# Towards Metrics-Driven Adaptive Security Management in E-Health IoT Applications

Reijo M. Savola
VTT Technical Research Centre of Finland
Kaitoväylä 1, FIN-90570 Oulu, Finland
+358 40 569 6380
reijo.savola@vtt.fi

Habtamu Abie
Norwegian Computing Center
Gaustadalléen 23, Blindern,
N-0314 Oslo, Norway
+47 22 85 25 95
habtamu.abie@nr.no

Markus Sihvonen
Mikkelin Puhelin Oyj
Mikonkatu 16
FIN-50100 Mikkeli, Finland
+358 40 756 4802
markus.sihvonen@greenpeak.fi

## ABSTRACT
E-health applications utilizing IoT (Internet of Things) technologies hold a significant promise: biomedical sensor networks and the appropriate interpretation of the data originating from them enable better self-care of chronic diseases, and thus are potential to imply remarkable savings in national healthcare budgets. However, security is a major concern in these applications due to varying use context, changing threats and the high privacy and confidentiality requirements of healthcare data. Novel adaptive security management solutions, based on security effectiveness, correctness and efficiency evidence, can be used to respond to these needs. We analyze security objectives of E-health IoT applications and their adaptive security decision-making needs, and propose a high-level adaptive security management mechanism based on security metrics to cope with the challenges.

## Categories and Subject Descriptors
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

## General Terms
Management, Measurement, Security.

## Keywords
IoT, Security Metrics, Adaptive Security

## 1. INTRODUCTION
The treatment of chronic medical diseases like diabetes, arthritis and COPD (Chronic Obstructive Pulmonary Disease) takes constantly increasing proportion of national healthcare budgets [1]. At the same time, it is a trend that elderly people are living longer in their own home. Novel E-health IoT (Internet of Things) applications enable continuous monitoring of patients with chronic diseases and health and well-being of elderly persons in general. Smart use of sensor technologies is core to the IoT applications. Use of these technologies can help to reduce the reaction time to severe conditions and to achieve better self-care results. Use of these kinds of IoT applications incorporates many security critical system components, complex and networked software, and is subject to high privacy requirements.

The main contribution of this paper is in the (i) analysis of SOs (Security Objectives) and related adaptive security management needs of the envisioned E-health IoT environment, and in (ii) definition of a high-level adaptive security management mechanism utilizing security metrics.

The rest of the paper is structured as follows. Section 2 discusses the background from the E-health perspective, including high-level use scenarios. Section 3 discusses the SOs and adaptive security needs of the scenarios. Section 4 proposes our initial adaptive security management approach. Section 5 presents related work, before Section 6 offers conclusions and poses future research questions.

## 2. BACKGROUND
E-health IoT applications can be used in a variety of use scenarios. In the following we discuss E-health IoT applications for (i) patient monitoring, (ii) chronic disease self-care and (iii) elderly persons monitoring.

Figure 1 illustrates the use scenarios under discussion here. Sensors such as blood glucose and blood pressure meters, ECG (Electrocardiography), well-being meters and motion detectors can be used to offer input for better self-care decisions. Commonly used wireless device interconnectivity standards such as ZigBee [3] enable easy interconnection of sensors. However, we address here sensors in general, utilizing any applicable technology. It is important to aim at integrated and seamless use of e-health sensors and data management for elderly persons and people with chronic diseases, because (i) seniors often have chronic conditions, and (ii) many E-health measurements needed for overall health and chronic disease monitoring are the same.

Sensors of IoT applications can form a BSN (Biomedical Sensor Network). It can be considered a special case of Wireless Sensor Network (WSN) [2]. A gateway device (or node) outputs data streams which contain sensor data from the BSN, and possibly some context data such as time and space information and meta data specifying in more detail the contents. In addition to the gateway device, the BSN can be connected to medical devices of ambulance vehicles or aircraft in paramedic scenarios. The problem with wireless sensors is that wireless communication can be intercepted quite easily, causing privacy, confidentiality,


*7th International Conference on Body Area Networks (BODYNETS 2012), Workshop on Security Tools and Techniques for Internet of Things (SeTTIT 2012), September 24–26, 2012, Oslo, Norway.*




