Threats Identification for the Smart Internet of Things in eHealth and Adaptive Security Countermeasures

Kashif Habib
Norwegian Computing Center
Oslo, Norway
Kashif.Sheikh@nr.no

Wolfgang Leister
Norwegian Computing Center
Oslo, Norway
Wolfgang.Leister@nr.no

***Abstract*— The Things in the smart Internet of Things (IoT) depend more on self decision making abilities instead of relying on human interventions. In the IoT, static security mechanisms are not well suited to handle all security risks sufficiently. A security mechanism can be considered static if it is developed with fixed security measures whereas an adaptive security mechanism can be considered dynamic if it can continuously monitor, analyse, and reassess a security risk at runtime. Adaptive security mechanisms can be a better choice to secure dynamic and heterogeneous computing systems in the IoT. This paper presents a patient monitoring scenario using the smart IoT and aims at highlighting all important assets, vulnerabilities, and threats that can harm assets and disrupt eHealth systems. We describe adaptive security and introduce a concept of adaptive security countermeasures for the smart IoT in eHealth.**

Keywords—IoT; eHealth; adaptive security; threats.

I. INTRODUCTION

A patient Monitoring System (PMS) is comprised of three segments: (i) Body Area Network (BAN), (ii) communication network, (iii) hospitals and health care enterprises [1]. As depicted in Fig. 1, the BAN includes the actual patient, medical sensors, and the patient's smartphone. The devices in the BAN are usually configured by clinical staff for data collection. The patient's smartphone collects the monitored information which is then forwarded to the hospital via communication networks. These communication networks including broadband network and 3G/4G networks connect the BAN with a hospital network. Hospital and the healthcare enterprise evaluate the Patient's medical data and respond accordingly. The healthcare enterprises 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. The patient monitoring sessions keep the patient connected with healthcare workers, even when the patient is outside the hospital environment.

Many eHealth systems are currently protected by using static security mechanisms in which a system's security goals and requirements are not continuously reassessed based on the dynamically changing environments. A security mechanism can be considered static if it is developed with fixed security measures and these security measures remains unchanged throughout its lifetime. Static security mechanisms may not be adequate to protect systems that are exposed to various operating conditions such as the smart IoT. The IoT's are mostly comprised of different hardware configurations, variable user preferences, multiple access networks, and diverse physical environments. In such a dynamic system, a security mechanism should be capable of monitoring all aspects of the system that can help to perform adaptation [2]. Thus, the problem of security management is quite complex in a dynamic environment; therefore adaptive security concepts can potentially solve security related problems.

Answers to the following questions may provide a basis to determine the suitability of adaptive security to protect the smart IoT in eHealth against threats.

1) Which security threats can harm the smart IoT in eHealth?
2) How can we acquire knowledge about threats?
3) What is the potential harm for not protecting the IoT in eHealth against security threats?

In the recent past, there has been a significant growth in the research devoted to the field of adaptive security [3]. So far, the research in adaptive security has not only covered a broad range of different application areas [4], but there have been also significant advancements in terms of understanding theoretical issues and developing technical solutions that made the realisation of adaptive security possible [5].

In order to elaborate the necessary concepts, this paper presents threat detection and prevention for the smart IoT in eHealth. Related research is highlighted in Section II. Section III describes threat detection and prevention using adaptive security mechanisms. Finally, Section IV concludes the paper.

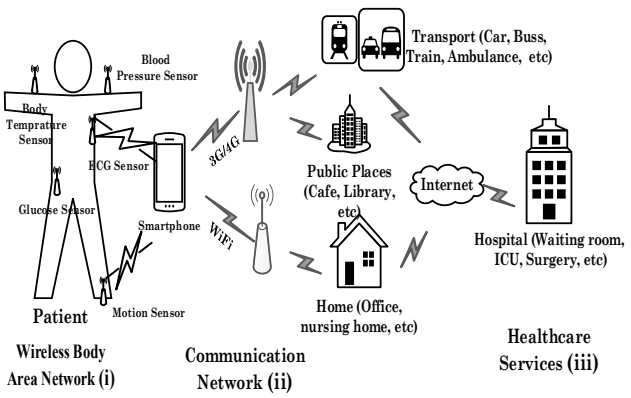

Fig. 1. Patient monitoring scenario

Citation: Kashif Habib and Wolfgang Leister: "Threats identification for the smart Internet of Things in eHealth and adaptive security countermeasures," Proc. 7th International Conference on New Technologies, Mobility and Security (NTMS), Paris, 2015, pp. 1-5. doi: 10.1109/NTMS.2015.7266525

