An Evaluation Framework for Adaptive Security for the IoT in eHealth

Wolfgang Leister
Norsk Regnesentral
Oslo, Norway
wolfgang.leister@nr.no

Mohamed Hamdi
School of Communication Engineering
Tunisia
mmh@supcom.rnu.tn

Habtamu Abie
Norsk Regnesentral
Oslo, Norway
habtamu.abie@nr.no

Stefan Poslad
Queen Mary University
London, UK
stefan.poslad@qmul.ac.uk

Arild Torjusen
Norsk Regnesentral
Oslo, Norway
arild.torjusen@nr.no

***Abstract*—We present an assessment framework to evaluate adaptive security algorithms specifically for the Internet of Things (IoT) in eHealth applications. The successful deployment of the IoT depends on ensuring security and privacy, which need to adapt to the processing capabilities and resource use of the IoT. We develop a framework for the assessment and validation of context-aware adaptive security solutions for the IoT in eHealth that can quantify the characteristics and requirements of a situation. We present the properties to be fulfilled by a scenario to assess and quantify characteristics for the adaptive security solutions for eHealth. We then develop scenarios for patients with chronic diseases using biomedical sensors. These scenarios are used to create storylines for a chronic patient living at home or being treated in the hospital. We show numeric examples for how to apply our framework. We also present guidelines how to integrate our framework to evaluating adaptive security solutions.**

***Keywords*—Internet of Things; evaluation framework; scenarios; assessment; eHealth systems; adaptive security.**

I. Introduction

Wireless Body Sensor Networks (WBSNs) improve the efficiency of eHealth applications by monitoring vital signs of a patient using low-rate communication media and constitute an important part of the Internet of Things (IoT) by bringing humans into the IoT. However, the successful deployment of the IoT depends on ensuring security and privacy, which need to adapt to the processing capabilities and resource use of the IoT. To evaluate such adaptive mechanisms we introduced evaluation scenarios specifically designed for applications in eHealth and proposed an evaluation framework [1]. This evaluation framework is extended in this study with a quantitative component that allows us to quantify the quality of security solutions.

The "Adaptive Security for Smart Internet of Things in eHealth" (ASSET) project researches and develops risk-based adaptive security methods and mechanisms for IoT that will estimate and predict risk and future benefits using game theory and context awareness [2]. The security methods and mechanisms will adapt their security decisions based upon those estimates and predictions.

The main application area of ASSET is health and welfare. Health organisations may deploy IoT-based services to enhance traditional medical services and reduce delay for treatment of critical patients. In a case study, we evaluate the technologies we developed for adaptive security using both simulation and implementation in a testbed based upon realistic cases. Blood pressure, electrocardiogram (ECG) and heart rate values can be gathered from patients and anonymised. The sensor data can be stored in different biomedical sensor nodes that are capable of communicating with any of the following connectivity options ZigBee, Wi-Fi, 3G, GPRS, Bluetooth, and 6LoWPAN. For instance, a smartphone with a suitable transceiver could act as an access point between sensor nodes and a medical centre. For the evaluation, we developed a set of scenarios to assess the adaptive security models, techniques, and prototypes that will be introduced in ASSET. These scenarios describe the foreseeable interactions between the various actors and the patient monitoring system based on IoT.

In computing, a scenario is a narrative: it most commonly describes foreseeable interactions of user roles and the technical system, which usually includes computer hardware and software. A scenario has a goal, a time-frame, and scope. Alexander and Maiden [3] describe several types of scenarios, such as stories, situations (alternative worlds), simulations, story boards, sequences, and structures. Scenarios have interaction points and decision points where the technology under consideration can interact with the scenario. This means that the scenarios developed for a particular situation have to take into consideration the technologies used by the different actors. The importance of scenarios in the assessment of security solutions has been discussed in the literature [4], [5]. This work focuses on the development of scenarios that support the evaluation of adaptive security techniques for the IoT in eHealth.

There are many definitions of the IoT. For instance, while the ITU-T [6] defines the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies", the European Research Cluster on the Internet of Things (IERC) defines the IoT as "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where

physical and virtual *things* have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network" [7]. For our purposes we use Abie and Balasingham's shorter definition: "IoT is a network of things" [2]. Habib and Leister [8] present a review of IoT layer models, including the ITU-T IoT reference model [6].

The primary contributions and advances of this study are the development of a quantitative framework for the assessment of adaptive security solutions on the basis of security, privacy, Quality of Service (QoS) requirements, and costs.

In Section II, the requirements and the proposed assessment framework are described including metrics that make this framework quantifiable in order to enable comparison of various situations. We define the properties that must be fulfilled by a scenario to assess adaptive security schemes for eHealth. We show the interaction between the scenarios, the threats, and the countermeasures in an assessment framework for the ASSET project.

In Section III, we describe the extension of a previously developed generic system model, which is used for the structure of the scenarios in Section III-A with different QoS requirements, contexts and adaptive security methods and mechanisms. These scenarios, first proposed by Leister et al. [9], include a patient monitored at home scenario, a hospital scenario, and an emergency scenario. These scenarios are reviewed and their adequacy to the evaluation of adaptive security techniques for the IoT is analysed. We propose storylines that can support requirements analysis, as well as adaptive security design, implementation, evaluation, and testing.

Further, in Section IV, we present storylines for both the home monitoring scenario and the hospital scenario. These storylines are used in Section V to show how our framework can be applied to selected episodes of the home scenario and storyline. In Section VI, we show how to use our framework in the context of adaptive security as defined by Abie and Balasingham [2]. Finally, Section VII discusses our framework and relates it to other work before Section VIII offers concluding remarks and future prospects.

II. The ASSET Evaluation Framework

Designing the scenarios is of central significance for the ASSET project. They depict the operation of systems, here applied to IoT-based eHealth systems, in the form of actions and event sequences. In addition, scenarios facilitate the detection of threats and the identification of the solutions to cope with these threats. In a scenario-based assessment, a set of scenarios is developed to convey the design requirements. With regard to the specific objectives of IoT-based systems, the scenarios should capture two types of requirements:

1) *Security requirements:* Novel adaptive security and privacy mechanisms and methods are required to adapt to the dynamic context of the IoT and changing threats to them. Thus, the scenarios should be generic enough to capture the security needs for the data processed and exchanged within a patient monitoring system. This is particularly challenging because this system encompasses multiple networking technologies, data, users, and applications, addressing varying processing capabilities and resource use.

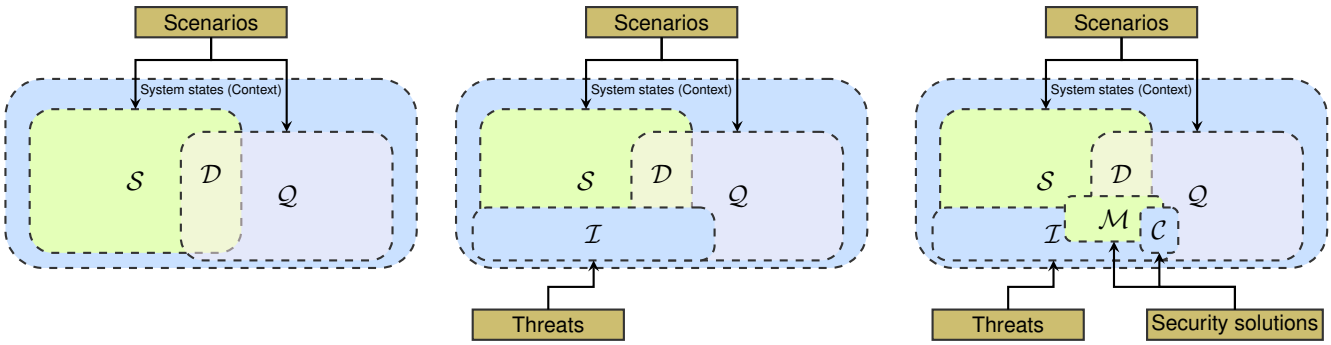
   In an assessment context, privacy and security requirements are related. Privacy addresses the ability to control the information one reveals about oneself over the Internet and who can access that information.
2) *QoS requirements:* QoS addresses the overall performance of a system regarding technical parameters. Unlike many traditional applications and services relying on communication networks, eHealth applications have stringent QoS requirements. Items such as the communication delay, the quality of the communication channels, and the lifetime of the self-powered sensor nodes are crucial context parameters that have significant impact on the safety of the patient. The scenarios should highlight the needs in terms of QoS requirements and illustrate the dynamic interplay between these needs and the security requirements.

Security and QoS mechanisms are interrelated. Adaptation of security mechanisms may impact the QoS and vice-versa. QoS requires adaptive security mechanisms to ensure appropriate level of QoS. While adapting poor security mechanisms can hamper the performance of QoS, an inappropriate QoS level can leak sensitive information about the importance of the service in question. Therefore, adaptation must consider both security and QoS together to achieve the best possible security and QoS levels. Otherwise, weaker security and/or less effective QoS guarantees may be the result. For example, the requirement of using stronger cryptographic algorithms could have negative impact on the performance or battery consumption.

A. Requirements and Sets of States

The ASSET scenarios appear as a component of an assessment framework that will serve to improve the applicability of the security techniques proposed in the frame of the project. The other components of the assessment framework are (*i*) a set of threats describing the actions that violate the security requirements, (*ii*) a set of security solutions that mitigate the threats, and (*iii*) a set of system states representing the dynamic context in which the patient monitoring system operates. Fig. 1 illustrates the ASSET assessment framework. The security and QoS requirements are the output of the scenario design activity. In other terms, the scenarios should give information about the set of reliable states from the security requirements, here denoted as $\mathcal{S}$, and the set of states where the QoS is acceptable, here denoted as $\mathcal{Q}$. The intersection of these sets is the set of desirable states, denoted in Fig. 1(a) by $\mathcal{D}$ (Desirable), where the security and QoS requirements are balanced.