DOI 10.4108/icst.bodynets.2012.250241

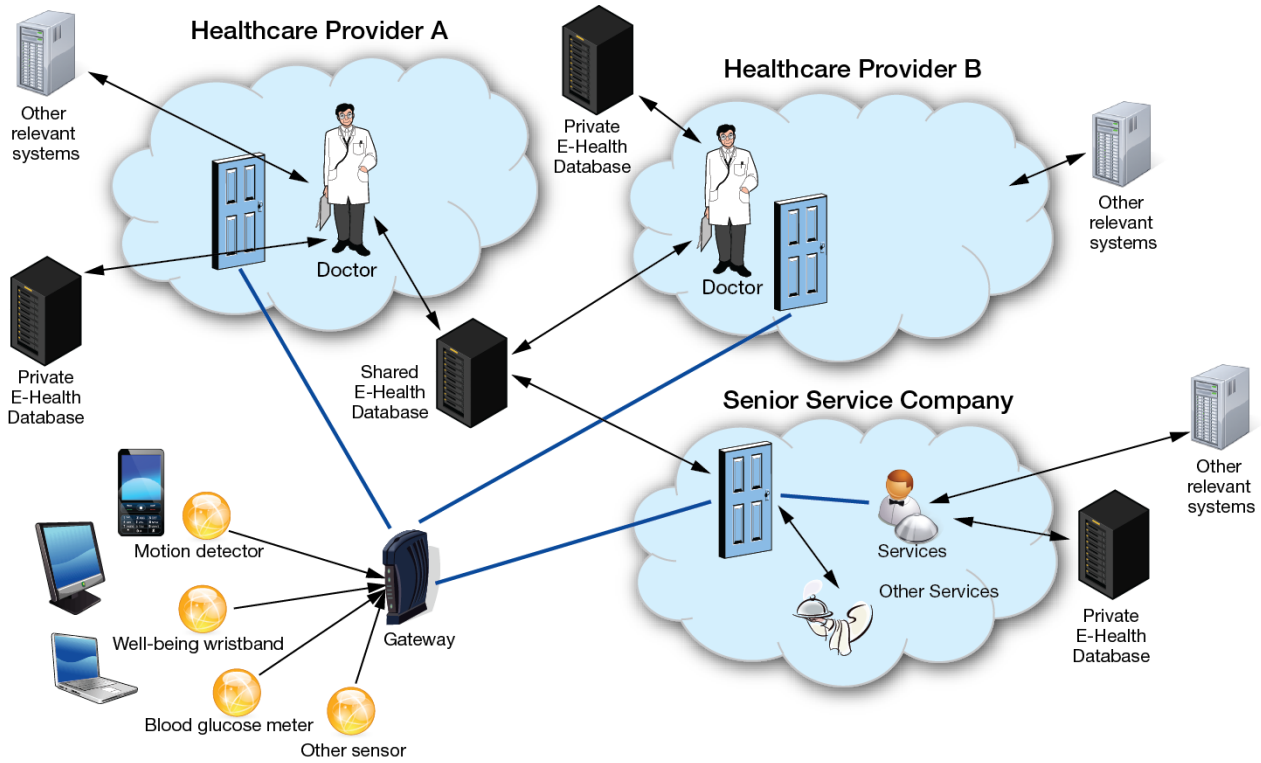


**Figure 1. Use of IoT technology in self-care of chronic diseases and senior services.**

integrity and availability threats. Moreover, fake nodes can also exist. Adequate physical access control measures are needed to protect the BSN from these close-to-sensor threats.

Most biomedical data can be assumed to be transmitted in one direction. This is a special case of IoT systems, since actuators are not used often. However, feedback is offered in the form of personal medical counseling or applications designed for it. Both connection-based and connectionless channels are used in E-health scenarios.

It is important to have controlled collaboration and information sharing between different healthcare providers concerning the patient's health information. The provider can change every now and then, when responsibilities are changed in national and community healthcare system. Moreover, people travel nowadays a lot, and it is important that the nearest provider has access to the up-to-date health information.