TABLE I. ADAPTIVE SECURTY RESEARCH

Research Projects / Techniques	Adaptive Security Description
An Evaluation Framework for Adaptive Security for the IoT in eHealth [9].	A framework for the assessment and validation of context-aware adaptive security solutions for the IoT in eHealth.
Towards Run-Time Verification of Adaptive Security for IoT in eHealth [10].	Integrates run-time verification enablers in the feedback adaptation loop of the adaptive security framework for IoT in the eHealth settings.
Intrusion detection inter-component adaptive negotiation [11].	The intrusion detection system (IDS) evolves and as the environment changes.
Game-Based Adaptive Security in the IoT for eHealth [12].	Proposes a game based model for adaptive security in the IoT for eHealth applications.
Context sensitive adaptive authentication [13].	Adaptively authenticate a user on the basis of the location of his sensed identity.
Towards self-protecting ubiquitous systems: monitoring trust-based interactions [14].	A monitor architecture development to enable self-protective actions. The monitor is independent of application specific factors, requiring the application to specify its concerns in terms of both cost and trust observables.
GEMOM Project: Robust, Secure, Self-Adaptive and Resilient Messaging Middleware for Business Critical Systems [15].	This study presents a self-adaptive and resilient messaging middleware that provides solutions to overcome limitations in self-adaptability, and assurance against security threats and erroneous input during run-time in the face of changing threats.
Self-protection for Distributed Component-Based Applications [16].	It describes a self-protected system, similarly to a natural immune system which has the ability to detect the intrusion of foreign elements and react while it is still in progress.
Adaptive Rule-Based Malware Detection Employing Learning Classifier Systems [17].	Self-training adaptive malware detection system which dynamically evolves detection rules. Improvement in the accuracy of malware detection using learning classifier system.
Testbed for Adaptive Security for IoT in eHealth [18].	Describes the setup of a test bed for adaptive security for the IoT in eHealth.
Vigilante: end-to-end containment of internet worms [19].	Automatically contain worms, It not only depends upon using network-level information about the worms but also relies on collaborative worm detection at end hosts.
Metrics-Driven Security Objective Decomposition for an E-Health Application with Adaptive Security Management [20].	Developed a context-aware Markov game theoretic model for security metrics risk impact assessment to measurably evaluate and validate the run-time adaptivity of IoT security solutions
Adaptive trust negotiation and access control [21].	Adaptive access control using TrustBuilder and generic authorization and access-control application program interface to create a system with more flexibility and responsiveness to attacks.
Multi-Level Intrusion Detection System (ML-IDS) [22].	Multi-level IDS that uses autonomic computing to automate the control and management of ML-IDS.
Applying component-based design to self-protection of ubiquitous systems [23].	An integrated solution for self-protected pervasive systems in terms of a 3-level architecture containing two control loops at the network and node levels.
Vulnerability Assessment in Autonomic Networks and Services [24].	A survey to analyse methods and techniques contributing to the discovery, the description and the detection of vulnerabilities.

II. RELATED RESEARCH

The development of adaptive security mechanisms has been an active research field [6, 7, 8]. Many adaptive security approaches have been proposed in the recent past with an effort to enhance the effectiveness of security services such as, intrusion detection and prevention, malware detection, authentication, access control, vulnerability detection, and encryption, etc. Related research efforts in existing approaches are briefly presented in Table I. However, we found that there is a lack of work towards developing adaptive security approaches for securing the eHealth domain in the IoT.

III. THREAT DETECTION AND PREVENTION

A. Assets, vulnerabilities, and threat identification

To better understand the associated risk in the IoT based eHealth system, we identify key assets (personal, physical, information, and intangible assets) which are depicted in Table II. The assets identification is based on the eHealth scenario described earlier.

Once the key system assets are identified, next step is to identify the vulnerabilities that can be exploited by a threat agent to harm a system [25]. Table III shows vulnerabilities and affected assets if these vulnerabilities are exploited. Threats can be launched against the PMS by exploiting the vulnerabilities, as highlighted in Table IV.