One of the intrinsic features of the ASSET scenarios is that the sets of security requirements and QoS requirements could vary in time and space. This will make the threats and the security solutions also vary in time and space. Threats



(a) (b) (c)

Fig. 1: The ASSET assessment framework.

are viewed as potential events that may generate insecure system states, while countermeasures are intended to thwart the effects of these threats. The realisation of a threat reduces the set of secure states in the scenario of interest and affects the QoS. This is represented by the region $\mathcal{I}$ (Impact) in Fig. 1(b). This region represents a set of states that will not fulfil the security or QoS requirements if a threat is realised. The countermeasures or *controls* [10] will reduce both the likelihood of a threat being realised and the impact of an emerging threat. Hence, the size of the set of potentially insecure states is decreased. Fig. 1(c) illustrates the effect of the countermeasures through the Region $\mathcal{M}$ (Mitigate). This region extends the set of secure states. Nonetheless, the countermeasures can have a negative effect on the QoS, represented by the region $\mathcal{C}$ (Cost), consisting of power, processing resources, memory, communication overhead, and cases where QoS requirements may not be fulfilled.

These elements are used in a scenario-based assessment framework to evaluate the strength of the adaptive security solutions. For instance, the scenarios allow us to evaluate the strength of the security controls to minimise the impact of threats in a given context.

For adaptive security solutions, the proposed protection techniques will vary in time and space according to the context. This is not conveyed by the scenario representation of Fig. 1. To overcome this issue, we derive a set of storylines from the ASSET scenarios. These can be viewed as a sequential application of the scenarios in a way that the selection of the appropriate countermeasures must take into consideration:

- *The space transition between scenarios.* Space encompasses much useful information that affect the security decision-making process. For instance, the location of the WBSN may increase/decrease its vulnerability. Moreover, mobility introduces significant challenges including horizontal and vertical handover management, i.e, managing handover on the same layer or within the same access technology and between different layers or different access technologies, respectively.
- *The time transitions between scenarios (with its implications on the context).* The time interplay between the threats and countermeasures has a substantial and dynamic impact on the environment where the patient monitoring system is deployed. The amount of energy, memory, and processing resources are crucial parameters from the QoS perspective and the security solutions have to adapt accordingly. In addition, the state of the communication channel and the proper temporal interplay in all these contexts are important in the selection of the appropriate security decisions.

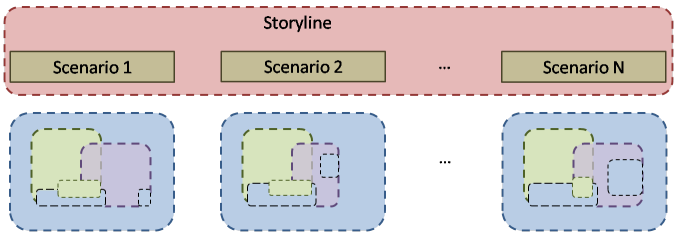


Fig. 2: Illustration of context changes during the execution of a storyline. The use of the different shaded regions follows that of Fig. 1

Fig. 2 illustrates the evolution of the storyline and the underlying impact on the context. Of course, the sequence of scenarios forming a storyline should be consistent so that it translates to a real-case situation.

B. Making the ASSET Framework Quantifiable

Assessing the qualities of a given system state can be done by means of data given by human assessors and by means of objective data from measurements. Our goal is to establish an estimation function that takes measured data as input and which is a prerequisite to implement functionality for adaptive security. To establish such an estimation function the assessment a panel of users and specialists is queried to calibrate a function that uses measured data as input. Similar methodology has been used to estimate the quality of streamed video [11]. In the following we present how to assess a given system state by using human assessors.

To make the ASSET framework quantifiable we define a real function $0 \leq q(\text{system state}) \leq 1$ that shall express

the degree of how well the requirements are fulfilled in the system state in question. A low value, below a given threshold, denotes that the system state in question is unacceptable, while a value close to 1 denotes that most requirements are well fulfilled.

The function q is composed of three parts: *1*) security requirements that need to be fulfilled, expressed in the function q_S; *2*) degree of fulfilled QoS requirements, expressed in the function q_Q; and *3*) costs that occur due to mitigation of threats. The function q is then composed of a product of all partial functions of $q_{i\in\{S,Q,C\}}$: $q = \prod_i {q_i}^{w_i}$. The weights are real numbers $0 \leq w_i < \infty$ and express the importance of a single q_i, large values indicating more importance. A weight $w_i = 1$ is considered neutral. The importance of each parameter is defined by the assessor according to the nature of the requirement before assessing the q_i values.

The above definition has the disadvantage that the resulting q is sensitive to the number k of factors q_i that are used to define it. To mitigate this we propose to replace the weights by $v_i = \frac{w_i}{\sum_{j=1}^{k} w_j}$ resulting in $\hat{q}_i = {q_i}^{\frac{w_i}{\sum_{j=1}^{k} w_j}}$. Thus, the value q is expressed by:

$$q = \prod_i \hat{q}_i = \prod_i {q_i}^{\frac{w_i}{\sum_{j=1}^{k} w_j}} \tag{1}$$

1) Security Requirements: Define $\mathcal{G}_\mathcal{S} = (\mathcal{S} \setminus \mathcal{I}) \cup \mathcal{M}$ as a set of states where security requirements are fulfilled or threats are mitigated. For states j outside $\mathcal{G}_\mathcal{S}$ we define a deviation from the ideal requirements and a normalised distance $d_{S_j} : 0 \leq d_{S_j} \leq 1$ according to a suitable metric to denote how far the current state is from ideal fulfilment of the requirement. We set $d_{S_j} = 1$ when deviations cannot be tolerated. Thus, we define the following function:

$$q_{S_j} = \begin{cases} 1 & \text{if state } \in \mathcal{G}_\mathcal{S} \\ 1 - d_{S_j} & \text{if state } \notin \mathcal{G}_\mathcal{S} \end{cases}$$

2) QoS Requirements: Define $\mathcal{G}_\mathcal{Q} = \mathcal{Q} \setminus \mathcal{C}$ as a set of states where all QoS requirements are fulfilled and possible effects from the mitigation are tolerable. For states j outside $\mathcal{G}_\mathcal{Q}$ we define a deviation from the ideal QoS requirement and a normalised distance $d_{Q_j} : 0 \leq d_{Q_j} \leq 1$ according to a suitable metric to denote how far the current state is from ideal fulfilment of the requirement. We set $d_{Q_j} = 1$ when QoS requirements are insufficiently fulfilled.

QoS requirements may be unfulfilled due to influences from the environment, or become unfulfilled due to adaptation. The latter could, for instance, happen if a security requirement to avoid eavesdropping was met by reducing signal strength, which could impact the available bandwidth or even data availability.

Thus, we define the following function:

$$q_{Q_j} = \begin{cases} 1 & \text{if state } \in \mathcal{G}_\mathcal{Q} \\ 1 - d_{Q_j} & \text{if state } \notin \mathcal{G}_\mathcal{Q} \end{cases}$$

3) Mitigation Costs: Besides the effect on QoS there may be other costs implied by mitigation, e.g., real costs in payroll or material, changes to the environment, costs for the patient, virtual costs for a lower QoS, and so on. States with unacceptable costs are included in the area $\mathcal{C}$. For costs outside $\mathcal{C}$ we define relative costs on a normalised scale $d_C : 0 \leq d_C \leq 1$. We define the following function:

$$q_C = \begin{cases} 1 - d_C & \text{if costs } \notin \mathcal{C} \\ 0 & \text{if costs } \in \mathcal{C} \end{cases}$$

C. Assessment to define the q_i values

To aid human assessors in assessing the values for q_i (i.e. the value indicating how far a given requirement is from the ideal fulfilment) we propose to base the assessment on a set of questions that are evaluated based on a Likert scale [12]. A Likert scale is a psychometric scale commonly involved in research that employs questionnaires where the questions are to be answered from *best* to *worst* on a scale of n steps, where n is an odd integer number.

If the questionnaire to be filled out by an assessor is designed so that each q_i corresponds to one question on a Likert scale we propose to use a function e that takes the response $\tilde{q}_i \in \mathbb{N}$ for $0 \leq \tilde{q}_i \leq n - 1$ as an argument. We use two approaches to express the q_i.

1) Linear Approach:

$$q_i = e_\alpha(\tilde{q}_i) = \frac{\tilde{q}_i}{n - 1} \tag{2}$$

2) Logarithmic Approach:

$$q_i = e_\beta(\tilde{q}_i) = \log_n (\tilde{q}_i + 1) \tag{3}$$

Using the logarithmic approach leaves less impact of bad values than the linear approach. There are some caveats on using a logarithmic function for values on a Likert scale, as noted by Nevill and Lane [13]. Particularly, the values on the Likert scale should express a continuous and rather equidistant increase of quality.

3) Other Methods: In case the questionnaire is designed in a way that several independent questions result in one value for q_i, Bayesian networks developed by Perl and Russell [14] can be employed. However, we consider the design of the questionnaires and the use of Bayesian networks as future work. Note also that for Bayesian networks more data from an assessment are necessary than for the above mentioned methods.

While the Likert scale is useful for assessing opinions on a psychometric scale, i.e., subjective data, we need, as well, to be able to assess objective data. In these cases, we set up a scale where discrete choices on a questionnaire are mapped to a similar scale as the Likert scale to reflect the quantity of data based on an objective value. This way of creating assessment data are quite common for assessments, such as in the estimation of the quality of software products in the OpenBRR [15, 16].