In addition to travelling, there are a lot of other needs for adaptiveness, as discussed in Table 2 of Section 3.2. In addition, collaboration between the healthcare providers responsible for chronic disease treatment and companies offering E-health services for elderly people is needed. In this kind of collaboration, privacy and data confidentiality are major challenges. The data managed should be classified to different privacy levels, and should be validated by metrics.

The access to these data has to be tight according to the role or other authorization classification of the users within the service providers. Examples of the roles include medical doctor, doctor specialized in diabetes care, nurse, healthcare consultant, well-being consultant, and security service provider.

The other relevant systems shown in Figure 1 include, e.g., customer management and billing systems. In the following, we refer to the above described system model by term SuI (System under Investigation).

Informed tradeoff decisions between security effectiveness, efficiency and usability are needed in the envisioned system. There are always limited financial, effort and performance resources available for security solutions. In addition, elderly persons need simple-to-use self-care solutions, no matter what the individual service providers are.

# 3. SECURITY IN E-HEALTH IoT

In this section, we discuss the security domains and the high-level SOs inherent to the possible use scenarios of Figure 1. The mobility, change of context, and change of security risks call for adaptive security solutions in order to cope with these rapidly evolving constraints.

## 3.1 Security Domains

A *security domain* is a part of the overall infrastructure under clear administration by a stakeholder, applying specific security policies. Figure 1 assumes multiple security domains which need to collaborate. Leister et al. [2] propose the *communication levels* (CL) of Table 1 for patient monitoring, ensuring adequate isolation and interfaces.

The security management should take into account the characteristics of security domains, and adaptive security management should support switching security domains in a seamless way. All listed CLs can be considered also as different security domains from communication perspective. The bigger CL number, the further the activity is from an individual patient.

**Table 1. Communication levels for E-Health IoT [2].**

| CL | Description |
|---|---|
| 0 | Patient |
| 1 | Personal sensor network like BSN. The sensors form BSN. |
| IIa | Paramedic scenarios |
| IIb | Smart home scenarios. The patient is in a smart home environment. |
| IIc | Mobility scenarios. The patient is mobile, using available cellular networks or WLANs (Wireless Local Area Networks) |
| IId | Intensive care or surgery. Utilization of appropriate data in specific emergency situations. |
| IIe | Pre- or postoperative sensor data management |
| III | Healthcare information system comprising the hospital network, computing facilities, databases and access terminals in the hospital. |

We propose three additional CLs to extend the viewpoint to the envisioned SuI:

- CL IIIa: Utilization of BSN data by medical doctors and other healthcare personnel in non-emergency treatment of individual patient with a chronic disease.
- CL IV: Information sharing between different healthcare providers concerning medical information of an individual patient.
- CL V: Information sharing between healthcare providers and medical research organizations for the purposes of research, new solutions development, and feedback to CL 0–IV.

## 3.2 Security Objectives

Table 2 lists SOs of the SuI. Moreover, the core needs for adaptive security solutions are identified in the table. In the table, 'end-user' refers to a patient with a chronic disease or an elderly person. 'Service provider user' means doctors, other medical experts and supporting personnel being part of the end-user's care.

