Risk-Based Adaptive Security for Smart IoT in eHealth

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

Ilangko Balasingham
The Intervention Center, Oslo University Hospital
0027 Oslo, Norway
+47 23 07 01 01
ilangko.balasingham@medisin.uio.no

ABSTRACT
Emerging Internet of Things (IoTs) technologies provide many benefits to the improvement of eHealth. The successful deployment of IoTs depends on ensuring security and privacy that need to adapt to their processing capabilities and resource use. IoTs are vulnerable to attacks since communications are mostly wireless, unattended things are usually vulnerable to physical attacks, and most IoT components are constrained by energy, communications, and computation capabilities necessary for the implementation of complex security-supporting schemes. This paper describes a risk-based adaptive security framework for IoTs in eHealth that will estimate and predict risk damages and future benefits using game theory and context-awareness techniques. The paper also describes the validation case study.

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

General Terms
Management, Measurement, Security.

Keywords
Adaptive Security, IoT, eHealth, Security Metrics, Adaptive Risk Management

1. INTRODUCTION
Emerging Internet of Things (IoTs) technologies provide many benefits to eHealth, e.g., tracking of objects and people (staff and patients), identification and authentication of people, patient mobility, and automatic sensing and collection of data which constitute real-time information on patient health indicators as a basis for medical diagnosis [3]. However the successful development and deployment of IoT based services require that security and privacy are guaranteed.

IoTs are vulnerable to attacks since communications are mostly wireless, unattended things are usually vulnerable to physical attacks, and most IoT components are constrained by energy, communications, and computation capabilities necessary for the implementation of complex security-supporting schemes [13, 3]. Most current security models and mechanisms that address the IoT's problems and allow a system to detect and recover from errors or attacks are hard to change, reuse, and analyze; thus making infrastructures that are inflexible, lost investments, and damages resulting from mechanisms not matching the threats.

The main contribution of this paper is a novel risk-based adaptive security framework for IoT in eHealth. The framework will estimate and predict risk damages and future benefits using game theory and context-awareness techniques. The security methods and mechanisms of the framework will adapt their security decisions upon those estimates and predictions. The framework incorporates a practical and systematic evaluation models utilizing security metrics for validation of the adaptation.

This paper describes this approach that will increase security to an appropriate level by adapting to the dynamic changing conditions of IoTs, including usability, threats, diversity, and heterogeneity. The paper also describes the validation case study that will lead to the design of adaptive strategies for the dynamic interplay between security and data transmission in a mobile patient monitoring system.

The rest of the paper is structured as follows. Section 2 discusses the background and state of the art, including eHealth, IoT, and security and privacy. Section 3 proposes our risk-based adaptive security framework. Section 4 presents the validation case study, and finally, Section 5 offers conclusions and future work.

2. BACKGROUND AND STATE OF THE ART
In this section, we discuss the motivating digital health ecosystem and the characteristics of smart IoTs in eHealth. We also motivate the need for the risk-based adaptive security, and give brief state-of-the-art in game theory and risk analysis, security, privacy and metrics.

2.1 Risk Management
Risk management practice helps to provide a rational and cost-effective framework as a foundation for security measurement and decision making. However, major criticisms of its objective methods are difficulty in measuring the frequency of rare events, limited practicality, the inability to account for emerging threats, and the unreliable information sources, such as the employees or past incidents, of the risk dependency values [19].

Despite all these criticisms risk analysis is still one of the techniques used to measure the strength of the protection mechanisms, an estimation of the probability of specific threats, vulnerabilities and their consequences and costs. Threat analysis

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.2012.250235

is the first step in risk analysis for the identification of sources and types of threats and their likelihood. Ed Felten [22] states "The first rule of security analysis is this: understand your threat model. Experience teaches that if you don't have a clear threat model -a clear idea of what you are trying to prevent and what technical capabilities your adversaries have -then you won't be able to think analytically about how to proceed. The threat model is the starting point of any security analysis". This shows that risk management is the kingpin in meeting the demands for security and privacy. It has, after all, been stated that "because absolute security is impossible to achieve", a security framework that does not incorporate a risk management approach incorporating detection and reaction, is incomplete [27]. Following this, we propose a novel risk-based adaptive security framework for IoT to estimate and predict risk damages and future benefits, and to learn identified new or unknown threats to IoT based eHealth systems.