When objective data are used as input, e.g., as the result of measurements, these data on a continuous scale can be mapped

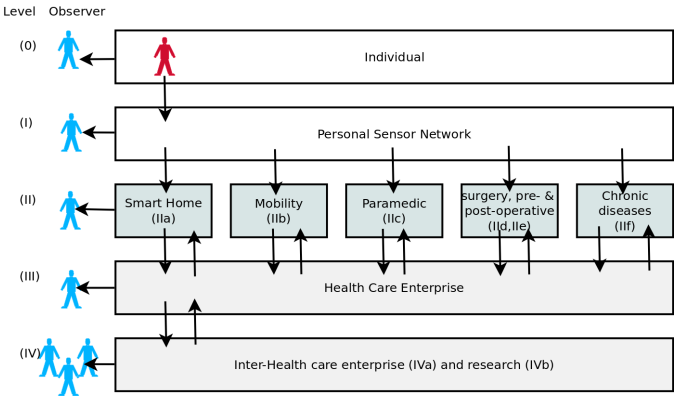


Fig. 3: Generic eHealth framework indicating the use cases in five levels (Extended from [17]).

into the value range $0 \leq q_i \leq 1$ and used in eq. (1). Note, however, that the mapping function does not necessarily need to be linear, and a specific assessment phase may be necessary to develop a suitable function that maps the values into the value range $0 \leq q_i \leq 1$.

4) Assessment by Subject Panels: For an assessment often several individuals are put into an assessment panel. These subjects perform the assessment individually while the results are put together into one assessment result. Further work needs to show whether it is more practicable to calculate individual q values and then calculate some mean value of these or whether to calculate mean values for each $\tilde{q}_i$.

III. Extended Generic Model for eHealth Scenarios

In the following sections, we develop the scenarios of the ASSET project and show how storylines can be extracted. We also underline the role of the storyline in the assessment of adaptive security techniques for eHealth. Before delving into the details of scenario and storyline engineering, we highlight the major properties that a scenario should have in order to be useful for evaluating adaptive security.

Patient monitoring systems are a major data source in healthcare environments. During the last decade, the development of pervasive computing architectures based on the IoT has consistently improved the efficiency of such monitoring systems thereby introducing new use cases and requirements. It is important that these monitoring systems maintain a certain level of availability, QoS, and that they are secure and protect the privacy of the patient. Previously, we have analysed the security and privacy for patient monitoring systems with an emphasis on wireless sensor networks [17] and suggested a framework for providing privacy, security, adaptation, and QoS in patient monitoring systems [18]. We divided patient monitoring systems into four Generic Levels (GLs): (0) the patient; (I) the personal sensor network; (II) devices in the closer environment following several scenarios; and (III) the healthcare information system.

We review the generic model presented by Leister et al. [18] and extended by Savola et al. [19]. This extended generic model contains three new levels related to the monitoring of chronic diseases, the communication between multiple healthcare providers, and the communication between healthcare providers and medical research institutions, respectively. Consequently, the extended generic model is composed of five levels numbered from (0) to (IV) depending on the logical distance to the patient to whom Level (0) is assigned. Multiple types are considered at Level (II). Note that only one of these types applies at a time. However, it must be possible to switch between the types in Level (II) depending on the activity of the patient. To this purpose, the communication between Levels (II) and (III) is two-way. The key levels of our extended generic model are as follows, as shown in Fig. 3:

(0) **Patient.** This is the actual patient.

(I) **Personal sensor network.** The personal sensor network denotes the patient and the sensors measuring the medical data. These sensors are connected to each other in a WBSN. While this sensor network can be connected randomly, in most cases one special WBSN node is appointed to be a Personal Cluster Head (PCH), which forwards the collected data outside the range of the WBSN.

(IIa) **Smart home.** The patient is in a smart-home environment where the personal sensor network interacts with various networks and applications within this environment. The smart home infrastructure may be connected to a healthcare enterprise infrastructure using long-distance data communication.

(IIb) **Mobility.** The patient is mobile, e.g., using public or personal transportation facilities. The personal sensor network of the patient is connected to the infrastructure of a healthcare enterprise via a mobile device, e.g., a mobile Internet connection.

(IIc) **Paramedic.** The WBSN is connected to the medical devices of an ambulance (car, plane, and helicopter) via the PCH. The devices of the ambulance can work autonomously, showing the patient status locally. Alternatively, the devices of the ambulance can communicate with an external healthcare infrastructure, e.g., at a hospital.

(IId) **Intensive care/surgery.** During an operation the sensor data are transferred to the PCH or directly to the hospital infrastructure over a local area network. The sensors are in a very controlled environment, but some sensors may be very resource limited due to their size, so extra transport nodes close to the sensors may be needed.

(IIe) **Pre- and postoperative.** During pre- and postoperative phases of a treatment, and for use in hospital bedrooms, the sensor data are transferred from the sensor network to the PCH and then to the healthcare information system.

(IIf) **Chronic disease treatment.** The WBSN data are

used by healthcare personnel in non-emergency treatment of individual patients with a chronic disease.

(III) **Healthcare information system.** This is considered a trusted environment. It consists of the hospital network, the computing facilities, databases, and access terminals in the hospital.

(IVa) **Inter-healthcare provider.** Information is shared between different healthcare providers concerning medical information of an individual patient.

(IVb) **Healthcare provider and research.** Information is shared between healthcare providers and medical research organisations for the purposes of research, new solutions development, etc.

A. The Structure of the Scenarios

Through the potential interactions between these levels, notice that the model can support the elaboration of multiple scenarios where the actors interact by switching from a level to another. The scenarios in healthcare using biomedical sensor networks are quite complex. Therefore, they need to be efficiently structured. We consider three main scenarios (hereafter denoted as *overall scenarios*) and we decompose them into sub-scenarios (hereafter denoted as *core scenarios*). A particular interest is given to the transitions between the core scenarios since these transitions constitute substantial sources of threats. Here, we consider three scenarios, a home scenario A shown in Fig. 4, a hospital scenario B shown in Fig. 6, as well as an emergency scenario C.

Each of these overall scenarios contain a set of core scenarios which are denoted by the scenario identifier A, B, or C, followed by a dash and the core scenario numbering using roman numbers. The transitions between these core scenarios model the interaction between the various components of the patient monitoring system. In this paper, we focus mostly on Scenario A where the patient is supposed to be monitored outside the hospital while performing normal daily actions. To extract useful technical cases for the evaluation phase we need to structure the scenario according to the patient's actions and situation.

TABLE I shows a list of core scenarios used in our work, which overall scenario they belong to, and which transitions are useful. Note that other transitions are theoretically possible, but these are either unlikely or can be achieved by combining a series of transitions, e.g., taking Core Scenario A-ii (moving) as an intermediate for Overall Scenario A. Omitting unlikely transitions helps to reduce the number of states when modelling the scenarios.

B. The Structure of the Home Scenario

In Scenario A, a monitored patient can be in various contexts performing normal daily actions. For example, for a patient with diabetes the following situations apply:

- The patient is at home or a nursing home using monitoring equipment.
- The patient uses sensors and communicates electronically with the doctor's office.

TABLE I: Overview of core scenarios. The bullets mark scenarios that are part of the respective core scenario.

core scenario & name		scenario A	B	C	transition to core scenario
i	home monitoring	•			ii, xiv
ii	moving	•			i, iii, iv, viii, vi, v
iii	public transport	•			ii
iv	vehicle transport	•			ii
v	shop	•			ii
vi	café	•			ii
vii	doctor's office	•			ii, xiv
viii	waiting room	•	•		vii, ix, ii
ix	diagnosis		•	•	x, xi, xii, ii
x	operation		•		xi
xi	intensive care		•		xii
xii	observation		•		ii, xi, ix
xiii	accident			•	xiv
xiv	ambulance			•	ix

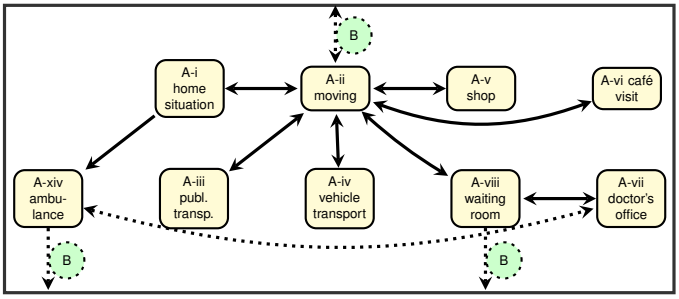


Fig. 4: The Home Scenario with the underlying core scenarios and their transitions.

- The patient uses specific monitoring equipment for diabetes.
- The patient visits the doctor's office regularly and uses public transport or a car to get there.
- At the waiting room the patient can communicate data to the health care infrastructure of the doctor's office.
- The patient regularly takes walking or jogging trips.
- The patient regularly visits a café with friends; this includes walking or commuting with public transport.
- In case of an emergency or planned surgery, not necessarily related to her condition, the patient may be sent to a hospital with an ambulance.

This list of situations is not yet a useful narrative. It needs to be structured and enriched with the specific context information, such as the necessary devices of the IoT, the communication channels, and actions of the involved actors. This is done in the core scenarios that describe a specific part of an overall scenario; e.g., a situation a patient experiences. Each core scenarios can be part of several overall scenarios.

1) Home Situation (monitored at home) (A-i): Biomedical sensors are employed in an environment where the patient is at home or in a nursing home. The patient is monitored by a WBSN, and the sensor data and alarms can be transmitted to medical centres and emergency dispatch units. The patient uses a smartphone with health-diary software that also imple-

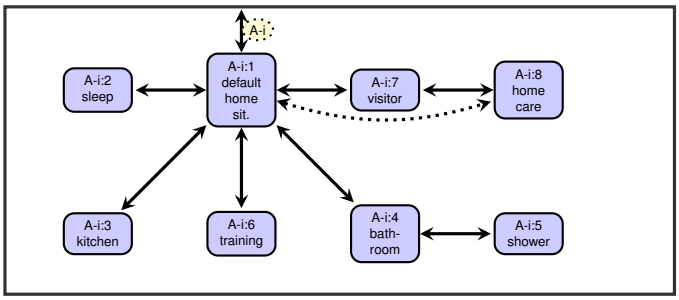


Fig. 5: The detail-scenarios of the home-situation.

ments personal health records (PHR) and stores measurements continuously.