TABLE II. ASSETS FOR THE IOT IN EHEALTH

Asset Name	Asset Description	Asset Custodian	Asset Location
A1:Patient	A person requiring RPM service	Patient	Home, outdoor, hospital.
A2:Medical staff	Hospital employees	Healthcare enterprise	Hospital
A3:Technical staff	Hospital employees	Healthcare enterprise	Hospital
A4:Patient monitoring devices	Medical sensors to monitor patient's health status	Patient / Healthcare enterprise	Home, outdoor, hospital.
A5:Smartphone	Collects data from sensors	Patient	Home, outdoor, hospital.
A6: Sensors to smartphone connectivity	Connects sensors and smartphone	Patient	Home, outdoor, hospital.
A7:Smartphone to Wi-Fi connectivity	Connection between smartphone and Wi-Fi	Broadband network provider	Home, hospital.
A8:Wi-Fi to Internet connectivity	Connects broadband network with the Internet	Broadband network provider	Home
A9:Smartphone to 3G connectivity	Connects smartphone with a mobile network	Mobile network provider	Home, outdoor, hospital.
A10:Hospital IT system	The IT equipment at the hospital	Healthcare enterprise	Hospital.
A11:Patient's data records	Patient's health information	Healthcare enterprise	Hospital.
A12:Mobility	Movement across different locations	Patient	Home, outdoor, hospital.
A13:Hosptal data centre	Collect patient's data and provides responses	Healthcare enterprise	Hospital

TABLE III. VULNERABILITIES FOR THE IOT IN EHEALTH

Vulnerabilities	Affected Assets	Description
V1:Implementation deficiencies	A4, A5, A6, A7, A8, A9, A10, A12.	Inadequate implementations of system components can cause malfunctioning
V2:Lack of usability	A4, A5.	Patient's inability to manage monitoring devices due to complexity
V3:Unprotected environment	A4, A5.	Use of monitoring devices in public places
V4:Inadequate interoperability between devices	A4, A5, A6, A7, A8, A9.	Uncertified devices can cause interoperability issues.
V5:Low performance of devices	A4, A5.	Limited memory and processing power in monitoring devices can deteriorate performance.
V6:Unprotected communication channels	A6, A7, A8, A9, A10, A12.	Publically available channels can allow an attacker to intercept communication.
V7:Absence of authentication mechanism	A4, A5, A6, A7, A8, A9, A10, A11.	An attacker can get unauthorised access to system and data.
V8:Absence of access control mechanism	A4, A5, A10, A11, A12, A13.	An attacker can get unauthorised access to system and data.
V9:Patient's insufficient awareness about devices usage	A4, A5, A6, A7, A8, A9.	Patient's inability to use the devices correctly can interrupt the monitoring system.
V10:Staff's insufficient awareness about devices usage	A2, A3, A4, A5, A6, A7, A8, A9, A10, A12, A13.	Staff's inadequate training may allow an attacker to easily exploit the vulnerabilities.
V11:Succeptible to malwares	A4, A5, A10, A11, A12, A13.	Infrequent updates of security patches can expose the system against malwares.
V12:Plain text data storage	A4, A5, A10, A11, A13.	Clear text data can allow an attacker to revel patient's information.
V13:Wireless communication interception	A6, A7, A8, A9, A10.	An attacker can intercept communication to reveal and modify patient's data.
V14:Data traceability	A4, A5, A10, A11, A13.	Lack of data traceability mechanism can allow an attacker to use patient's data for malicious use.
V15:Data linkability	A10, A11, A13.	Data linkability may allow an attacker to identify a patient.