**Table 2. SOs for the SuI.**

| SO | Description | Adaptivity need |
|---|---|---|
| 1. End-user authentication and authorization (CL 0–II) | Adequate authentication strength is a highly critical parameter in ensuring that the right person receives the right treatment. Authentication is based on multiple mechanisms, and may include passwords, smart cards, biometrics, RFID (Radio Frequency Identification) tags and buttons, and their fusion. Usability of authentication mechanism(s) is emphasized especially for seniors. | Adaptive authentication mechanisms are needed to cope with changing context of use, security threats and the user behavior. Efficiency and usability of security controls are important objectives for adaptive mechanisms. Adaptive solutions can be used to setting requirements and for enforcing the sufficient authentication mechanisms. |
| 2. Sensor and BSN authentication (CL I) | Authentication of sensors should be strong especially in the case where data is used to make direct interpretations of the patient's health. The challenge in using sensors, however, is the lack of computer power for sophisticated and effective authentication algorithm. Sensor registration to the gateway has an important role. | Adaptive authentication mechanisms are needed to set requirements which take into account the criticality of decisions to be made by the end-user and the service provider user based on the sensor input. The possibility of fake sensors should be minimized in possibly varying situations. |
| 3. Service provider user authentication (CL III–V) | The data accessed and used by service provider users have inherently different privacy levels. The pre-authorized roles for service provider users should indicate the type of data that a person can access. | Adaptive authentication mechanisms are needed to cope with changing demands depending on the privacy level and the official authorization level for making treatment decisions. |
| 4. Service provider user authorization (CL III–V) | Depending on the authentication strength and context, persons with pre-authorized roles can access critical information. | Adaptive authorization techniques are needed to set the adequate requirements and to enforce the sufficient authorization mechanisms. |
| 5. Data integrity (all levels) | Especially in paramedic situations, lost, delayed or altered data can cause direct damage to the patient's health. Moreover, indirectly, data integrity is important to longer-time treatment decisions. | Adaptive data integrity techniques are needed to maintain adequate data integrity especially during alarm situations. |
| 6. Privacy and data confidentiality (all levels) | Privacy requirements, and at the same time, data confidentiality requirements are emphasized in healthcare. Strong confidentiality algorithms, key distribution and associated processes are crucial. Compliance to appropriate privacy legislation and regulations is needed. | Adaptive security decision-making should adapt requirements for privacy and data confidentiality based on the data processing needs, roles of stakeholders, regulations and legislations, and the privacy level of data indicated by privacy metrics. |
| 7. Availability (all levels) | Availability of data from the BSN to service providers is important especially in paramedic and alarm situations. Availability of the service provider's systems can be critical for health and life. | Adaptive techniques are needed to balance the load in the system and to use resilience solutions to maintain adequate availability. |
| 8. Non-repudiation (all levels) | Due to the high privacy and data confidentiality requirements, non-repudiation is important in the envisioned environment. Especially in medical alarm situations, there can be non-repudiation challenges. | Adaptive authentication mechanisms are needed to ensure the adequate non-repudiation level despite of changing conditions and selection of security controls. Specific adaptive solutions are needed to medical alarm situations. |

