is the patient, so lack of patient's awareness and training or negligence regarding use of sensors and devices may result in lost and stolen data and devices. For data collection and forwarding, the BAN utilises a patient's personal device such, as smartphone that is vulnerable against unauthorised access. The patient may install an application on smartphone that can enable the patient monitoring software to share data with other applications or may even become unresponsive.

Frequency jamming refers to a threat where an adversary intentionally interferes with frequencies of the BAN by using external device. The interference can make the devices and components in the network unresponsive leading into network blockage. Data collision is a threat at link layer communication in the BAN, where an adversary tries to corrupt the data frame by transmitting at same frequency which is used by the actual node. Data collision refers to a situation where the bits sequence in the data frame header is changed due to collision. At the receiving end, the error checking mechanism detects that as an error and rejects received data. Thus, a change in the data frame header is a threat to data availability in the BAN.

Compromised data routing is a threat at network layer communication in the BAN where an adversary can exploit the vulnerabilities of routing protocols to misdirect the data. Some possible routing related threats are spoofing, selective forwarding, sinkhole, Sybil, and worm holes. Route spoofing is a threat to data routing in BAN where an adversary may spoof the routing information. Route spoofing may create routing loops, isolate nodes in the network, and poise the source route. Route forwarding is a threat where an adversary may compromise a node in the network to allow only selective forwarding of medical parameters. Such forwarding can prevent the hospital from receiving complete medical data of the patient.

Sinkhole is an attack where an adversary can forge the routing table so that the nodes forward their data to a selected node. Once the network nodes starts forwarding their data to a compromised node, the adversary may exploit other vulnerabilities in the network to initiate other attacks. Sybil is a threat in which a node illegitimately claims multiple identities in a BAN. Sybil attack can be very damaging where an adversary can forge a network node to act maliciously by claiming false identities or by impersonating other devices with fraudulent intention. Wormhole is a threat that can be setup in active or passive modes. An adversary can selectively analyse network traffic and drop packets to cause disturbance in data flow over the network. In a wormhole attack, an adversary forges a node that can forward packets to a particular node in a tunnel. In reality the forwarding tunnel is a false route that gives control to an adversary to selectively drop or forward received packets.

Data flooding is an attack at the transport layer in the BAN, where an adversary can exhaust the memory resources by sending connection requests repeatedly. The flood of connection requests can consume the memory resource that develops resource constraints for genuine nodes. The lack of data synchronisation is a threat at transport layer in the BAN where an adversary can de-synchronise the pre-established connection by sending request for retransmission of missed frames. Repeated retransmission of frames can exhaust resources and degrade network performance. Data eavesdropping is a threat to patient's privacy and safety, where an adversary can intercept a message for further analysis. The intercepted messages may contain information related to patient's disease and physical location that can help the adversary to extract useful and confidential data.

The DoS is an attack that occurs when the overall traffic exceeds outside the total capacity of the system. The adversary can compromise nodes to initiate the DoS attack. DoS attack is very harmful for patient monitoring because unavailable system may affect the patient's life and safety. Threats such as jamming, exhaustion, flooding, desynchronisation, and compromised routing can cause DoS attack in a PMS.

2) Communication Network

The broadband communication channels are mostly used when patient is at locations such as home, nursing home, doctor's office, hospital, and transported to the hospital in an emergency scenario. The data transmission equipment such as patient's smartphone can perform data switch to the mobile networks that depends upon the patient's activity such as when visiting public places (transport, shop, café, etc.). While the patient's data is transferred using communication network, the adversary can exploit the vulnerabilities in network protocols, system applications, and operating system.