Here, the sensors may not be monitoring or transmitting the physiological patient data continuously in order to reduce battery power consumption. Instead, depending on a predefined algorithm, abnormal sensor data from certain sensors may activate an alarm that is sent to a central monitoring unit.

On a regular basis, the patient transmits measurements to the medical information system at the doctor's office, thus synchronising the PHR with the medical information system; the patient also has an audio-/video-conversation where medical questions are discussed. During these sessions the patient may take pictures with the smart phone camera or perform other measurements.

In this scenario, the following characteristics are given:

1) Ease of use and non-intrusiveness are important issues.
2) Very low power consumption, enabling a long life span of the batteries, is required.
3) A network infrastructure is available, such as access to the Internet via LAN, WLAN, or mobile networks.
4) Limited mobility, handoff is possible, but infrequent.
5) Privacy and observability of signals are important requirements.

Core Scenario A-i can be split up into several detail-scenarios that may depend on the patient's activities, time of the day, or context, as shown in Fig. 5. These sub-scenarios may include the generic scenario (A-i:1), sleeping (A-i:2), kitchen work (A-i:3), visiting the bathroom (A-i:4), taking a shower (A-i:5), training (A-i:6), receiving a visitor (A-i:7), or receiving a home care nurse (A-i:8). All these detail scenarios create different challenges regarding security and QoS that need to be addressed by adaptive security methods. For example, when taking a shower, the sensors may need to be unmounted, while receiving visitors may create the need to give access to selected data or devices.

2) Moving (Walking, Jogging, Cycling) Scenario (A-ii): The patient does daily training, i.e., jogs in the nearby park, or does shorter walks from the home to the public transport, to the café, shop, or doctor's office. A common feature in these situations is that the patient needs to use a smartphone as a device that collects sensor data, using the mobile networks to transmit the data. When walking, jogging, or taking a bicycle ride in the park many other people and their devices may interfere with the communication of the smartphone.

When walking in the woods, there may be several spots which are not covered by a mobile network. In this case, the signal is so weak that only emergency calls from another provider will work. While data traffic is not possible, SMS messages can be used to send data with very low bandwidth, possibly after several retries. For an average walking trip, this outage may last for some minutes. However, SMS is asynchronous and messages may take minutes to days to arrive. Thus, it may be quicker to wait until the user, if still mobile, moves to a region where there is network coverage.

3) Transport Scenarios: We consider two transport scenarios, one with public transport, and one with commuting by car.

Core Scenario A-iii presents a situation where a patient commutes to a doctor's office or to a café using public transport. Here, the patient needs to use a smartphone as a device that collects sensor data, using the mobile networks to transmit the data. Blind spots without connectivity to a mobile network, roaming, varying data transmission quality, etc., are parts of this scenario. This scenario can be applied to long-distance trains, planes, etc.

In Core Scenario A-iv the patient uses her own or another's (private) car to commute to a shop, a café, or the doctor's office. Here, the patient needs to use a smartphone as a device that collects sensor data, using the mobile networks or networks installed or used in the car to transmit the data. Blind spots without connectivity to a mobile network, roaming, varying data transmission quality, etc., are parts of this scenario.

4) Shop Scenario (A-v): Another situation defined by Core Scenario A-v is when the patient is in a shop. In addition to the conditions of A-vi, the patient is given the opportunity to check groceries to be compliant with the patient's diet and allergy-prohibition plans, access information from the shop, and use a shopping list.

5) Café Scenario (A-vi): The patient visits a café. Here, the patient needs to use a smartphone as a device that collects sensor data, using mobile networks or café's WLAN zone for data transfer. Switching between the WLAN and mobile networks may occur, the WLAN may be of varying quality, many other café visitors may interfere, or the WLAN may not actually be connected to the Internet.

6) Doctor's Office Scenario (A-vii): The patient is in the doctor's office, usually after some time in a waiting room (A-viii). Here, the patient can have extra sensors attached. These extra sensors, as well as the existing sensors, can communicate with the doctor's infrastructure either through the smartphone of the patient, or directly, depending on the needs. A doctor can change a sensor's characteristics, which requires the possibility to re-program the sensor devices.

7) Waiting Room Scenario (A-viii): The patient is in a waiting room at a doctor's office or a hospital. Patients that are known to the healthcare system can be connected from their smartphone to the healthcare network; here, specific actions for collecting data from the device or other preparations can

be performed. Once the patient is in the range of the waiting room, the smartphone can transfer large amounts of stored patient data directly to the infrastructure of the medical centre via short-range communication, instead of using long-range mobile communication.

8) Other scenarios: In the scenario structure we foresee that the patient can undergo a transition to other core scenarios in a different overall scenario in order to cover situations that else would be outside the scenario structure. For instance, a patient could get ill and be brought to a hospital in an ambulance (B-xiv) or an emergency situation happens (Scenario C). Note that the use of devices in the IoT could be different in Scenarios A, B, and C: as an example, in an emergency situation the use of one of the patient's own sensors would not be possible in all cases.

C. The Structure of the Hospital Scenario

In Scenario B, the biomedical sensors are used in a hospital environment. Here, the patient is located in an operating room (OR) or intensive care unit (ICU) while undergoing intensive monitoring of vital physiological parameters. Additional sensors may be required during this procedure to monitor other physiological parameters. The patient may be moved between different rooms during the treatment, e.g., from the OR to the ICU, but monitoring must continue. The sensor data may need to be transferred over different wireless networks. The system should be able to cope with a breakdown in sensor nodes, new software updates, wireless network traffic congestion, and interferences from other wireless networks and biomedical devices.

In Scenario B, a fixed network infrastructure is available between Levels (II) and (III) which can be accessed by the sink nodes of the biomedical sensor network. The scenario includes a complex communication environment. Interference from co-existing wireless networks, mobile networks, and various medical facilities is possible; this may reduce the performance of the transmission. The network topology in this scenario is fixed, but changes to the network topology may happen while patients are moving or being moved from one place to another, possibly causing handoff to other gateways. However, roaming to other networks is not part of this scenario in order to stay within the hospital domain.

Note that scenarios that seem to be similar in Scenario B and in Scenario A may have differences that are not obvious. Thus, one cannot use reasoning performed in one scenario in another without checking the context and other conditions. For instance, A-vii (doctor's office) could be different from a similar situation in a hospital (B-ix) since the hospital is connected to a different kind of network infrastructure. Usually, the primary healthcare points (doctor's office) and hospitals have different security requirements and policies.

1) Hospital Diagnosis Scenario (B-ix): The patient is examined; extra sensors are attached, and existing sensors on the patient may be accessed both directly and via the patient's smartphone. In addition, NFC tags are used to identify objects.

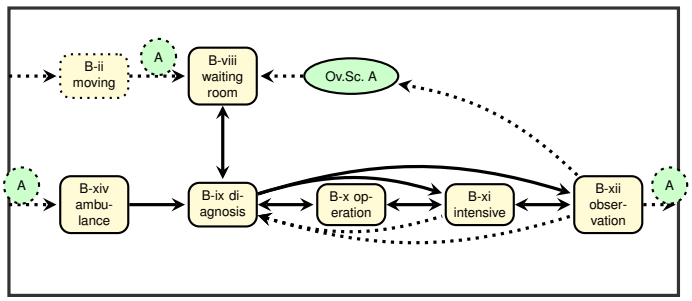


Fig. 6: The Hospital Scenario with the underlying core scenarios and their transitions.

The medical personnel can re-configure and re-program the sensors during diagnosis.

2) Hospital Operation Scenario (B-x): The patient is undergoing surgery; extra sensors are attached, and existing sensors on the patient are accessed directly by the hospital system rather than through the smartphone of the patient. In this scenario, the QoS is set very high, while security-wise the sensors are in a protected zone. The medical personnel can re-program the sensors during the operation.

3) Hospital Intensive Care Scenario (B-xi): The patient is in intensive care after an operation. Extra sensors are attached, and existing sensors on the patient may be accessed both through the patient's smartphone, and directly through the hospital infrastructure. In addition, NFC tags are used to identify objects. In most cases, the smartphone will be used as PCH. The medical personnel can re-program the sensors during intensive care.

4) Hospital Observation Scenario (B-xii): The patient is in a room under "normal" observation; in contrast to the home situation, the patient's smartphone has direct access to the hospital systems and will deliver data directly with higher QoS through the secured hospital systems.

D. The Structure of the Emergency Scenario

The Emergency Scenario (C) presents an emergency situation where victims are provided with sensors, patients are transported with an ambulance (car, helicopter, plane) and delivered to the emergency reception at a hospital. In Scenario C the use of sensors is not planned beforehand, health personnel must improvise, the identity of the patient may be unknown, and the infrastructure may be partially unavailable. Despite this, the expectation is that severely injured patients are stabilised, and they survive the transport to the emergency reception in the best condition possible.

We include the first scenario of the Hospital Scenario, the diagnosis phase when the patient arrives in Core Scenario C-ix. Here, the rather unplanned interventions at the emergency site are adapted to the routines at the hospital.

1) Accident Site Scenario (C-xiii): This scenario is a disaster and accident response scenario where biomedical sensors are deployed to measure values such as blood pressure, temperature, pulse and ECG in an ad-hoc network at the site of an accident. Wired or wireless communications infrastructures

may be damaged or unavailable, and a large number of severely injured people may overwhelm the emergency field personnel. This could prevent them from providing efficient and effective emergency rescue. Biomedical sensor networks can be quickly deployed to monitor vital signs. A large number of injured can be monitored simultaneously.