2.2 Game Theory and Risk Analysis

Game theory is a mathematical tool that allows modeling conflict and cooperation between two or more separate parties - the players. The players are assumed to behave rationally, i.e. they are triggered by the selfish incentive of maximizing their individual benefit (or risk measure), which is usually expressed in terms of a utility function [33]. A game consists of three elements (i) players that can make decisions in the game, (ii) strategies that players can commit, and (iii) payoffs which are the gains or losses experienced when the players commit to strategies. Game theory has been used extensively in risk analysis to model a variety of problems [5, 14, 15, 19, 31-34].

In the words of Cox [32], "game-theoretic formulations of attack-defense conflicts (and other adversarial risks) can greatly improve upon some current risk analyses that attempt to model attacker decisions as random variables or uncertain attributes of targets ("threats") and that seek to elicit their values from the defender's own experts. Game theory models that clarify the nature of the interacting decisions made by attackers and defenders and that distinguish clearly between strategic choices (decision nodes in a game tree) and random variables (chance nodes, not controlled by either attacker or defender) can produce more sensible and effective risk management recommendations for allocating defensive resources than current risk scoring models. Thus, risk analysis and game theory are (or should be) mutually reinforcing."

In the book, "Game Theoretic Risk Analysis of Security Threats", Bier and Azaiez [31] introduce reliability and risk analysis in the face of threats by intelligent agents where game-theoretic models are developed for identifying optimal and/or equilibrium defense and attack strategies in systems of varying degrees of complexity. The authors' primary foci are to integrate game theory and reliability methodologies into a set of techniques to predict, detect, diminish, and stop intentional attacks at targets that vary in complexity, and to highlight work by researchers who combine reliability and risk analysis with game theory methods to create a set of functional tools that can be used to offset intentional, intelligent threats (including threats of terrorism and war). Manshaei et al. [34] also summarize the current adopted game-theoretical approaches and main results obtained from the respective models, analyzed how the defender can gain a deeper understanding of the attacker's strategies and the potential attack risks through the equilibrium analysis of the security game, and reviewed and compared existing security games in computer networks in terms of players, game models, game-theoretic approaches, and equilibrium analysis.

2.3 Digital Health Ecosystems

Hadzic and Dillon [28] state that the digital ecosystem approach integrates and uses the concepts of a given natural domain to the digital world, reproducing or interpreting some of the mechanisms of natural ecosystems. They further state that it is a self-organizing digital infrastructure aimed at creating a digital environment for networked health organizations that supports the cooperation, the knowledge sharing, the development of open and adaptive technologies and evolutionary business models.

As one of the building block of the digital ecosystem [21], the IoT [18], "an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders". The privacy of citizens as well as the correct functioning of the administration and the efficiency of the economy in the e-Society is all also dependent on robust security. Therefore there is a need for the security and robustness of public and private information systems and infrastructure, and enhancement of the security and privacy of health organizations and private persons.

These challenges can be met through the development of adaptive and context-aware security for the next generation of eHealth digital ecosystems, which can enable communicating health organizations both in public and private sector to design and implement context aware security and privacy protection and thus adaptive to patients' needs. Such adaptive eHealth systems will improve end user's confidence in service providers.

2.4 Smart IoTs in eHealth

IoT is defined, in a nutshell, as a worldwide network of interconnected objects [24]. Smart here represents that the IoT possesses self-abilities or capabilities such as self-learning, self-adapting, and self-reasoning to adapt to dynamic environments. IoTs improve the quality of our lives, just to cite a few: at home, while travelling, when sick, at work, when jogging, and at the gym [3]. IoTs in the Healthcare can help tracking of objects and people (staff and patients), identification and authentication of people, and automatic data collection and sensing. The collected data constitute real-time information on patient health indicators as a basis for medical diagnosis. The provision of adaptability capability of IoTs can reduce the delay for treatment of critical patients enhancing traditional medical services.