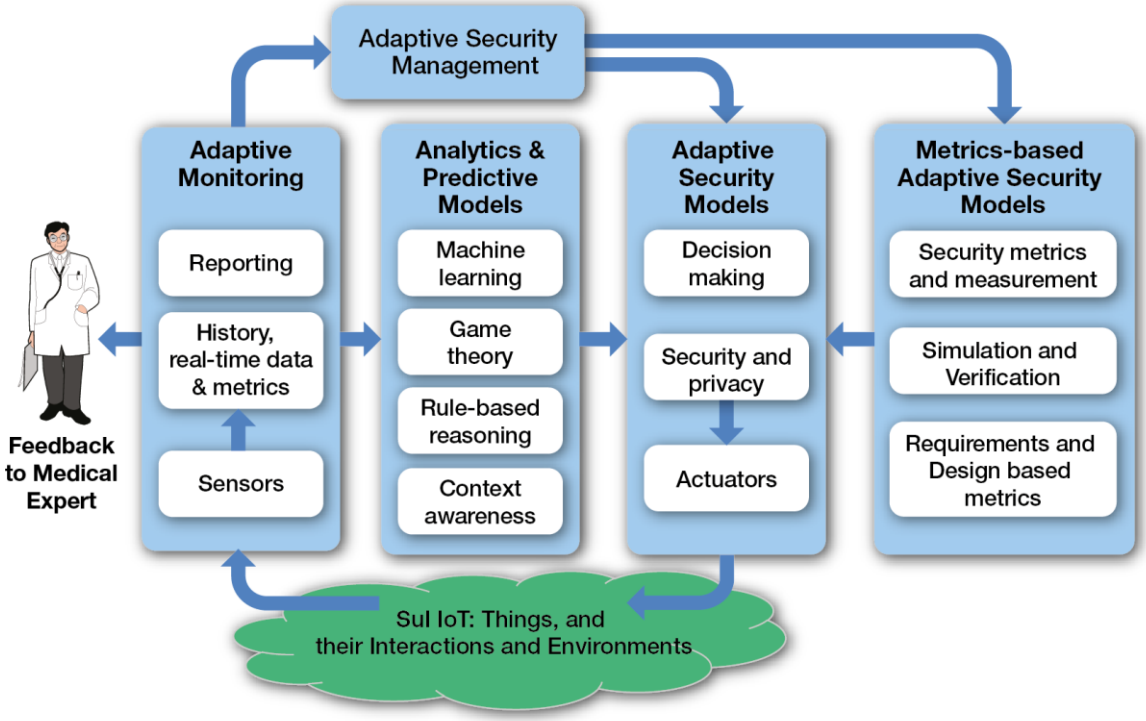


**Figure 2. Proposed adaptive security management model.**

A dynamic network topology, because of mobile nodes, energy constraints and lower bandwidth of IoT networks, make them vulnerable to attacks like DoS (Denial-of-Service). Other types of attacks include especially eavesdropping, masquerading, and unauthorized disclosure. The risks include life-threating situations, loss of business, loss of personal information, misuse of access, and data destruction. Seizure of a service or even a larger infrastructure section can be possible by utilizing various sub-patterns. For example, the connection of the healthcare information system and other associated systems is a critical point, since the access control in the latter case is often not as strict as in the former one. Authenticity of sensor data can be an issue too, since the sensors often have limited computing resources, and sophisticated sensor identity solutions are not possible before a gateway device.

In general, management of healthcare data is strictly regulated in most parts of the world. A well-known example is the United States HIPAA (Health Insurance Portability and Accountability Act) [4]. Due to the high privacy requirements of medical data, it is essential to develop and deploy strong end-to-end security mechanisms for all SOs.

## 4. PROPOSED ADAPTIVE SECURITY APPROACH

In this section, we propose an adaptive security management model for the envisioned SuI, and discuss the evidence needed from security metrics for the approach.

### 4.1 Adaptive Security Management Model

Adaptive security here refers to a security solution that learns and adapts to changing environment dynamically and anticipates unknown threats. It involves gathering contextual information both from within the system and from the environment, measuring security level and metrics, analyzing the collected information and responding to changes (i) by adjusting internal working parameters such as encryption schemes, security protocols, security policies, security algorithms, different authentication and authorization mechanisms, changing the QoS (Quality of Service) available to applications, and automating reconfiguration of the protection mechanisms, and/or (ii) by making dynamic changes in the structure of the security system [5]. To meet these challenges, our adaptive security management model integrates the following models: (i) a continuous cycle of monitoring to monitor the information about context and status of the SuI IoT which is exploited at runtime in the adaptation process, (ii) analytics and predictive functions to analyze the monitored information and predict future events, (iii) decision making adaptive security models to determine whether changes and adaptation should be made or not, and, if to be made, to select the 'best' adaptive security model for the given situation, and to apply the identified changes and adaptation, and (iv) metrics-based adaptive security models to measurably evaluate and validate the run-time adaptivity meeting the challenges in the changing environments and today's rising threat situation.

Figure 2 illustrates the proposed adaptive security management model. It is built on a basic feedback structure. The model closes the adaptive control loop of management of security and privacy risks, dynamically taking into account the necessary context information to ensure efficiency over time applying the Monitor-Analyze-Adapt (plan, execute and learn) methodology. The 'Adapt' phase is the phase where the effective reaction is made on the security and privacy. This adaptive security management is a metric-driven adaptive decision-making system for measuring and validating the strength of the adaptive security models for SuI IoT.

The cycle model of the metrics-based adaptive security is similar to the ISO/IEC 27005 Standard's PDCA (Plan-Do-Check-Act) cycle [6]; During the 'Plan' phase the metrics are established, during the 'Do' phase they are implemented and operated, during the 'Check' phase monitored and reviewed, and during the 'Act' phase maintained and improved [7]. Real-time metrics allow us to monitor the adaptive metrics in real time to ensure comparable adaptive metrics results, the past against present.

In general, metrics-based adaptive decision-making can be used for the following purposes in the SuI:

- Setting sufficient security and privacy for a given situation, and
- Selecting an adequate security control implementation (or actually, enabling its deployment) for a given situation.

## 4.2 Role of Security Metrics

Effectiveness is the main measurement objective of security mechanisms, but efficiency of the mechanisms is also important, as well as, usability. Correctness, including configuration correctness, and compliance to regulations is an important underlying measurement objective. Promising security metrics development techniques such as hierarchical decomposition of security objectives [8], [9] can be utilized in connection with the adaptive management model discussed above.