TABLE IV. THREATS FOR THE IOT IN EHEALTH

Threats/ Attacks	Affected Assets	Impact Description
T1: Data impairment	A4, A5, A10, A11, A13.	Degradation of signal quality, bit errors, delay distortion, noise, and attenuation.
T2: Dropped data	A4, A5, A6, A7, A8, A9, A11, A12, A13.	An attacker can deliberately drop data exchanged between; sensors and smartphone, smartphone and hospital network.
T3: Data counterfeit	A11.	An attacker can insert counterfeit content into a network through a compromised node.
T4: Data disclosure	A1, A10, A11, A13.	Accidental or intentional data sharing with unauthorised users.
T5: Frequency jamming	A3, A4, A5, A6, A7, A8, A9, A12.	The interference can make the devices and components in the network unresponsive leading into network blockage.
T6: Data collision	A4, A6, A7, A8, A9, A11, A13.	Bit sequence of frame header can change due to collision. Error checking mechanism detects that as an error and rejects received data.
T7: Compromised data routing	A3, A4, A5, A6, A7, A8, A9, A11, A12.	An attacker can exploit vulnerabilities of routing protocols to misdirect the data. (e.g., route spoofing, selective forwarding, Sybil, worm holes)
T8: Data flooding	A3, A4, A5, A6, A7, A8, A9, A11, A12.	An attacker can exhaust memory resources by sending connection requests repeatedly. The flood of requests can consume memory resources.
T9: Data eavesdropping	A4, A5, A10, A11, A12, A13.	The intercepted messages may contain information related to patient's disease and physical locations.
T10: Denial of Service (DoS)	A1, A3, A4, A5, A6, A7, A8, A9, A10, A11, A12, A13.	An adversary can initiate a signalling attack on a base station by actuating extra state signals that clog the base station. A smartphone cannot send data due to base station unavailability. A DoS attack on hospital LAN can harm a PMS.
T11:Data tempering	A3, A5, A10, A11.	An attacker can modify the message contents of the intercepted data.
T12: Unauthorised access	A4, A5, A10, A11, A13.	An attacker can access patient's data and network resources using patient's identity.
T13: Data spoofing	A4, A5, A11, A13.	An attacker can send fabricated data from a fake source.
T14: Device spoofing	A4, A5, A6, A7, A8, A9, A11, A12.	An attacker can use illegitimate device to collects data from sensors and transfers to the hospital.
T15: Rouge access point	A4, A5, A7, A8, A11, A12.	The smartphone can connect to a rouge access point that is set up by the adversary to fully control patient's data.
T16: Man-in-the-middle	A4, A5, A8, A9, A11, A12.	An attacker can exploit the vulnerabilities of the initial handshake between patient's smartphone and base station.
T17: Data scrambling	A6, A7, A8, A11, A13.	Scrambling is jamming attack on radio frequency during transmission of control or management information frames.
T18:Removable media threat	A10, A11, A13.	Removable distribution media can be used to steal information and to propagate viruses in a PMS.
T19: Physical security	A4, A5, A10, A11, A12, A13.	Smartphone inherits the risk of lost device. Physical security requires restricted physical access to the medical servers.
T20: Social engineering	A2, A3, A11, A13.	An adversary can obtain patient data from healthcare personnel using social engineering techniques.
T21: software attacks (malware, viruses, worms, Trojans, spyware)	A3, A4, A5, A10, A11, A13.	Changes and updates in software configuration of patient monitoring devices can cause system malfunctioning. Paramedic staff may install contaminated software upgrades that propagates virus into the system. 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.
T22: Faulty hardware	A4, A5, A6, A7, A8, A10.	Hardware issues such as faulty devices can cause interruption in a PMS.
T23: Data interception	A4, A5, A10, A12, A13.	An attacker can intercept the data at; sensors to smartphone, smartphone to hospital network, and hospital LAN.

B. Threat detection and prevention using adaptive security

The IoT in eHealth has been evolving in the recent past mainly due to the increased use of mobile technologies. At the same time, security threats are advancing towards dynamic and evolving behaviour. Primarily, the goals and objectives of attacks and countermeasures are opposed to each other. Security attacks aim at manipulating an information system's weaknesses, whereas countermeasures try to protect assets. In case of evolving threats, protection of eHealth system assets highly depends upon system abilities to detect and understand environmental changes. Detecting environmental changes and adjusting the system parameters based upon those changes can be referred to as adaptation. Adaptation procedures analyse system's internal and external conditions which they lean through monitoring functions. Fig. 2 adapted from the risk assessment domain [26] illustrates an abstract relationship between assets, vulnerabilities, threats, risk, security requirements, and adaptive security for the IoT in eHealth.