Although IoTs can provide such simplest and least expensive solutions to wirelessly connect health monitoring devices in the home to personal health records and hospitals, the successful development and deployment of IoT based services require that security and privacy are guaranteed. As recently discussed in [13] and [3],

- IoTs are vulnerable to attacks since communications are mostly wireless and thus eavesdroppable, things are usually unattended and thus vulnerable to physical attacks, and most IoT elements are short on both the energy and computing resources necessary for the implementation of complex security-supporting schemes.
- The pervasiveness of Radio Frequency Identification (RFID) tags and increased access to RFID readers in IoT will make it possible to collect and cross-reference cheaply a vast amount

of data in order to infer sensitive personal information, thus leading to yet another source of information about our movements, health and habits, and making privacy and security matters of growing concern and a key issue for end-users and IoT service providers.

- Deploying a thing in a new context, for which it was not specifically designed, may expose vulnerabilities and allow unwanted side-effects to occur, which may turn previously harmless protocol flaws into critical flaws. Indeed, it is emphasized that ‘‘to the extent that everyday smart things (objects) become information security risks, the IoT could distribute those risks far more widely than the Internet has to date” [3].

Most current security models and mechanisms that address these problems and allow a system to detect and recover from errors/attacks are hard to change, reuse, and analyse and thus making infrastructures inflexible, lost investment, damages realized through mechanisms not matching the threats, etc. Therefore, there is a need for the development of risk-based adaptive security methods and mechanisms for IoTs that increase security to an appropriate level. The security methods and mechanisms should adapt to dynamic changing conditions of IoT including usability, threats, and diversity/heterogeneity.

Atzoria et al. in their paper “The Internet of Things: A survey” [3] describe the many benefits provided by the IoT technologies to the healthcare domain. There are also plenty of seminal papers on securing internet [24], new security and privacy challenges in IoTs [18], a review of security in the Internet of Things [25], a survey of the Internet of Things [3], Internet of Things strategic research roadmap [12], privacy and security issues in the Internet of Things [26], and Ubiquitous Computing (Smart Devices, Environments and Interactions) [13].

2.5 Security and Privacy

One of the key issues in the security and privacy of IoTs in eHealth is data integrity that also involves authentication, access control and secure communication. The two frequently asked questions are, (i) How do you trust the data our sensors are sending?, and (ii) in fact how do we even know it is a sensor that is sending data at all, and not a bot or piece of malware? To briefly answer these questions, enforcing the security and privacy of IoT system lies on the key abilities of taking preventive measures so that hackers can hardly break into the system and hide their tracks, of distinguishing suspicious activities from the normal operations of the system, and of once detected, stopping the malicious processes in a comprehensive and efficient way.

The general threats to security objectives (authentication, authorization, confidentiality, integrity, availability, and non-repudiation) such as masquerading, unauthorized access, eavesdropping, loss or corruption of information, repudiation, forgery, and DoS (Denial of Service) also apply to IoT based systems.

Current access control models [4], trust and risk based access control policies [4, 17], and other approaches [8, 10, 11] that use automated inferring of policies provide access control, but don’t adapt to changing circumstances as which characterize the IoT. Several solutions that use some cryptographic algorithms have also been proposed for sensor networks and RFID systems, but since typical cryptographic algorithms demand large amounts of resources in terms of energy and bandwidth, both at the source and the destination, such solutions cannot immediately be applied to the IoT [3]. There are plenty of proposals on privacy risk models, risk analysis, vulnerability assessment, threats and asset evaluation, and risk-based access controls [6, 9, 14, 15, 11]. This study will complement these proposals by providing risk-based adaptive security models in IoT environment, an environment that allows thorough integration of everyday objects and activities with information processing [12].

Security metrics provide a comprehensive approach to measuring risks, threats, operational activities, and the effectiveness of data protection in an IoT system. Comprehensive overviews of security metrics approaches and objectives can be found in [16]. In [23], security metrics built on risk management approach have been proposed. Jafari et al. [30] proposed an approach for developing security metrics for assessing security posture of healthcare organizations. A comprehensive survey of IoT security and privacy can be found in [24-26].