In this scenario, the following characteristics are given:

1) The sensor network must operate autonomously, and needs a high degree of self-organisation. The network topology is highly dynamic. Therefore, the sensor nodes should be able to discover each other and setup a sensor network autonomously.
2) A fixed network infrastructure is not available; data transferred from Level (II) to Level (III) must use a mobile network or other specific wireless network, such as microwave, or digital trunk communication.
3) The radio link may be unstable and the radio link quality may vary. Additionally, the communication environment is rather complex, since many sensor nodes may be deployed in a small area, possibly causing severe channel competition.
4) High degree of mobility. Handoffs are possible and may be frequent.
5) Blue-light functionality. That is, being able to re-use sensors on short notice with high flexibility (short-cutting some of the usual procedures).

2) Ambulance Scenario (C-xiv): The patient is in an ambulance. The sensors on the patient are connected to the ambulance's information system, which is connected to a hospital infrastructure via a mobile network connection. The communication between the patient's sensors is either directly to the ambulance infrastructure, or via the mobile phone. The ambulance and the patient's mobile phone may use different carriers. Some properties in this scenario are common with Scenario iv (vehicle transport).

Note that once the patient is inside the ambulance, sensors should communicate with devices in the ambulance without involving the mobile carrier.

IV. Storylines for the Scenarios

The set of overall scenarios, core scenarios, and transitions can be used to create *storylines* that can be used as case studies in ASSET. We present the storylines developed for the Scenarios A and B. Parts of these storylines will be used in the following analysis to evaluate the diverse functions in the IoT. We have not yet developed a storyline for Scenario C.

A. Storyline for the Home Scenario

We developed the storyline for the home scenario as follows: Petra has both a heart condition and diabetes. In a hospital, she had two sensors placed in or on her body: one heart sensor and one blood sugar sensor. In addition, she uses external sensors to measure blood pressure, heart beat, inertial sensors, etc., as well as a camera. Inertial sensors can be used to detect if Petra falls in order to automatically call for help while cameras could be used to assess her mood [20]. Petra is living in her home that has been prepared for the monitoring system and is commissioned with the necessary data connections so that her vital signs can be periodically reported to the healthcare personnel in levels (II) (nurse or doctor) or (III) (patient records) as introduced in Fig. 3; several technologies can be applied to achieve this.

The patient monitoring system is set up so that the sensor data are transmitted wirelessly (several transmission technologies are possible) to a smartphone that acts as PCH. The PCH communicates with the hospital infrastructure (Level (III)).

1. Petra is now being monitored at home but data are acquired remotely (A-i); the following requirements are important:
   a. Petra wants the data related to her medical condition to remain confidential from neighbours, i.e., people close-by, but outside her home. The confidentiality requirement includes physiological data, location data, data retrieved from a smart-home environment, such as temperature and humidity, as well as other metadata and health records.
   b. Petra wants her data to remain confidential from visitors, i.e., people inside her home.
2. Petra takes a bath in her home (planned sensor acquisition disruption; A-i);
   a. the sensors are water-proof; the PCH is close enough to receive signals;
   b. the sensors need to be removed;
      i. a change in the values implicitly indicates the sensor removal; or
      ii. patient must notify the PCH about the sensors going off-line;
3. Petra is sleeping and sensors fall off (unplanned sensor acquisition disruption; A-i).
4. Petra leaves her home for training outdoors or a stroll in the park nearby (A-ii);
   a. she is walking alone with her sensors communicating to the PCH;
   b. she meets an acquaintance, Linda who has similar sensor equipment; note that Petra's sensors could communicate through Linda's sensor network; they continue walking together;
   c. when they walk further, Petra looses the communication channel to the health care institution because of the terrain. She could either connect through the open, mobile WLAN-zones that are offered or use Linda's PCH as communication channel.
5. Petra leaves her home to visit her friends in a café (A-vi, A-ii, A-iii, A-iv).
6. Petra visits her regular doctor for a check-up; the doctor's office is within walking distance from her home (A-ii, A-vii, A-viii).
7. Petra becomes ill and is transported by an emergency ambulance to the hospital (B-xiv); transition to the Overall Hospital Scenario B.

B. Storyline for the Hospital Scenario

We developed the storyline for the hospital scenario as follows: Petra has both a heart condition and diabetes. One year ago, she had two sensors placed in or on her body: one heart sensor and one blood sugar sensor that both communicate wirelessly. In addition, she uses external sensors as described for the storyline of Scenario A. Petra suddenly gets ill while being at home. This is detected by the patient monitoring system installed at her home.

1. Petra is taken in an ambulance to the hospital (B-xiv). In addition to the sensors she is using, the paramedics use EEG and ECG sensors. The information from all sensors is available in the ambulance from three possible sources:
   a. information received directly from the sensors, available on the displays in the ambulance;
   b. information received from the PCH that Petra is using;
   c. information received from the healthcare records.
2. After the ambulance arrives at the hospital, Petra is moved to a room where diagnosis of her condition is performed (B-ix). Different sensors are used to find out her condition. These sensors are removed after diagnosis.
3. It becomes clear that Petra needs to undergo surgery (B-x). During surgery sensors are used to measure certain biomedical values. However, the medical procedure also creates electromagnetic noise in the same band as the data transmission between sensors uses.
4. After the surgery, Petra is moved to intensive care (B-xi) where a variety of sensors are used to observe her biomedical values.
5. After two days, Petra is moved to a recovery room with three other patients to allow time for her surgery wound to heal and for observation (B-xii). In addition to the heart and blood sugar sensors, two additional sensors are now used, but these will be removed after the observation phase is over. The two other patients in the same room are using the same kind of sensors.
   a. The sensors Petra is using transmit their readings to her PCH.
   b. Petra's additional sensors transmit their readings to a base station in the patients' room, while her ordinary sensors are still report to her PCH.
6. Petra is discharged from hospital; transition to Overall Scenario A.

C. Applying the Storylines

As described by Savola and Abie [21] and Savola et al. [19] the data integrity, privacy, data confidentiality, availability, and non-repudiation requirements should be met for all core scenarios and communication levels presented in Section III, specifically end-user authentication and authorisation for scenarios in Levels (0)-(II), sensor and WBSN authentication for scenario in Level (I), service provider user authentication for scenarios in Levels (III) and (IV), and service provider user authorisation in Levels (III) and (IV). This is also true for both storylines described above since these scenarios apply to both storylines but in varying situations and contexts. The adaptive security requirements for both storylines therefore can be summarised as follows:

1) End-user authentication and authorisation: The adaptive authentication mechanisms must cope with changing context of use, security threats and the user behaviour in order to enforce context-aware authentication mechanisms in an efficient and usable manner.

2) Sensor and WBSN authentication: Adaptive authentication mechanisms must cope with critical decisions to be made by the end-user and the service provider user based on the sensor input in order to minimise the possibility of fake sensors in possibly varying situations.

3) Service provider user authentication: Adaptive authentication mechanisms must cope with changing demands depending on the privacy level and the official authorisation level for making treatment decisions.

4) Service provider user authorisation: Adaptive authorisation techniques must cope with setting the adequate requirements and enforcing the sufficient authorisation mechanisms based on the strength of the authentication, context, and user role.

5) Data integrity (all levels): Adaptive data integrity techniques must maintain adequate data integrity especially during alarm situations allowing patients health security and longer-time treatment decisions

6) Privacy and data confidentiality (all levels): Adaptive security decision-making must adapt to privacy and data confidentiality requirements based on the data processing needs, roles of stakeholders, regulations and legislation, and the privacy level of data indicated by privacy metrics. Since context can affect privacy, adaptive security must be able to adapt to different types of context such as time, space, physiological parameter sensing, environmental sensing, and noisy data. The context must also be collected and evaluated in real time in a secure and accurate manner.

7) Availability (all levels): Adaptive techniques must balance the load in the system and use resilience solutions to maintain adequate availability, which is critical for health and life.

8) Non-repudiation (all levels): Adaptive authentication mechanisms must ensure the adequate non-repudiation level despite of changing conditions and selection of security controls.

Walking through these story lines or threat analysing them will show that the above adaptive security requirements must be met for their success and proper functioning. For example, the security requirement pointed out in Step 1.a of the storyline is related to confidentiality and privacy, which are often emphasised in healthcare. Strong confidentiality algorithms, key distribution, associated processes, and compliance to appropriate privacy legislation and regulations are crucial.

V. Evaluating the Home Scenario

We use selected parts of Scenario A to illustrate how to use the ASSET framework. We go through the scenario

TABLE II: Numeric results for Example 1: applying the ASSET framework using the logarithmic approach from eq. (3)

	S_1		S_2		S_3		S_4		Q_1		Q_2		C		q_{total}
w_i	0.4		0.8		2.0		1.0		1.0		1.5		1.0		$\sum = 7.4$
	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	$\tilde{q}$	$\hat{q}$	q_{total}
Case I	6	0.997	8	0.991	8	0.977	10	1.000	10	1.000	10	1.000	10	1.000	0.965
Case II	6	0.997	10	1.000	8	0.977	10	1.000	10	1.000	10	1.000	1	0.846	0.824
Case III	7	0.998	9	0.996	8	0.977	9	0.995	8	0.988	10	1.000	10	1.000	0.954
Case IV	6	0.997	8	0.991	10	1.000	10	1.000	8	0.988	9	0.992	10	1.000	0.968
Case V	6	0.997	8	0.991	9	0.989	10	1.000	9	0.995	10	1.000	10	1.000	0.972
Case III+IV	6	0.997	9	0.996	10	1.000	10	1.000	9	0.995	10	1.000	10	1.000	0.987

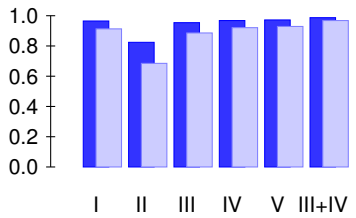


Fig. 7: Visualising the results for q_{total} from Example 1. The dark blue bars represent the results using the logarithmic function e_β, as shown in eq. (3), while the light blue bars represent the results using the linear function e_α, as shown in eq. (2).