The fundamental concepts of adaptive security have been borrowed from the human autonomic nervous system [27], autonomic computing [28], and self-adaptive software [29] to develop self-managing security systems. Adaptive systems tend to minimise human interaction through automatic system processes. Like the human nervous system, adaptive systems have a tendency to protect themselves from threats, recover from faults, and reconfigure themselves with environmental changes [28]. A system's internal conditions and external environmental conditions can impact system's performance. Primarily, adaptive systems use various sensors and actuators to sense internal and external environmental changes in a system's operating environment. Adaptive systems try to countermeasure the effects of changes in the environment by changing the system's operating parameters [30]. The self-adaptive software is designed to develop a system that can adjust its attributes when there is a change in the self and in the context of a system, where self means the whole system and context refers to everything in the operating environment which can affect system behaviour [29]. The components of the adaptive security are monitor, analyser, adapter, and adaptive knowledge database [31]. The monitor function collects security related information, the analyser finds out the adaptation requirements, and the adapter determines the adaptation plan for execution.

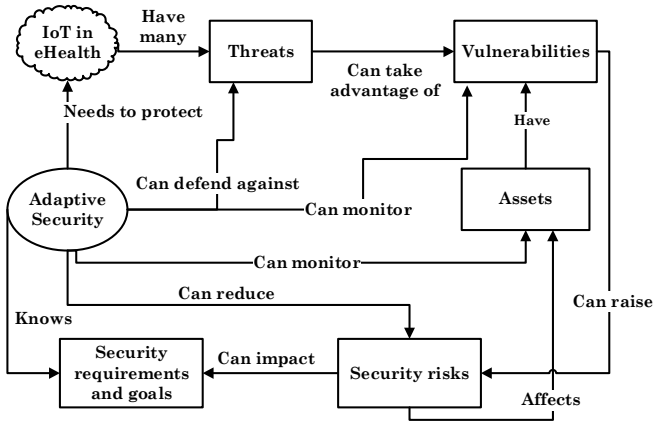

Fig. 2. Relational concept

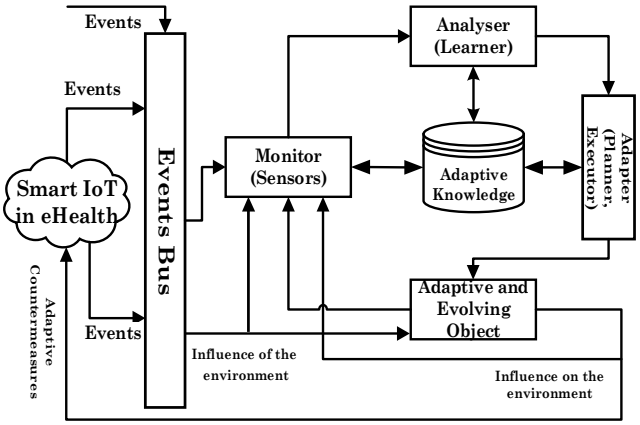

Fig. 3. Adaptive threat detection and prevention for the IoT in eHealth

As depicted in Fig. 3 adapted from [15], security events in the internal and external environment can be gathered using various environmental sensors and various system monitoring components in the devices. These events are then further analysed by an analyser function to detect if the current event is a threat to a system. The analyser determines the effect of threat on system performance that is further handled by a planning function which plans an appropriate action. The planning function can use a knowledge base or learning mechanism to decide a new action from a set of available actions. The action decided by a planning function is executed by an execution function to bring back system's behaviour into balance state within the changed environment. The knowledge database serves as reference knowledge for all phases of adaptation process and at the same time each phase also stores its processed information in it for use in next cycle.

A threat can demonstrate its adapting features mainly through two aspects, i.e., threat behaviour and a change or alteration in form or qualities [32]. Threat behaviour means that a threat such as malware, virus, and spyware can take different actions to achieve adaptability. Whereas, change or alteration in threat qualities means that a threat can achieve adaptability through changes in its structure. Different actions that a threat uses to exploit vulnerabilities show threat behavior. If a threat agent uses same actions over a period of time, it is possible that a defence mechanism would be able to counter such threats. Therefore, adapting threats seeks to modify their behaviour so that it becomes difficult for a defence mechanism to easily detect them. Usually, vulnerability can be exploited using various methods to attack an information system. Hence, adapting threats agent can use new actions through attack vector modification.