In this paper we apply similar principles and methodology as those used by the highly successful EU GEMOM project [1-2] to develop its adaptive security and metrics models. The GEMOM project produced a significant and measurable increase in the end-to-end security and resilience within a message-oriented middleware but did not deal with energy-aware QoS metrics for IoT devices. This paper focuses on the development of risk-based adaptive security and metrics for deployment in a smart IoT, an environment characterized by diversity of behavior and capability, periodic scarcity of computing resources, and infrastructures in changing conditions, and under changing threat models.

3. PROPOSED ADAPTIVE FRAMEWORK

Adaptive security here refers to a security solution that learns, and adapts to changing environment dynamically and anticipates unknown threats without sacrificing too much of the efficiency, flexibility, reliability and security of the IoT system [1, 2]. 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.

The analysis part of such an adaptive approach requires flexible learning and decision making processes for parametrical, structural and goal adaptation that help set priorities and make the best decision when both the qualitative and the quantitative aspects of a decision need to be considered [1, 2]. In this section we present a high level risk-based adaptive framework that meets these challenges.

The framework 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. It applies the Monitor-Analyze-Adapt (plan, execute and learn) methodology using feedback mechanisms. The actual effective reaction on the security and privacy is made during the “Adapt” phase. Table I shows the alignment of the ISO/IEC 27005:2008 Plan-Do-Check-Act (PDCA) [20] based ISMS, ISRM and our ARM methodology.

Figure 1 depicts our risk-based adaptive security framework for IoT. The framework consists of (i) the adaptive risk management model, (ii) the adaptive monitoring model, (iii) the analytics and predictive models, (iv) the adaptive decision-making models, and (v) the evaluation and validation models. The following sections describe the high level key features of these models.

Table I. Alignment of ISO/IEC 27005 ISMS, ISRM and ARM

Information Security Management system (ISMS) Process	Information Security Risk Management (ISRM) Process	Adaptive Risk Management (ARM) Process/ Methodology
Plan	Establish the context Risk assessment Risk treatment planning Risk acceptance	Analyze (plan) - establish security
Do	Implementation of risk treatment plan	Adapt (Execute) - adapt, implement and operate security
Check	Continual monitoring and reviewing of risks	Monitor - monitor and review security
Act	Maintain and improve the ISRM process	Adapt (learn) - maintain, learn & improve security

3.1 Adaptive Risk Management

Adaptive risk management (ARM) here refers to a risk management model which is capable to learn, adapt, prevent, identify and respond to known and unknown threats in real-time. The key function of this model is the development of risk-based adaptive security methods and mechanisms for smart IoTs that estimate and predict risk damages and future benefits by integrating adaptive monitoring, analytics and predictive models, adaptive decision-making models, and evaluation and validation models in a continuous cycle, thus enabling the security methods and mechanisms to adapt their security decisions upon those estimates and predictions.

To meet these challenges the ARM model takes the following five required measures [27]: (i) Identify - ability to predict problems, (ii) analyze - ability to predict impact, (iii) plan - ability to implement planned actions, (iv) track - ability to maintain management focus on risk mitigation actions, and (v) control - ability to reduce risk exposure. These are achieved through the coordination of the other models which are described in the ensuing sections.

3.2 Adaptive Security Monitoring

In [2], we introduced reference architecture of a general monitoring framework, which can be utilized for obtaining automated technical evidence for the purposes of continuous operational security monitoring. The adaptive security monitoring model will adapt this architecture with a continuous cycle of monitoring of the information about context and status of the smart IoTs which is exploited at runtime in the adaptation process.