TABLE III: The 11-value scale for $\tilde{q}_{S_2}$ of Example 1

$\tilde{q}_{S_2}$	Description
10	not observable outside apartment
9	barely observable in adjacent apartments; cannot be interpreted
8	barely observable in adjacent apartments; need advanced equipment to interpret
7	observable in parts of adjacent apartments, but not beyond
6	well observable in adjacent apartments, but not beyond
5	observable in range $>$ 30m; on street
4	observable in range $>$ 50m on street
3	observable in range $>$ 100m on street
2	observable on street from running car
1	observable through wide-range network
0	n/a

description, and comment on the use of the framework. Note, however, that the numerical values are for illustration purposes. These values are based on rough estimates instead of a careful assessment. Different methods for assessment were proposed above in Section II-C, but applying and evaluating the different methods remain future work.

A. Confidentiality and Observability

In the storyline of the Home Scenario, Petra is monitored at home with the requirement that she wants her data to be confidential for people inside and outside her home. Let us assume that the properties of data observability and data confidentiality are essential in this first case, i.e., are in $\mathcal{S}$.

Here, data observability means that a third party can observe the signal sent from a device and, thus, deduce the existence of this device and some meta-data. For instance, neighbours of Petra may observe the signals from her sensors and make assumptions about her health conditions from this. As countermeasures the apartment could be shielded or the signal strength of the sensors could be reduced. While shielding the apartment is too expensive, reducing the signal strength, however, could have an impact on the data availability since some corners in Petra's apartment would not be covered.

Data confidentiality means that a third party cannot interpret the received signals. Cryptographic methods and authentication are often used to assure data confidentiality. Countermeasures when threats occur could use a different cryptographic method or authentication protocol. However, using a different cryptographic method could have a negative impact on the performance or battery consumption.

For a numeric example, here denoted as Example 1, we use the following variables: q_{S_1} is the value for observability inside the apartment; q_{S_2} is the value for observability outside the apartment; q_{S_3} is the value for confidentiality; q_{S_4} is the value for availability; q_{Q_1} is the value for bandwidth; q_{Q_2} is the value for battery consumption; and q_C are other mitigation costs. Recall that the value of q_i indicates how far a given requirement is from the ideal fulfilment, where 1 is complete fulfilment of the requirement. We use the following cases: *I*) the base case, i.e., the apartment is not shielded, rather simple encryption algorithms and authentication protocols are used, and sensors transmit at normal power; *II*) shielding the apartment; *III*) reducing transmission power; *IV*) using different encryption algorithm; and *V*) using different authentication protocol.

As outlined in in Section II-B, for objective assessment we need to establish a scale using n steps similarly to the Likert scale. For an example, we present a possible scale for the requirement $\tilde{q}_{S_2}$ (observability outside apartment) on a scale with 11 values in TABLE III. The value of $\tilde{q}_{S_2} = 0$ is marked as not applicable to indicate that for observability outside the apartment no situation is considered totally unacceptable. Note that marking $\tilde{q}_{S_2} = 0$ implies $q = 0$ for this alternative, i.e., it would be marked as totally unacceptable.

In an experiment, we assessed the values for $\tilde{q}_{S_{i=1\ldots4}}$, $\tilde{q}_{Q_{i=1\ldots2}}$, and $\tilde{q}_{Q_C}$ by using a rough estimate. We also assigned values for the weights w_i using intuition; we are aware that these values need to be assessed more thoroughly at a later stage. The assessment values, weights, and results for $\hat{q}_i$ and q_{total} are shown in TABLE II for the logarithmic approach from eq. (3). We also applied the linear approach from eq. (2) to the same data. Both results for q_{total} are visualised in Fig. 7.

In our example we see that the logarithmic approach and the linear approach show similar behaviour with respect to ranking

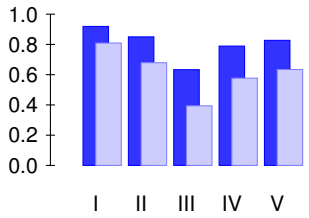


Fig. 8: Visualising the results from Example 2. The dark blue bars represent the results using the logarithmic function e_β, as shown in eq. (3) while the light blue bars represent the results using the linear function e_α, as shown in eq. (2).

TABLE IV: Example 2 for applying the ASSET framework using the logarithmic approach from eq. (3)

q_i	S_1	S_2	S_3	S_4	Q_1	Q_2	C	q_{total}
w_i	1	1	2	1	1	1.5	1	$\sum = 8.5$
Case I	7	6	8	9	8	9	10	0.919
Case II	7	6	4	9	8	9	9	0.850
Case III	7	5	4	1	1	8	9	0.633
Case IV	7	5	3	9	7	7	8	0.789
Case V	7	6	4	9	6	8	8	0.827

the alternatives. However, the logarithmic approach results in higher values and less differences for the values in-between. In this particular example, a combination of cases III and IV, gives the best result while case II delivers the lowest result, which is reasonable.

B. Assessment of Changes in Time

As Example 2 we use the part of the storyline where Petra is taking a stroll in the park. We assume that her sensors are connected wirelessly to her smartphone in its function as a PCH, and the PCH is communicating through a wireless network with the health care infrastructure through a public wireless network offered by a telephony provider. Further, we assume that her smartphone can connect using a WLAN.

In this example, we use different definitions for q_{S_1} and q_{S_1} by using the observability of the sensors and the PCH, respectively. We take into account effects for wide area networks that indicate that battery consumption is higher when the signal strength from the base station is weak or the connection is lost.

For a numeric example we use the following variables: q_{S_1} is the value for observability of the sensors; q_{S_2} is the value for observability of the PCH; q_{S_3} is the value for confidentiality; q_{S_4} is the value for availability; q_{Q_1} is the value for bandwidth; q_{Q_2} is the value for battery consumption; and q_C are other mitigation costs. We use the following cases from the storyline of Scenario A: *I*) walking alone in the park; *II*) meeting Linda; *III*) loosing connection; *IV*) connect to open, mobile WLAN; and *V*) using Linda's PCH as communication channel.

In an experiment, as above, we assessed the values for $\tilde{q}_{S_{i=1\ldots4}}$, $\tilde{q}_{Q_{i=1\ldots2}}$, and $\tilde{q}_C$ by using a rough estimate and assigned values for the weights w_i using intuition. The assessment values $\tilde{q}_i$, weights, and q_{total} are shown in TABLE IV for the logarithmic approach from eq. (3). We also applied the linear approach from eq. (2) to the same data. Both results for q_{total} are visualised in Fig. 8.

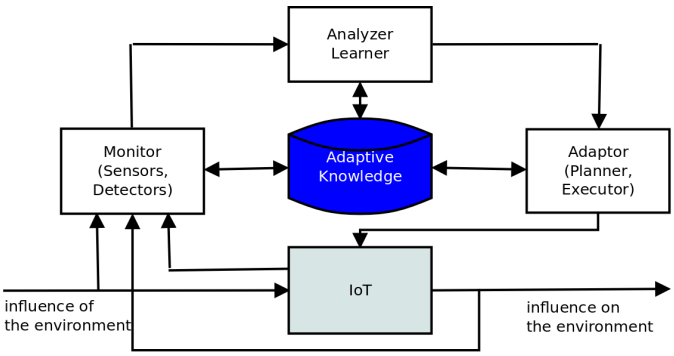


Fig. 9: The Adaptive Security concept, adapted for the IoT by Abie [24].

In this example we see how the security situation changes due to changes of the context (I–II–III), i.e., when Petra meets Linda or Petra looses connection. This example also shows that the assessment can give a hint which one of two possible actions (IV or V) would promise a better security situation.

VI. Applying the Framework to Adaptive Security

Abie and Balasingham [2] define the term *adaptive security* as *"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"*. Abie and Balasingham present the *Adaptive Risk Management* (ARM) framework that is based on a feedback loop known from cybernetics [22] with the five measures (*i*) identify, (*ii*) analyse, (*iii*) plan, (*iv*) track, and (*v*) control. This results in four steps in the adaptation loop, aligned to ISO/IEC 27005:2008 [10] and the *Plan–Do–Check–Act* (PDCA) model of ISO/IEC 27001:2005 [23].

Abie [24] presented a functional description on the concept of adaptive security for a message-oriented infrastructure; he adapted this concept to the IoT, as shown in Fig. 9. He identified the following functionality to be essential for adaptive security to be implemented: *a*) being self-aware using a feedback loop and a history database; *b*) being context-aware using sensors and feedback from other nodes in the IoT; *c*) using security metrics to process the data from the sensors and the other nodes; *d*) using risk and threat estimation and prediction; *e*) using security metrics as defined by Savola et al. [19]; *f*) using methods such as Bayesian networks [25], game theory, Markov chains, etc. to support the threat estimation and prediction; *g*) using a decision making module to enforce appropriate security and privacy level; and *h*) communicating data to other nodes in the IoT.

A. Integrating the Estimation Function to Adaptive Security

In the adaptive security concept, the Monitor receives data from sensors, detectors, and other sources that are further used in the Analyser/Learner to make adaptive decisions. In this context, the ASSET evaluation framework can be used to

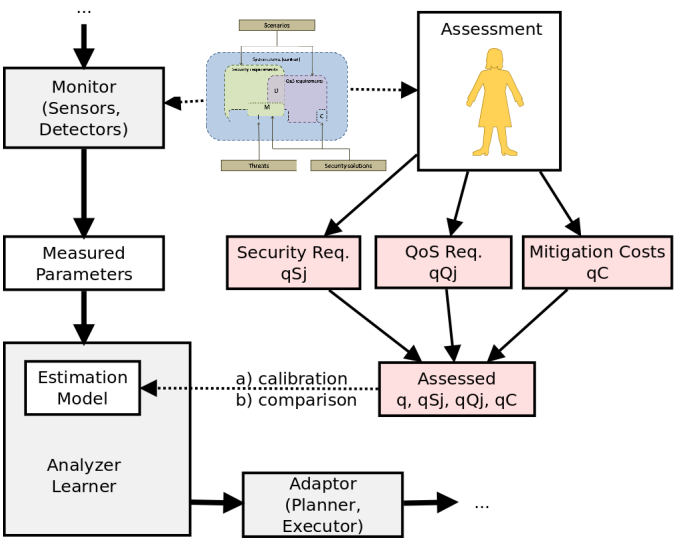


Fig. 10: Integration of the estimation framework into the adaptive security model.

provide the ground truth data *a*) to train the learning algorithms employed in the evaluation loop, and *b*) to evaluate whether the behaviour of the adaptive algorithms is reasonable.