The IoT in eHealth have energy constraints and it can happen that a sensor node can become unavailable due to empty battery. In such situation, self-configuration network architecture can allow a new sensor node to join communication path. When a new sensor node joins or an old sensor node leaves, adaptive security mechanism should not only be able to detect configurational changes but also continue providing same security level in the face of configurational changes. Along with detecting configurational changes, an

adaptive security mechanism can maintain knowledge base about network state, traffic patterns, and sensor nodes behaviour. A knowledge base can assist to detect anomalies in network state, traffic patterns, and sensor nodes behaviour. Anomaly detection features can detect a threat and respond subsequently. A response mechanism may include changes in cryptographic keys lengths, changes in routing tables, and changes in access control and authentication procedures. The IoT in eHealth is always subject to unanticipated attacks so adaptive security mechanisms should have threat learning and analysing capabilities enabling them to continue protecting information system through adjusting security levels.

IV. CONCLUSION

As dynamic information system such as the IoT in eHealth experience changing threat profile so it can be difficult for a static security mechanism to continue securing the system during its life cycle. Based on our findings in this article, we have shown that adaptive security mechanisms offer opportunities to countermeasure various attacks in the IoT for eHealth through continuous monitoring and analysis functions. Adaptive security mechanisms can potentially modify their behaviour at runtime and adjust security levels based on the given threat level. Therefore, security mechanisms for the IoT in eHealth should be developed using adaptive approach.

ACKNOWLEDGMENT

The work presented here has been carried out in the re-search project ASSET – Adaptive Security for Smart Internet of Things in eHealth (2012–2015) funded by The Research Council of Norway. This paper has been accepted for SmartCity Workshop 2015 held in conjunction with NTMS'2015.

REFERENCES

[1] K. Habib, A. Torjusen, and W. Leister, “Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth,” In proceedings of eTelemed 2015, The Seventh International Conference on eHealth, Telemedicine, and Social Medicine, 2015, pp. 73-78.

[2] E. Yuan, N. Esfahani, and S. Malek, “A Systematic Survey of Self-Protecting Software Systems,” ACM Trans. Auton. Adapt. Syst. 8, 4, Article 17, pp. 41, January 2014.

[3] F.T. Sheldon, S.G. Batsell, S.J. Prowell, and M.A. Langston, "Position Statement: Methodology to Support Dependable Survivable Cyber-Secure Infrastructures," HICSS '05, 2005, pp. -1-10.

[4] S-h. Park, W. Kim, and D-k. Kim,“Autonomic Protection System Using Adaptive Security Policy Computational Science and Its Applications,” ICCSA 2004, Springer Berlin Heidelberg, 3045, 2004, PP. 896-905.

[5] G. Qu, O.A. Rawashdeh, and D. Che, “Self-protection against attacks in an autonomic computing environment,” I. J. Comput. Appl. 17, 4. 2010, pp. 250–256.

[6] K. Habib, and W. Leister, “Adaptive Security for the Internet of Things Reference Model,” The Sixth Norwegian Information Security Conference, NISK’13, November 18-20, 2013, pp. 13-24.

[7] A. Evesti, and E. Ovaska, “Comparison of Adaptive Information Security Approaches,” ISRN Artificial Intelligence, vol. 2013, Article ID 482949, 2013, pp. 1-18.

[8] M. Emami-Taba, M. Amoui, and L. Tahvildari, “On the Road to Holistic Decision Making in Adaptive Security,” Technology Innovation Management Review, Talent First Network, 3, 2013, pp. 59-64.

[9] W. Leister, M. Hamdi, H. Abie, S. Poslad, and A. Torjusen, “An Evaluation Framework for Adaptive Security for the IoT in eHealth”, International Journal on Advances in Security, 7(3&4), 2014, pp 93-109.

[10] A. Torjusen, H. Abie, E. Paintsil, D. Trcek, and Å. Skomedal, “Towards Run-Time Verification of Adaptive Security for IoT in eHealth”, ECSAW, August 25 – 29, 2014, pp. 1-8.

[11] R. Feiertag et al., “Intrusion detection inter-component adaptive negotiation,” Computer Networks, Volume 34, Issue 4, October 2000, pp.605-621.