 ISBN: 978-1-61208-384-1

a) WiFi Communication Network Security Threats

Eavesdropping is a threat where the adversary can intercept the traffic to monitor patient's data. Data tampering is a threat where the adversary can modify the message contents of the intercepted data. Unauthorised access is a threat where the adversary can access patient's data and network resources using patient's identity. The smartphone can connect to a rouge access point that is set up by the adversary to fully control patient's data for malicious use. The adversary can disable the network from serving the patient through DoS attack. Jamming is a common type of this attack, wherein the adversary can use external frequency source to emit random radio signal or let out frequent packets transmission to keep the channel busy, so that the receiver can only receive rather than transmitting. While the smartphone transmits data towards hospital through access point, the adversary can exploit man-in-the-middle attack. The adversary can impersonate the patient to gain access into information and can also inject false data.

b) 3G/4G Communication Network Security Threats

The 4G network offers IP based communication for smartphones through which the devices can directly exchange data. In such a case, smartphone-to-smartphone attack is possible, wherein a compromised smartphone can aim at draining the battery of targeted smartphone through continuous network connection. Data eavesdropping is a threat in 3G/4G networks where the adversary analyse the traffic within a range of particular base station to monitor particular node. An adversary may interrupt management data exchanged between smartphone and base station to extract information regarding encryption scheme. Further, messages intercepted from targeted patient's smartphone can disclose confidential information. The mobility scenario supports patient's movement across different locations. As the patient moves from one location to another, sent messages can be used by an adversary to collect, aggregate, and analyse information regarding patient's movements and activities. Revealing the patient's location, movement, and activity tracking is a threat to patient's privacy. Before patient's smartphone starts transmitting data, it performs preliminary signalling operation with the serving base station. Signalling operations include authentication and key management, registration, and IP-based connection establishment. The adversary can initiate a signalling attack on the serving base station by actuating extra state signals that clog the base station. The excessive burden on the base station results in DoS attacks and the patient's smartphone cannot send data due to base station unavailability. A Man-in-the-middle attack can occur when the adversary exploits the vulnerabilities of the initial handshake between patient's smartphone and the base station. The adversary deceives the smartphone by appearing as a legitimate base station, can eavesdrop on all communication, and insert fake messages. Scrambling is jamming attack on radio frequency for short intervals of time during transmission of control or management information frames. This attack interrupts the communication that can prevent the patient's smartphone from sending data causing availability issue.

3) Hospital/Healthcare Enterprise Threats

An information system at the hospital receives patient's data. Both the patient's data and information system can be attacked from inside and outside of hospital network. An adversary can access the information system to remove and change patient's data or interrupt the system operations. In case of system interruption, the patient's data become unavailable to healthcare personnel that can cause serious harm to the patient's treatment. A malware can infect and propagate to the whole hospital network that can cause unavailability and disruption. Changes and updates in software configuration of patient monitoring servers can unstable the system configuration, resulting in system malfunctioning and communication interruption. The users who are not related to PMS may also browse machines linked to the PMS through the hospital wide network to perform malicious activities. Due to weak physical security procedures at the hospital, the unauthorised users can gain access into the information system. Even for personal gains, the authorised users can also disclose patient's data to concerned parties such as Health Insurance Company. Without proper awareness training, the healthcare personnel are vulnerable to social engineering attacks from adversary for obtaining patient's data. Without having a proper policy for need to know, the administrators responsible only for network management may also access patient's data and use it for wrong purposes. Removable distribution media is also a threat because it can be used to steal information and to propagate viruses in a PMS. The data exchange among computers of PMS through hospital LAN is vulnerable to interception by adversary for data sniffing. The hospital LAN is vulnerable to DoS attack that can jeopardise a PMS. Third party maintenance staff may install contaminated software upgrades that propagates virus into the system. Hardware issues, such as faulty devices can cause interruption in a PMS.

IV. RELATED WORK IN SECURITY OF EHEALTH SYSTEM

The security aspects of eHealth system have been an active research field among researchers. While discussing the security issues in an eHealth system, the existing literature mostly focus on either BAN or healthcare enterprise network. There is a lack of specific security analysis for an eHealth system where the security aspects of BAN, communication network, and healthcare enterprise are combined and treated for the whole PMS. A summary of related research efforts towards security of eHealth system are briefly highlighted in this section.