According to the findings from Table 2 (Items 1–4), *authentication* effectiveness (or strength) is one of the core parameters needed for adaptive security management in the envisioned SuI. In addition, strong enough authentication is a prerequisite for access control solutions. According to [8], the main properties contributing to authentication effectiveness are authentication identity uniqueness, structure and integrity, and authentication mechanism reliability and integrity. A more detailed hierarchical SMM (Security Metrics Model) for end-user authentication is available in [9], developed using the decomposition methodology from [8].

*Authorization* metrics are tightly coupled to authentication effectiveness. In addition to authentication effectiveness, they should take into account access control mechanism reliability and integrity, authorization policy effectiveness and authorization object integrity [8]. Support for both role-based and individual-based access control approaches is needed in the SuI. The former is better from scalability perspective, but the latter is needed in enforcing official medical authorization.

Metrics representing the effectiveness of *data integrity and confidentiality* algorithms, as well as related integrity and confidentiality assurance level in general in the SuI, are needed for the purposes of adaptive security decision-making in connection of Items 5 and 6 in Table 2. Security assurance metrics taxonomies, such as Ouedraogo et al.'s approach [10], can be used as the basis for metrics development.

*Privacy* metrics to be utilized in connection with adaptive security management of E-health data should be able to express the anonymity level of the data collection. Potential anonymity metrics approaches for the SuI include, e.g., *k*-Anonymity [11], ℓ-Diversity [12], and mix-based anonymity systems [13].

*Availability* metrics can rely on QoS, resilience, scalability, power consumption and self-healing parameters, as well as traffic pattern parameters monitored from the adequate fields from the communication protocols. Network security monitoring, IDS/IPS (Intrusion Detection and Prevention System) and vulnerability scanning tools can be utilized to offer input to availability metrics. Chen and Varshney [14] offer an overview of QoS factors of sensor networks.

*Non-repudiation* metrics should emphasize the system's ability to protect against an originator's false denial of having submitted data, or a recipient's false denial of having received data. Sufficient authentication strength is a prerequisite for non-repudiation solutions.

# 5. RELATED WORK

Jafari et al. [15] discuss security metrics for E-healthcare information systems. They propose security metrics development consisting of five elements: technology maturity analysis, threat analysis and modeling, requirements establishment, policies and mechanisms and system behavior. However, they neither discuss use of security metrics in adaptive security management nor propose specific metrics. Weiss et al. [7] propose security metrics built on risk management approach. In their approach, security is quantified in terms of incidents as a result of asset loss. Good incident knowledge is able to offer evidence especially to security effectiveness. However, the availability and attainability of these data is often a challenge in security measurement. In general, security metrics have been studied already for several years now. Comprehensive overviews of security metrics in general are found in, for example, [16–18].

A survey of adaptive security with a brief comparison, special features and benefits categorized according to types of adaptation can be found in [19]. The principles and methodology of our adaptive security management approach is similar to the highly successful EU FP7 GEMOM project [19], [5], [8], which produced a significant and measureable increase in the end-to-end adaptive security and resilience within a message-oriented middleware. Our model is different in that it focuses on the deployment of metrics-based adaptive security management in IoT environment, an environment characterized by diversity of behaviour and capability, wireless communication, constraint bandwidth, limited energy, and infrastructures in changing conditions, and under changing threat models.

# 6. CONCLUSIONS AND FUTURE WORK

We have discussed adaptive security management needs and initial solutions for E-health IoT applications especially for the treatment of chronic diseases and well-being of elderly people. Adaptive security management is needed especially for setting the sufficient security requirements and for enforcing the adequate security controls in the face of changing security risks and use context. Informed adaptive security decision-making is based on adequate security effectiveness, correctness and efficiency evidence offered by security metrics. The role of authentication and authorization effectiveness, as well as the confidentiality and privacy level evidence are emphasized.

In our future work, we aim at more detailed analysis and specification of security metrics and adaptive decision-making algorithm to be used in connection the envisioned system. Moreover, an experimentation system is planned to be built to investigate the characteristics of the metrics-driven adaptive security management in more detail.