3.3 Analytics and predictive Models

The analytics and predictive models analyze the monitored information from the adaptive monitoring model using game theory [5, 14, 15] and context awareness to estimate and predict security and privacy risks and future benefits dynamically, to

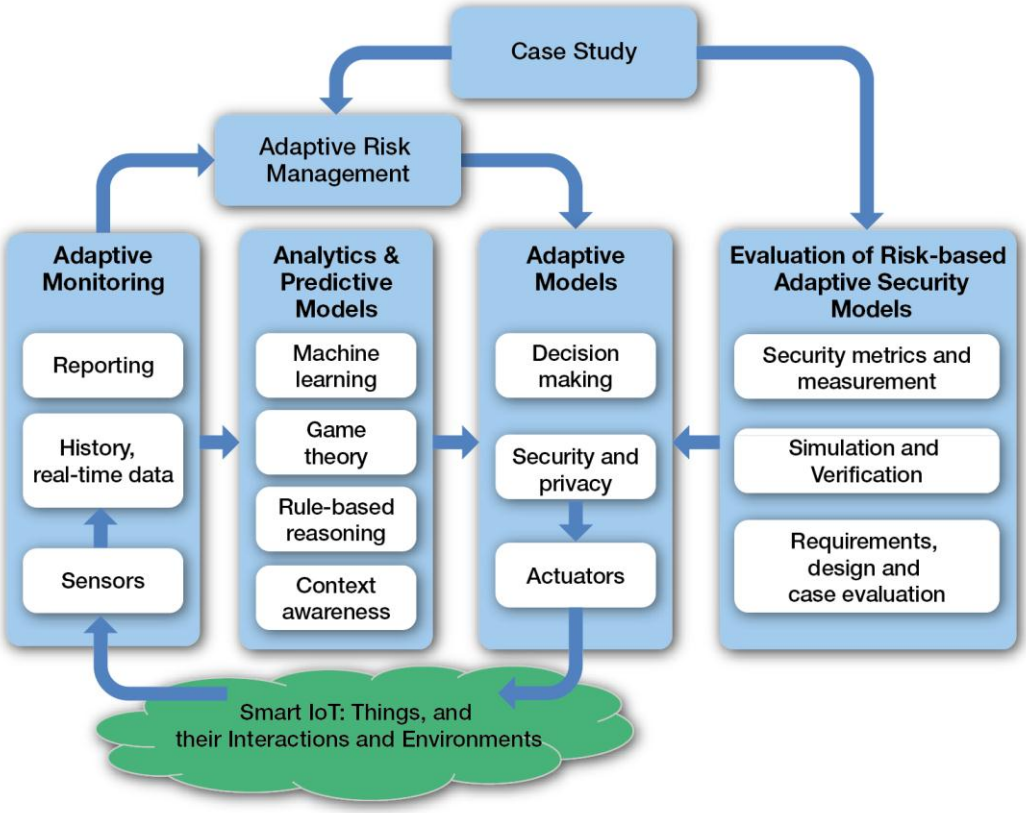

Figure 1. Proposed adaptive security management model.

understand and prioritize the decision making activities, and to analyze the socio-economic of adaptive security of smart IoTs. Game theory was chosen because it can model the dynamic behavior of stakeholders with conflicting interests including the strategies of real world adversaries [15].

The models will also further improve the accuracy of estimation and prediction mechanisms by applying optimized machine learning and rule-based algorithms, thus increasing the ability to precisely predict and measure the risk of damages and future benefits and adapt security decisions upon those predictions. Moreover, the models will improve the light-weight abilities of smart things by improving their context-awareness and self-abilities. This includes optimizing algorithms for different IoT processing capabilities to detect in real-time unknown security and privacy threats, respond to them, and adapt to the environment and changing degree of security and privacy breaches.

3.4 Adaptive Security Decision-Making Models

In IoT based eHealth, adaptive security decision-making is needed for adapting the means for protection of the IoTs themselves, their interactions and their environment from malicious intruders and authorized users. The adaptive decision-making model thus adapts to the dynamism of Things, their interactions, and the environment, and to the varying degrees of risk that the IoT eHealth system will be compromised. It does this by dynamically determining whether changes and adaptation should be made or not, and, if to be made, to select the 'best' adaptive security model for a given situation, and to apply the identified changes and adaptation by ensuring the highest likelihood of achieving the greatest benefit for the smallest risk. The overall adaptive decision-making model also learns and adapts to a changing IoT environment at run-time. It does this by (i) combining adaptive risk-based decision model, adaptive security and privacy models, and actuators to make effective adaptive reaction, and (ii) integrates different metrics for validation and verification, adaptive risk assessment, and predictive analytics models for estimation and prediction of security and privacy risks and impacts.