A case study to assess security risks and threats in a wireless BAN for the real time remote health monitoring system is presented by Lim et al. [13]. The authors assessed the security risk based on the critical needs of acknowledge risks and threats in real time eHealth system. Don et al. [14] described a conceptual architecture of activity based risk analysis for monitoring the health status of the patient. They used event filtration and aggregation based on the concept of situation awareness while utilising smartphone to transfer the data collected through sensors. They conclude that security

 ISBN: 978-1-61208-384-1

issues such as miss utilisation of the device, authentication, QoS, and reliability need proper solutions. Maglogiannis et al. [15] presented a model approach for performing risk analysis study of healthcare information system. They used Bayesian network to model the interrelationship between assets, threats, and vulnerabilities of healthcare information system in their methodology. They identified high rank risks and suggested several countermeasures to limit the vulnerabilities of the healthcare network operations. Shin [16] designed a framework and provided risk analysis for remote health monitoring systems. The author proposed a health monitoring architecture to provide security services such as authentication, audit, key management, and data fusion using unreliable personal mobile devices. However, they suggested that the concerns about privacy and information quality may obstruct the development of eHealth systems.

Security and privacy requirements in wireless BAN are surveyed and analysed by Li et al. [7]. In particular, the authors looked into security aspects such as secure distributed data storage and fine grained distributed data access control. They suggested that the security, usability, and privacy protection of the data collected from patient is a major concern either it is in storage or transmission. Saleem et al. [8] highlighted the security requirements and DoS attacks in WBAN. According to the authors, it is not appropriate and secure to directly adopt IEEE 802.15.4 security framework for WBAN.

Kargl et al. [17] analysed the security and privacy requirements of eHealth system. They presented an eHealth system model to discuss security threats and attacks, requirements, and recommended guidelines for security mechanisms. The authors analysed some healthcare projects to highlight security and privacy issues in healthcare system [18]. They presented a review of existing schemes to provide security solutions in healthcare scenario. Shahri et al. [12] studied the possible threats on health information system and presented a tree model for identification of threats to perform risk assessment. Leister et al. [19] presented the threat assessment of mobile PMS associated to both short range and long range mobile wireless communication infrastructure. In order to determine the security requirements, they emphasised mainly on biomedical sensor networks. Kotz [20] examined and developed taxonomy of privacy related threats to mobile health technologies. The technologies that could support privacy sensitive mobile health system are also discussed.

Leister et al. [21] presented a framework to evaluate adaptive security for the IoT in eHealth and developed scenarios to access the adaptive security solutions. The authors suggested that security and QoS mechanisms are interrelated and may impact each other. The security objectives of eHealth IoT applications and their adaptive security decision making needs are analysed by Savola et al. [22]. The authors proposed a high level adaptive security mechanism based on the security metrics to cope with that security challenges and issues.

The trend in the evolution of 4G wireless communications and its security is explored by Rahman et al. [23]. The authors introduced the system architecture, security requirements, and security issues of 4G wireless networks. Seddigh [24] studied the security issues in 4G networks. The study focused on the vulnerabilities and attacks at different layers in 4G network. The authors highlighted the security weaknesses in 4G networks and gave few suggestions on security issues and development of appropriate countermeasures. The inclusion of the smartphone into remote PMS can reduce cost and increase flexibility, but smartphone platform does not meet security protection requirements of international standards for health data [25].