For this we follow the following recipe: We use the storylines similarly as done in Section V where we assess the values q_i for all useful cases that can appear and calculate q with the suitable weights. On the other hand, the Monitor receives k measured values from diverse sensors and detectors. These measurements are denoted as s_k.

We postulate a function $u(s_k)$ that ideally is designed such that $u(s_k) = q$ for q as defined in eq. (1) for all relevant situations from the scenarios. In that way, using the function u, the input from the sensors and detectors will generate the same value as the assessment suggests. Alternatively, we can postulate functions $u_i(s_k)$ where $u_i(s_k) = q_i$ for all relevant situations. It is intended that the function u_i will generate the same value for each partial product as the assessment suggests.

The functions $u(s_k)$ and $u_i(s_k)$ could be instantiated in a learning phase. However, the adaptive security model can also handle this dynamically, so that the definition of these functions can vary over time.

The evaluation of the functions $u(s_k)$, respectively $u_i(s_k)$, will be handled in the Analyser and Learner components using regression, Bayesian networks, game theory, or similar. On the basis of the evaluated values from these functions, the Adaptor takes the necessary decisions. Fig. 10 illustrates how the estimation function can be integrated into the adaptive security model.

Based on the sets of system states the assessment of the values q, q_{S_i}, q_{Q_i}, and q_C is performed using a panel of users and specialists. This is shown on the right side of Fig. 10. These values are used to calibrate the estimation model. When the estimation function is established, these values can also be used to be compared with the estimation function for validation purposes. On the left side of Fig. 10, a part of the adaptation loop is shown with the components Monitor, Analyzer, and Adaptor. The Monitor component retrieves data from sensors and adaptors to a set of measured parameters. Using the estimation model, the Analyzer performs its tasks, and forwards the calculated values to the Adaptor component.

B. Evaluation Methods

For the purpose of evaluating the behaviour of the adaptive security methods we intend to employ the scenarios and storylines presented in Section V above together with implementations in a lab [26], simulation, and formal reasoning [27]. In an evaluation, we will go through each situation of the storylines, and assess or calculate the values q, q_{S_i}, q_{Q_i}, q_C, $u(s_k)$, and $u_i(s_k)$ as necessary.

Using a lab one could build all necessary equipment that contains all necessary functionality. According to the evaluation method, one will go through all states and situations defined by the storyline and assess or calculate all relevant values according to our framework. Thereafter, the adaptation algorithm will be applied, resulting in new states that are evaluated by assessing and calculating the relevant values. Comparing the calculated values $u(s_k)$, and $u_i(s_k)$ after each adaptation step with the desired and assessed values for q, q_{S_i}, q_{Q_i}, and q_C will give evidence on the behaviour of the adaptation algorithm. The goal is to evaluate whether the behaviour of the adaptation loop is close to the "right" decisions deduced from the assessment.

Note that in the absence of a lab, simulations or the use of formal methods can be considered. Here, instead of implementing the devices in real hardware the essential functionality is implemented in a model, and simulation and model checking techniques are used [27], [28].

VII. Discussion and Related Work

Our framework supports the evaluation of security solutions and provides a means to assess data for development and calibration of the estimation model. In this section, we discuss several issues regarding our framework. We also relate our work to frameworks that are described in the literature.

A. Issues and Concerns

The estimation model's design and the function $u(s_k)$ are not the focus here, but our framework can calibrate an estimation model. In principle, methods from machine learning, such as regression analysis, Bayesian networks, fuzzy logic, or game theory can be used to develop the function $u(s_k)$ introduced in Section VI. The assessed data will be used as training data while only the measurable data from sensors will be used in the adaptive security concept.

Using this concept, the estimation model and the function $u(s_k)$ will respond with a sufficiently correct estimate as long as the particular case has been part of the scenarios and storylines used in the assessment. Cases that are not covered in the assessment can still be estimated, but we cannot predict the appropriateness of the estimate. Thus, the framework needs to monitor continuously whether all relevant cases are covered,

and refine the estimation model with new assessments when missing cases are discovered.

In contrast to the adjustment of the estimation model, the evaluation of the function $u(s_k)$ can be performed in near real-time. Depending on the estimation principle, the evaluation can be done using partial evaluation when only a few parameters are updated at a time. Metrics for evaluation of such estimation models can be found in the literature for the chosen estimation principle [29].

One concern of our assessment model is that we use human assessment, which introduces subjectivity into the assessment. While it is viable to check objectively whether a system state fulfils a catalogue of guidelines or requirements, the severity of deviations from the ideal state are subjective. For instance, in healthcare applications, patients or health personnel might need to make choices whether to accept deficiencies in privacy or security to use a service.

There are assessment methods that make use of evaluation panels consisting of both laymen and experts in other application areas. For example, the estimation of video and audio quality [11] can be performed using subjective evaluations with user panels where each panel member evaluates content under well-defined conditions. Another example is the evaluation of the quality of open source software [15] where methods using a user-based rating have been related to more objective methods. It has been shown that the subjective methods give an appropriate estimate of the software quality, despite their simplicity [16]. Hence, we argue that subjective assessment can be applied also for security, privacy, QoS, and costs.

In healthcare applications, the balance between security, privacy, and QoS needs to be addressed. For instance, non-critical information could be made available with lower security to a user or security could be lowered when emergency access to the medical data is necessary. Our assessment framework can address such issues by modelling these as cases into the scenarios and storylines. The evaluation will then show whether the q_{total} is within acceptable borders.

Similarly, our assessment method is also suitable to assess alternative security methods for specific target groups, such as people with disabilities. For instance, Scenario A could be extended by Petra using an alternative authentication method, e.g., the one described by Fuglerud and Dale [30].

B. Security Metrics

Security metrics [31] provide a comprehensive approach to measuring risk, threats, operational activities, and the effectiveness of data protection in software systems. They also provide the means to compare different solutions and obtain evidence about the performance of operational security in adaptive security [32]. Some often-used metrics include the number and frequency of vulnerabilities or actual attacks. These are based on appropriate security and privacy goals.

Savola and Abie [33] present a methodology for developing security metrics using a risk-driven process; this starts from an analysis of threat and vulnerability of the system and aims to achieve a collection of security metrics and related measurement architecture. This concept has been extended to include adaptive security management for healthcare applications [19].

Weiß et al. [34] propose security metrics built on a risk management approach. Jafari et al. [35] develop security metrics to assess security posture of healthcare organisations. Abie and Balasingham [2] integrate security metrics into the validation of risk-based adaptive security for deployment in the IoT under changing threat models. Our work complements these proposals with a scenario-based framework for the assessment and validation of context-aware adaptive security solutions. The security metrics described by Weiß et al. and Jafari et al. are well suited as objective data described in Section II-C3.

C. Security Evaluation Frameworks

Frameworks for evaluating security and privacy in eHealth include a Common Criteria framework for the evaluation of information technology systems security [36], a framework for information security evaluation [37], a requirement-centric framework for information security evaluation [38], a scenario-based framework for the security evaluation of software architecture [39], and the OWASP risk rating methodology [40].

Recently, Shoniregun et al. [41] proposed a unified security evaluation framework for healthcare information systems by exploring the solutions and technologies currently available for evaluating security and privacy problems in such systems. The authors acknowledged the limitations of nearly all major efforts to measure or assess security such as Trusted Computer System Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC), Systems Security Engineering Capability Maturity Model (SSE-CMM), and Common Criteria. The authors also reviewed approaches to evaluation of healthcare information security and privacy, such as standards-based, privacy policy-based, ontology-based, security and privacy metrics-based, and model-based approaches to security and privacy evaluation.

Torjusen et al. [28] present a formal approach to verification of an adaptive security framework for the IoT, with integration of run-time verification enablers in the feedback adaptation loop and the instantiation of the resulting framework with Coloured Petri Nets for formally evaluating and validating self-adaptive security behaviour. Our work complements this concept by providing a scenario-based assessment to convey the design requirements.

D. eHealth Evaluation Frameworks

There are multiple evaluation frameworks for security and privacy in eHealth available, including the analysis of different parts, such as patient monitoring systems or electronic health record (EHR) systems. Note that an EHR can be part of the IoT in the sense that it is the data sink in a heath care organisation.

Fernández-Alemán et al. [42] conducted a comparative literature review of the security and privacy of the current EHR systems based on ISO 27799 [43]. They identified and analysed critical security and privacy aspects of EHR systems, such as the need for harmonisation of compliance standards to

resolve possible inconsistencies and conflicts among them, the use of efficient encryption scheme for the acquisition, development and maintenance of information systems, access control, communication and operational management, and the security of human resources. They have also discovered that although most EHR systems defined security controls these arent fully deployed in actual tools. Note also that their emphasis is not on wireless communication which is often used in the IoT. The research framework by Fernández-Alemán et al. is based on a literature review that is static by nature, while our framework is able to assess values that change dynamically.

Malin et al. [44] described the problems, perspectives and recent advances in biomedical data privacy by illustrating the space of data privacy in the biomedical domain as multidisciplinary; it crosses ethical, legal, and technical boundaries. This demonstrates that appropriate socio-technical solutions can be defined for emerging biomedical systems that can balance privacy and data utility and system usability. At the same time this highlights cloud computing as new computing, high-throughput technology that creates new challenges to privacy that biomedical community will need to handle in the future. Malin et al.'s work addresses more policies in different domains than assessing the security and privacy characteristics.