[12] M. Hamdi and H. Abie, “Game-Based Adaptive Security in the Internet of Things for eHealth”, IEEE ICC, 10-14 June, 2014, pp. 920-925.

[13] R. Hulsebosch, M. Bargh, G. Lenzini, P. Ebben, and S. Iacob, “Context sensitive adaptive authentication,” In Smart Sensing and Context, Springer, Volume 4793, 2007, pp. 93–109.

[14] C. English, S. Terzis, and P. Nixon, “Towards self-protecting ubiquitous systems: monitoring trust-based interactions,” Personal and Ubiquitous Computing, Springer, Volume 10, Issue 1, February 2006, pp 50-54.

[15] H. Abie, R. M. Savola, J. Bigham, I. Dattani, D. Rotondi, and G. Bormida, “Self-healing and secure adaptive messaging middleware for business-critical systems,” International Journal On Advances in Security, vol. 3, 2010, pp. 34–51.

[16] B, Claudel, N. De Palma, R. Lachaize, and D. Hagimont, “Self-protection for Distributed Component-Based Applications Stabilization, Safety, and Security of Distributed Systems,” Springer, 4280, 2006, pp. 184-198.

[17] J.J. Blount, D.R. Tauritz, S.A. Mulder, "Adaptive Rule-Based Malware Detection Employing Learning Classifier Systems: A Proof of Concept," Computer Software and Applications Conference Workshops (COMPSACW), July 18-22, 2011, pp. 110-115.

[18] Y. B. Woldegeorgis, H. Abie, and Mohamed Hamdi, “A Testbed for Adaptive Security for IoT in eHealth”, ASPI, Sept. 8, 2013, pp. 1-8.

[19] M. Costa et al., “Vigilante: end-to-end containment of internet worms,” SOSP '05, 2005, pp. 133-147.

[20] R. Savola, and H. Abie, “Metrics-Driven Security Objective Decomposition for an E-Health Application with Adaptive Security Management”, ASPI, Sept. 8, 2013, pp. 1-8.

[21] T. Ryutov, L. Zhou, C. Neuman, T. Leithead, and K.E. Seamons, “Adaptive trust negotiation and access control,” SACMAT '05, 2005, pp. 139-146.

[22] Y. Al-Nashif, A.A. Kumar, S. Hariri, Qu. Guangzhi, Y. Luo, F. Szidarovsky, "Multi-Level Intrusion Detection System (ML-IDS)," Autonomic Computing, ICAC '08, June 2-6, 2008, pp. 131-140.

[23] R. He, and M. Lacoste, “Applying component-based design to self-protection of ubiquitous systems” SEPS '08, 2008, pp. 9-14.

[24] M. Barrere, R. Badonnel, and O. Festor, "Vulnerability Assessment in Autonomic Networks and Services: A Survey," IEEE communications surveys & tutorials, vol.16, no.2, Second Quarter 2014, pp.988-1004.

[25] Identifying emerging and future risks in remote health monitoring and treatment, ENISA, Mar 01, 2009, http://www.enisa.europa.eu/publications/archive/being-diabetic-2011.

[26] J. Ash et al., Guide to Information Security for the Health Care Sector, eHealth Ontario, 2010, http://www.ehealthontario.on.ca.

[27] S. Dobson et al., “A survey of autonomic communications,” ACM Transaction, Autonomous Adaptive System, 1, 2, 2006, pp. 223-259.

[28] M. Parashar, and S. Hariri, “Autonomic Computing: An Overview,” Unconventional Programming Paradigms, Springer Berlin Heidelberg, 3566, 2005, pp. 257-269.

[29] M. Salehie, and L. Tahvildari, “Self-adaptive software: Landscape and research challenges,” ACM Trans. Auton. Adapt. Syst. 4, 2, Article 14, May 2009, pp. 1-42.

[30] IBM Corporation, “An architectural blueprint for autonomic computing,” Autonomic computing, white paper, 2006, pp. 1-36.

[31] H. Abie, "Adaptive security and trust management for autonomic message-oriented middleware," MASS '09, 2009, pp. 810-817.

[32] S. Price, Information Security Management Handbook, Sixth Edition, Volume 4, Auerbach Publications, 2010.