V. DISCUSSIONS AND SECURITY RECOMMENDATIONS

The security mechanisms for the IoT in eHealth should be generic enough to avoid interoperability issues among various platforms without affecting a system's usability. The existing security mechanisms that are developed for traditional computer networks may not be very well suited for the IoT in eHealth. One of the reasons for lesser suitability could be the dynamic and heterogeneous environment offered by the IoT, which can allow the patient to enjoy mobility scenarios. As the physical parameters of the patient are changed due to the mobility scenarios, the security requirements, vulnerabilities, and threats may also vary. Another reason could be resource constraints of the sensors, such as lack of storage capacity and processing power that may cause difficulties in terms of implementing traditional security mechanisms. The adaptive security mechanisms may work better than static security mechanisms for such resource constraints and dynamic environments. Adaptive security mechanisms have the potential to adjust security parameters to the level of detected threats, available energy and memory, and application requirements [26]. The adaptive security terminology refers to a situation, where security mechanisms or policies can change in automated or semi-automated way in response to events [27]. According to Abie [28], monitor, analyser, adapter, and adaptive knowledge database are the core components of the adaptive security model. The monitor collects security attributes and environmental data. The analyser determines the current security levels and matches it against the security requirements. The adapter decides by using a planning function about how and what security parameters need to be changed for adaptation.

Adaptive security mechanisms may provide better security against various security attacks in the PMS. For instance, encryption mechanisms are used to counter data confidentiality issues. Mostly, the strength of the encryption mechanisms depends upon the complexity of the algorithm requiring sufficient storage space and processing power. Such algorithms may drain sensor's battery making it unavailable. Thus, lightweight adaptive encryption mechanisms may be a better choice. The encryption mechanism may adapt to various key lengths based on the available energy level in the battery, patient's current location, and current threat level. The authentication mechanisms can provide the data and patient's proof of origin. The traditional authentication mechanisms built on passwords, tokens, and biometric modalities can be made adaptive using context information from the external environment and inside the system's environ-

 ISBN: 978-1-61208-384-1

ment. The context aware and adaptive authentication mechanisms could provide more flexibility to the whole PMS.

The patient's smartphone is used to collect and process vital signs for further transmission. Smartphone is a mobile device that inherits the risk of lost device. Therefore, the patient should be vigilant towards physical security of smartphone. For the sake of patient's convenience and ease in system's usability, one can ignore the login procedure that is necessary for patient/device authentication. Unencrypted data in the smartphone can be a threat to patient's privacy so clear text storage and transmission should be avoided. Software attacks such as malware, virus, worms, Trojan, spyware, and adware can infect the smartphone resulting in leaked and lost data. The smartphone should be equipped with security mechanism to guard against such threats. The smartphone has constraints in terms of energy and processing power so such security mechanisms that require much processing power may drain smartphone battery. Therefore, light weight security mechanisms should be encouraged to avoid such issue.

VI. CONCLUSION AND FUTURE WORK

The existing healthcare system can gain a lot from the IoT in terms of patient monitoring outside the hospital environment. However, security issues require flexible, context aware, and adaptive security mechanisms. While making a security decision, the security mechanisms should incorporate security requirements, threats, and attacks based on the patient's location and environmental context. We provided a security analysis of PMS for the IoT in eHealth. However, there is a need for a method that could determine the threat and attack level in a given context and adjust security mechanisms to balance system usability and quality of communication. In future, we plan to build a framework to develop context aware adaptive security mechanisms for the IoT in eHealth with a tendency to adapt a security decisions based on the given threat level.

ACKNOWLEDGMENT

The work presented here has been carried out in the research project ASSET – Adaptive Security for Smart Internet of Things in eHealth (2012–2015) funded by The Research Council of Norway.

REFERENCES

[1] K. Habib and W. Leister, "Adaptive Security for the Internet of Things Reference Model", 6th Norwegian Information Security Conference, NISK 2013, pp. 13-24.

[2] Vision and Challenges for Realizing the Internet of Things, European Union, pp. 1-236, 2010.

[3] Future Internet Strategic Research Agenda, Version 1.1, European Future Internet X-ETP Group, pp. 1-73, 2010.

[4] H. Abie and I. Balasingham, "Risk-Based Adaptive Security for Smart IoT in eHealth", BodyNets, 2012, pp. 269-275.

[5] K. Habib, A. Torjusen, and W. Leister, "A Novel Authentication Framework Based on Biometric and Radio Fingerprinting for the IoT in eHealth," SMART 2014, July 20 - 24, 2014, pp. 32-37.

[6] Minimum Security Requirements for Federal Information and Information Systems, NIST, FIPS PUB 200, 2006.