3.5 Evaluation and Validation models

Security Measurement and Metrics are needed for measurably evaluating and validating the run-time adaptivity of IoT security solutions meeting the challenges in the changing environments and today's rising threat situation. The promising security metrics development techniques developed in [16] using decomposition of security objectives will be adopted and further evolved with theory and mathematical models for measuring and validating the strength of the adaptive security models for IoT. The techniques allow us to capture requirements and design metrics at varying levels of abstraction to determine and identify gaps and hindrances at the architecture and design levels. As stated in [23] real-time metrics allow us to monitor the adaptive metrics in real time to ensure comparable adaptive metrics results, the past against present.

Predictive simulation and verification based security metrics can help to understand trade-offs between different solutions by varying assumptions on threats and requirements, to select better metrics that are risk indicators of current and future IoT security risks, and to provide a variety of benefits to decision-makers [29].

4. CASE STUDY: PATIENT MONITORING

Patient monitoring systems are a major data source in healthcare environments. It is important these systems maintain a certain level of availability, quality of service (QoS), security and the protection of privacy of the patient. Leister et al. [7] analyzed the security and privacy in patient monitoring systems with an emphasis on wireless sensor networks and suggested a framework for providing privacy, security, adaptation and QoS for patient monitoring systems. For our case study, IoT-based patient monitoring system is depicted in Figure 2. The patient can be either at home or in the hospital. Things include smart phones, tablets, sensors, sensor nodes, and actuator nodes.

The case study will lead to a simulation experiment in the following manner at a test-bed: Blood pressure, electrocardiogram (ECG) and heart rate will be gathered from real patients, where the patient ID will be removed and the sensor data made anonymous. The sensor data will be stored in three different ZigBee sensor nodes. A smart phone with ZigBee transceiver will act as an access point and communicates with both ZigBee sensor nodes and a Medical Centre. We will study two different scenarios such as home and hospital environments, where different QoS metrics and adaptive security methods and mechanisms will be analysed using game theory.

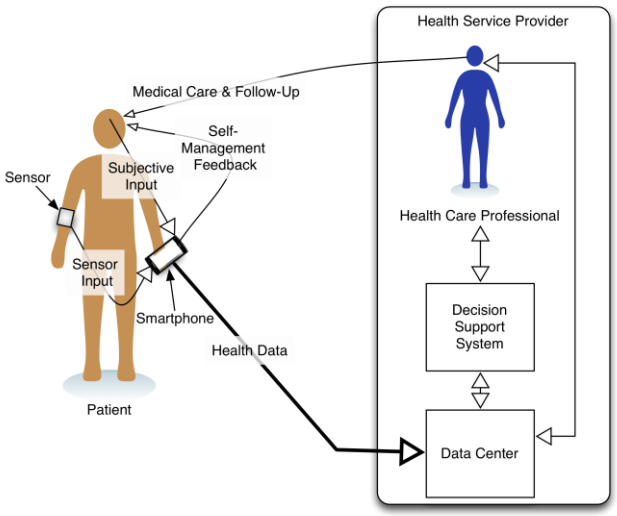

Figure 2. Patient monitoring case study.

We expect the case study to lead to the design of adaptive strategies for the dynamic interplay between security and data transmission in a mobile patient monitoring system. This will use information of link quality, data transmission rate, and processing capabilities of sensor nodes and smart phones. The security adaptation will take into account the various QoS metrics [7]. This will allow us to verify the necessary security and trust for the emerging IoTs in many e-Health applications in general and in the case study patient monitoring in particular. This will constitute a key innovator for future e-Health solutions in hospitals and health services.

Our analysis will also include the overhead cost of processing complexity on sensor nodes due to readjustment of the predictive models and adaptive security regime. The other overhead cost is additional data transmission due to transmission on the feedback

channels. The study will provide the tradeoff between desired QoS and security in bandwidth limited, battery driven wireless sensor networks.