## 7. ACKNOWLEDGMENTS

The work presented here has been carried out in two research projects: the ASSET – Adaptive Security for Smart Internet of Things in eHealth (2012–2015) funded by the Research Council of Norway in the VERDIKT program, and IoT Program (2012–2015) launched by the Finnish Strategic Centre for Science, Technology and Innovation TIVIT Plc. We wish to thank our colleagues involved in these projects for their related work and for helpful discussions that made this study possible.

## 8. REFERENCES

[1] WHO, *Preventing chronic diseases – a vital investment*. World Health Organization 2005. www.who.int/chp/chronic_disease_report/full_report.pdf [Accessed August 27, 2012].

[2] Leister, W., Schultz, T., Lie, A., Grythe, K., and Balasingham, I., Quality of service, adaptation, and security provisioning in wireless patient monitoring systems. In Laskovski, A.N. (Ed.): *Biomedical Engineering, Trends in Electronics, Communications and Software*, Intech, Croatia, 2011.

[3] ZigBee Alliance. www.zigbee.org [Accessed August 27, 2012].

[4] *Health Insurance Portability and Accountability Act* (HIPAA), 1996. U.S. Public Law 104–191.

[5] Abie, H., Adaptive security and trust management for autonomic message-oriented middleware, *IEEE 6th Int. Conference on Mobile Adhoc and Sensor Systems (MASS '09)*, 2009, pp. 810–817.

[6] ISO/IEC 27005:2008, *Information technology - Security techniques - Information security risk management*. International Organization for Standardization and International Electrotechnical Commission, 2008.

[7] Weiss, S., Weissmann, O., and Dressler, F., A comprehensive and comparative metric for information security, *Proc. ICTSM'05*, 2005, pp. 0–10.

[8] Savola, R. and Abie, H., Development of measurable security for a distributed messaging system, *Int. Journal on Advances in Security*, Vol. 2, No. 4, 2009, pp. 358–380.

[9] Savola, R., Kanstrén, T., Pentikäinen, H., et al., Utilizing a Risk-Driven Operational Security Assurance Methodology and Measurement Architecture – Experiences from a Case Study. In: *Proc. ICNS '12*, 2012, pp. 134–142.

[10] Ouedraogo, M., Savola, R., Mouratidis, H., et al., "Taxonomy of quality metrics for assessing assurance of security correctness," *Software Quality Journal*, Online First, 30 November 2011, 30 p.

[11] Samarati, P. and Sweeney, L., *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression*, Technical Report, CMU, SRI, 1998.

[12] Machanavajjhala, A., Gehrke, J., Kifer, D., and Venkitasubramaniam, M., ℓ-Diversity: privacy beyond *k*-Anonymity, *Proc. 22nd IEEE Int. Conf. on Data Engineering*, 2006.

[13] D. Chaum, D., The dining cryptographers problem: unconditional sender and recipient untraceability, *Journal of Cryptology*, 1(1), 1988 pp. 65–75.

[14] Chen, D., and Varshney, P.K., QoS support in wireless sensor networks: A survey, Proc. *ICWN '04*, 2004.

[15] Jafari, S., Mtenzi, F., Fitzpatrick, R., and O'Shea, B., Security metrics for e-healthcare information systems: a domain specific metrics approach, *Int. Journal of Digital Society*, Vol. 1, No. 4, 2010, pp. 238–245.

[16] Hermann, D.S., *Complete guide to security and privacy metrics – measuring regulatory compliance, operational resilience and ROI*, Auerbach Publications, 2007, 824 p.

[17] Jaquith, A., *Security metrics: Replacing fear, uncertainty and doubt*, Addison-Wesley, 2007.

[18] Bartol, N, Bates, B., Goertzel, K.M., and Winograd, T., *Measuring cyber security and information assurance: A state-of-the-art report*, Information Assurance Technology Analysis Center (IATAC), May 2009.

[19] Abie, H., Savola, R., Bigham, J., et al., Self-Healing and Secure Adaptive Messaging Middleware for Business Critical Systems, *Int. Journal on Advances in Security*, Vol. 3, No. 1&2, 2010, pp. 34-51.