[7] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," Wireless Communications, IEEE, vol.17, no.1, pp. 51-58, February. 2010.

[8] S. Saleem, S. Ullah, and K. S. Kwak, "A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks," Sensors; 11(2): pp. 1383-1395, 2011.

[9] M. M. Noor and W. H. Hassan, "Wireless Networks: Developments, Threats and Countermeasures," (IJDIWC) 3(1): pp. 119-134, 2013.

[10] B. Matt and C. C. Li, "A Survey of the Security and Threats of the IMT-Advanced Requirements for 4G Standards," IEEE Conference Anthology, 1-8 January. 2013, pp.1-5.

[11] Case Study, Threat Analysis of Medical Device. [Online]. http://www.ptatechnologies.com/default.htm

[12] A. B. Shahri and Z. Ismail, "A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS," Journal of Inf. Sec., Vol. 3 No. 2, pp. 169-176, 2012.

[13] S. Lim, T. H. Oh, and Y. B. Choi, T. Lakshman, "Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring," SUTC 2010, 2010, pp. 327-332.

[14] S. Don, E. Choi, and D. Min, "A Situation Aware Framework for Activity Based Risk Analysis of Patient Monitoring System," iCAST, Sep. 2011, pp. 15-19.

[15] I. Maglogiannis and E. Zafiropoulos, "Modeling Risk in Distributed Healthcare Information Systems," EMBS 2006, Aug. 30 - Sept. 3 2006, pp. 5447-5450.

[16] M. Shin, "Secure Remote Health Monitoring with Unreliable Mobile Devices," Journal of Biomedicine and Biotechnology, Article ID 546021, 5 pages, 2012.

[17] F. Kargl, E. Lawrence, M. Fischer, and Y. Y. Lim, "Security, Privacy and Legal Issues in Pervasive eHealth Monitoring Systems," ICMB, 7-8 July. 2008, pp. 296-304.

[18] P. Kumar and H-J. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey," Sensors: 12(1) pp. 55-91, 2012.

[19] W. Leister, H. Abie, A-K. Groven, T. Fretland, and I. Balasingham, "Threat Assessment of Wireless Patient Monitoring Systems," ICTTA, 7-11 April. 2008, pp.1-6.

[20] D. Kotz, "A threat taxonomy for mHealth privacy," COMSNETS, 4-8 Jan. 2011, pp. 1-6.

[21] W. Leister, M. Hamdi, H. Abie, and S. Poslad, "An Evaluation Scenario for Adaptive Security in eHealth," PESARO, IARIA, 23-27 February. 2014, pp. 6-11.

[22] R. M. Savola, H. Abie, and M. Sihvonen, "Towards Metrics-Driven Adaptive Security Management in e-Health IoT Applications," ICST, 2012, pp. 276-281.

[23] A. Rahman and K. Sharma, "Fourth Generation of Mobile Communication Network: Evolution, Prospects, Objectives, Challenges and Security," IJRIM, Vol. 2, Issue 2, 2012.

[24] N. Seddigh, B. Nandy, R. Makkar, and J. F. Beaumont, "Security advances and challenges in 4G wireless networks," PST, 17-19 Aug. 2010, pp. 62-71.

[25] C. C. Tan, L. Bai, D. S. Mastrogiannis, and J. Wu, "Security Analysis of Emerging Remote Obstetrics Monitoring Systems," Healthcom , 10-13 Oct. 2012, pp. 329-334.

[26] L. Gheorghe, R. Rughinis, and N. Tapus, "Adaptive Security Framework for Wireless Sensor Networks," INCoS, 19-21 Sept. 2012, pp. 636-641.

[27] L. Marcus, "Introduction to Logical Foundations of an Adaptive Security Infrastructure," July, 2004, pp.1-12.

[28] H. Abie, "Adaptive Security and Trust Management for Autonomic Message-Oriented Middleware," MASS, 12-15 Oct. 2009, pp. 810-817.

 ISBN: 978-1-61208-384-1