5. CONCLUSIONS AND FUTURE WORK

In this paper, we have introduced an innovative risk-based adaptive security framework for IoT in eHealth to estimate and predict risk damages and future benefits, and to learn identified new or unknown threats to IoT eHealth systems. The framework is based on a continuous cycle of adaptive risk management, adaptive security monitoring, predictive analytics, automated adaptive decision-making, and evaluation and validation metrics.

Our future work includes the further development and prototyping of the models for estimating and predicting risks and benefits using game theory and context awareness, methodology for security measurement and metrics for validating the effectiveness of the adaptation, and light-weight abilities in smart things that will allow them to detect in real-time unknown security and privacy threats, respond to them, and adapt to the environment and changing degree of security and privacy breaches. It also includes validating them in a simulated eHealth patient monitoring scenarios described above.

6. ACKNOWLEDGMENTS

The work presented here has been carried out in a research project ASSET – Adaptive Security for Smart Internet of Things in eHealth (2012–2015) funded by The Research Council of Norway. We wish to thank our colleagues involved in this project for their related work and for helpful discussions that made this study possible.

7. REFERENCES

[1] Abie, H. 2009. Adaptive Security and Trust Management for Autonomic Message-Oriented Middleware. In *IEEE 6th Int. Conf. on Mobile Adhoc and Sensor Systems (MASS '09)*, (12-15 Oct. 2009), 810-817

[2] Abie, H. Savola, R., Bigham, J. et al. 2010. Self-Healing and Secure Adaptive Messaging Middleware for Business Critical Systems. In *Int. J. on Advances in Security*, 3, 1&2, (September 5, 2010), 34-51.

[3] Atzoria, L., Ierab, A., and Morabito, G. 2010. The Internet of Things: A survey. *Computer Networks*, 54, 15, (8 October, 2010), 2787-2805.

[4] Cheng, P. C., Rohatgi, P., Keser, C. et al. 2007. *Fuzzy multi-level security: An experiment on quantified risk-adaptive access control*. Technical Report RC24190, IBM Research.

[5] Hausken, K. 2002. Probabilistic Risk Analysis and Game Theory. *Risk Analysis*, 22, 1, 17-27.

[6] Hong, J., Ng, J., Lederer, S., and Landay, J. 2004. Privacy risk models for designing privacy-sensitive ubiquitous computing systems. In *D. Benyon; P. Moody; D. Gruen and I. McAra-McWilliam (Eds.): Proc. of the 2004 conference on Designing interactive systems: processes, practices, methods, and techniques*, (August 1, 2004), NY, 91-100.

[7] Leister, W., Schulz, T., Lie, A., et al. 2011. Quality of Service, Adaptation, and Security Provisioning in Wireless Patient Monitoring Systems, Quality of Service, Adaptation, and Security Provisioning in Wireless Patient Monitoring Systems. *Biomedical Engineering, Trends in Electronics, Communications and Software*, Ed. Anthony N. Laskovski, InTech, (January 2011), 711-736.

[8] Lim, Y. T., Cheng, P. C., Rohatgi, P., and Clark, J. A. 2008. MLS security policy evolution with genetic programming. In *GECCO '08: Proc. of the 10th annual conference on Genetic and evolutionary computation*, NY, ACM, 1571-1578.

[9] Mccgraw, R.W. 2009. Risk-Adaptable Access Control (RAdAC), http://csrc.nist.gov/news_events/privilege-management-workshop/presentations/Bob_McGraw.pdf, (retrieved 30.06.2012)

[10] Ni, Q., Lobo, J., Calo, S. B. et al. 2009. Automating role-based provisioning by learning from examples. In *Barbara Carminati and James Joshi, editors, SACMAT*, ACM, 75-84.

[11] Ni, Q., Bertino, E., and Lobo, J. 2010. Risk-based Access Control Systems Built on Fuzzy Inferences. In *ASIACCS'10* (Beijing, China, April 13–16, 2010), 250-260.

[12] Ovidiu, V., Harrison, M., Vogt, H. et al. 2009. *Internet of Things Strategic Research Roadmap*. Cluster of European Research Projects on the Internet of Things, CERP-IoT.

[13] Poslad, S. 2009. *Ubiquitous Computing: Smart Devices, Environments and Interactions*. Wiley, ISBN: 978-0-470-03560-3, 2009.

[14] Rajbhandari, L. and Snekkenes, E. 2011. Mapping between Classical Risk Management and Game Theoretical Approaches. In *Proc. of 12th Joint IFIP TC6 and TC11 Conf. on Communications and Multimedia Security (CMS 2011)*, 147-154.

[15] Rajbhandari, L. and Snekkenes, E. 2011. Using Game Theory to Analyze Risk to Privacy. In *An Initial Insight, Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology*, 352, 41-51.

[16] Savola, R. and Abie, H. 2009. Development of Measurable Security for a Distributed Messaging System, *In: Int. J. on Advances in Security*, 2, 4, ISSN 1942-2636, (Published in March 2010), 358-380.

[17] Srivatsa, M., Balfe, S., Paterson, K. G., and Rohatgi, P. 2008. Trust management for secure information Flows. *In P. Ning, P. F. Syverson, and S. Jha, editors, ACM Conference on Computer and Communications Security*, ACM, 175-188.

[18] Webera, R. H. 2010. Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26, 1, (January 2010), 23-30.

[19] Chorppath, A.K. and Alpcan, T. 2012. Risk Management for IT Security: When Theory Meets Practice. In *5th Int. Conference on New Technologies, Mobility and Security (NTMS 2012)*, 1-5.

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

[21] Nachira, F., Dini, P., and Nicolai, A. 2007. *A network of digital business ecosystems for Europe: roots, processes and perspectives.* European Commission, Brussels, Introductory Paper.

[22] Felten, E. 2003. DRM and the First Rule of Security Analysis. Freedom to Tinker (2003), http://www.freedom-to-tinker.com/index.php?p=317. (Retrieved 28.06.2012)

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

[24] Roman,R., Najera, P., and Lopez, J. 2011. Securing the Internet of Things. In *IEEE Computer*, 44, 9, 51-58.

[25] Suo, H., Wan, J., Zou C., and Liu, J. 2012. Security in the Internet of Things: A Review. In *Int. Conf. Computer Science and Electronics Engineering (ICCSEE)*, 3, 648-651.

[26] Medaglia, C. M., and Serbanati, A. 2010. An Overview of Privacy and Security Issues in the Internet of Things. In *The Internet of Things*, 5, 389-395.

[27] Abie, H. 2012. Risk Analysis, Risk Assessment, Risk Management, http://www.nr.no/~abie/RiskAnalysis.htm, (retrieved 26.06.2012).

[28] Hadzic, M. and Dillon, T.S. 2008. Application of Digital Ecosystems in Health Domain. In *2008 Second IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2008)*, 543-547.

[29] Beres, Y., Mont, M.C., Griffin, J., and Shiu, S. 2009. *Using Security Metrics Coupled with Predictive Modelling and Simulation to Assess Security Processes*. Technical Report, HPL-2009-142, HP Laboratories.

[30] Jafari, S., Mtenzi, F., Fitzpatrick, R., and O'Shea, B. 2010. Security metrics for e-healthcare information systems: a domain specific metrics approach, *Int. Journal of Digital Society*, 1, 4, (December 2010), 238–245.

[31] Bier, V. M. and Azaiez M. N. 2008. Game Theoretic Risk Analysis of Security Threats, Springer, 236 pages.

[32] Cox, L. A. 2009. Game Theory and Risk Analysis. Risk Analysis, 29(8), 1062-1068.

[33] Maillé , P., Reichl, P., and Tuffin, B. 2011. Of Threats and Costs: A Game-Theoretic Approach to Security Risk Management, N. Gülpınar et al. (eds.), Performance Models and Risk Management in Communications Systems, Springer Optimization and Its Applications, 46, 33-53.

[34] [Manshaei 2010] Manshaei, M. H., Zhu, Q., Alpcan, T., Basar, T., and Hubaux, J-P. 2010. Game Theory Meets Network Security and Privacy, ACM Computing Surveys, December 2011.