Kierkegaard [45] highlights the benefits and the key concerns of a centralised supranational health network that allows access to health information anyplace and anytime by enhancing efficiency, effectiveness, accuracy, completeness and accessibility, and generally improving the quality of healthcare services. These benefits lead to an increase of the amount of information collected, processed, filtered, transferred or retained. In in turn, this increases the potential abuse and privacy threats to such information. Thus, privacy and data protection need to be embedded within the infrastructure. Note that a potential single point of failure of such an infrastructure is a major concern. Also Kierkegaard's work addresses more policies in different domains than assessing the security and privacy characteristics.

Boxwala et al. [46] proposed statistical and machine learning methods to help identify suspicious, i.e., potentially inappropriate, access to EHRs using logistic regression training and support vector machine models and concluded that such methods can play an important role in helping privacy officers detect suspicious access to EHRs. While their methods and ours can predict suspicious accesses (threats), our framework goes further by identifying a set of security solutions that mitigate these threats and a set of system states that represent the dynamic context in which the patient monitoring system operates and adapts specialised to the type of scenarios and story lines used.

Peleg et al. [47] presented a framework for situation-based access control for privacy management through modelling using object-process methodology to structure the scenarios and conceive a situation-based access control model. The framework is intended for traditional role-based access control. Their work and ours are similar in expressing scenarios of patients data access as a basis of preserving of patients security and privacy. They differ in that their solution is access control specific while ours is applicable to any security or quality of service requirements. The framework by Peleg et al. is qualitative while we have added quantitative components in our framework.

Note that the above described frameworks by Boxwala et al. and Peleg et al. can produce values that can be used as input values q_i for our framework, as described in Section II-C3.

VIII. Conclusion

We presented an evaluation framework for adaptive security to be applied for the IoT in eHealth applications. We highlighted the role of the scenarios in the evaluation framework. The framework is based on a generic system model, security and QoS requirements for eHealth applications, and a generic assessment framework. Further, the framework uses sets of states that are used to estimate how well the security and QoS requirements are fulfilled.

For evaluation purposes we presented three scenarios, a home scenario, a hospital scenario, and an emergency scenario. These scenarios are annotated with requirements and outlined as storylines which can be used to evaluate adaptive security algorithms. Our evaluation methodology is designed to compare results from lab experiments and simulations with the assessment by human observers.

The scenarios cover multiple core scenarios representing a range of eHealth IoT situations. These address specific requirements related to the context, the data-communication, the devices, and the actions of the involved actors. The core scenarios are specific to the eHealth case, and make it possible to identify relevant cases that need to be evaluated, such as situations where IoT devices need to be removed or disconnected, the use of ample communication channels, or the impact of mobility.

Storylines for a patient with chronic diseases have been described and analysed. In the future, the overall scenarios, as well as the underlying core scenarios and storylines will be used in the ASSET project to evaluate the adaptive security algorithms. We posit that the framework, methodologies, and scenarios presented here can be used as a blueprint for evaluations of adaptive algorithms beyond the analysis of the adaptive algorithms of the ASSET project.

IX. Acknowledgments

The work presented here has been carried out in the project ASSET – Adaptive Security for Smart Internet of Things in eHealth (2012–2015) funded by the Research Council of Norway in the VERDIKT programme. We wish to thank our colleagues involved in this project for helpful discussions that made this study possible. Particularly, we want to thank Ragnar Hauge for discussions while developing this work. We also wish to thank the anonymous reviewers for valuable comments.

References

[1] W. Leister, M. Hamdi, H. Abie, and S. Poslad, "An evaluation scenario for adaptive security in eHealth," in PESARO 2014 – The Fourth International Conference on Performance, Safety and Robustness in Complex Systems and Applications. IARIA, 2014, pp. 6–11.

[2] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth," in BODYNETS 2012 – 7th International Conference on Body Area Networks. ACM, 2012.

[3] I. F. Alexander and N. Maiden, Eds., "Scenarios, Stories, Use Cases: Through the Systems Development Life-Cycle". John Wiley & Sons, 2004.

[4] S. Faily and I. Flechais, "A meta-model for usable secure requirements engineering," in SESS – ICSE Workshop on Software Engineering for Secure Systems. Association for Computing Machinery (ACM), 2010.

[5] H. Mouratidis and P. Giorgini, "Security attack testing (SAT)–testing the security of information systems at design time," Information Systems, vol. 32, no. 1, Jan. 2007, pp. 1166–1183.

[6] ITU-T, "Overview of the Internet of Things," International Telecommunication Union, Recommendation Y.2060 (06/2012), 2013. [Online]. Available: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559 [Accessed: 13. Nov. 2014].

[7] O. Vermesan, P. Friess, P. Guillemin, H. Sundmaeker, M. Eisenhauer, K. Moessner, F. L. Gall, and P. Cousin, "Internet of things strategic research and innovation agenda," in Internet of Things–Global Technological and Societal Trends. River Publishers, 2011, pp. 7–151.

[8] K. Habib and W. Leister, "Adaptive security for the Internet of Things reference model," in Proceeding of Norwegian Information Security Conference, NISK 2013, C. Rong and V. Oleshchuk, Eds., 2013, pp. 13–24.

[9] W. Leister, H. Abie, and S. Poslad, "Defining the ASSET scenarios," Norsk Regnesentral, NR Note DART/17/2012, Dec. 2012.

[10] "ISO/IEC 27005:2008 Information technology–Security techniques–Information security risk management," International Organization for Standardization and International Electrotechnical Commission, standard, 2008.

[11] W. Leister, S. Boudko, and T. H. Røssvoll, "Adaptive video streaming through estimation of subjective video quality," International Journal on Advances in Systems and Measurements, vol. 4, no. 1&2, 2011, pp. 109–121. [Online]. Available: http://www.iariajournals.org/systems_and_measurements/ [Accessed: 1. Nov 2014].

[12] R. Likert, "A technique for the measurement of attitudes." Archives of Psychology, vol. 22, no. 140, 1932, pp. 1–55.

[13] A. Nevill and A. Lane, "Why self-report likert scale data should not be log-transformed," Journal of Sports Sciences, vol. 25, no. 1, 2007, pp. 1–2.

[14] J. Perl and S. Russell, "Bayesian networks," in Handbook of Brain Theory and Neural Networks, M. Arbib, Ed. Cambridge, MA: MIT Press, 2003, pp. 157–160.

[15] A. Wasserman, M. Pal, and C. Chan, "The business readiness rating model: an evaluation framework for open source," in Proc. EFOSS Workshop, Como, Italy, Jun. 2006.

[16] A.-K. Groven, K. Haaland, R. Glott, and A. Tannenberg, "Security measurements within the framework of quality assessment models for free/libre open source software," in Proc. Fourth European Conference on Software Architecture: Companion Volume, ser. ECSA '10. New York, NY, USA: ACM, 2010, pp. 229–235.

[17] W. Leister, T. Fretland, and I. Balasingham, "Security and authentication architecture using MPEG-21 for wireless patient monitoring systems," International Journal on Advances in Security, vol. 2, no. 1, 2009, pp. 16–29. [Online]. Available: http://www.iariajournals.org/security/ [Accessed: 1. Nov 2014].

[18] W. Leister, T. Schulz, A. Lie, K. H. Grythe, and I. Balasingham, "Quality of service, adaptation, and security provisioning in wireless patient monitoring systems," in Biomedical Engineering Trends in electronics, communications and software. INTECH, 2011, pp. 711–736.

[19] R. M. Savola, H. Abie, and M. Sihvonen, "Towards metrics-driven adaptive security management in e-health IoT applications," in BODYNETS 2012 – 7th International Conference on Body Area Networks. ACM, 2012.

[20] J. Hernandez, M. E. Hoque, and R. W. Picard, "Mood meter: large-scale and long-term smile monitoring system," in ACM SIGGRAPH 2012 Emerging Technologies, ser. SIGGRAPH '12. New York, NY, USA: ACM, 2012, pp. 15:1–15:1.

[21] R. M. Savola and H. Abie, "Metrics-driven security objective decomposition for an e-health application with adaptive security management," in ASPI 2013 – International Workshop on Adaptive Security & Privacy management for the Internet of Things. ACM, 2013.

[22] W. R. Ashby, "An Introduction to Cybernetics". London: Chapman & Hall, 1957.

[23] ISO, "ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements," International Organization for Standardization and International Electrotechnical Commission, standard, 2005.

[24] H. Abie, "Adaptive security and trust management for autonomic message-oriented middleware," in IEEE Symposium on Trust, Security and Privacy for Pervasive Applications (TSP 2009). Macau, China: IEEE, 2009, pp. 810–817.

[25] J. Pearl, "Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. Representation and Reasoning Series". Morgan Kaufmann, 1988.

[26] Y. B. Woldegeorgis, H. Abie, and M. Hamdi, "A testbed for adaptive security for IoT in eHealth," in ASPI 2013 – International Workshop on Adaptive Security & Privacy management for the Internet of Things. ACM, 2013.

[27] W. Leister, J. Bjørk, R. Schlatte, E. B. Johnsen, and A. Griesmayer, "Exploiting model variability in ABS to verify distributed algorithms," International Journal On Advances in Telecommunications, vol. 5, no. 1&2, 2012, pp. 55–68. [Online]. Available: http://www.iariajournals.org/telecommunications/ [Accessed: 1. Nov 2014].

[28] A. B. Torjusen, H. Abie, E. Paintsil, D. Trcek, and A. Skomedal, "Towards run-time verification of adaptive security for IoT in eHealth," in Proc. 2014 European Conf. on Software Architecture Workshops, ser. ECSAW '14. New York, NY, USA: ACM, 2014, pp. 4:1–4:8.

[29] B. G. Marcot, "Metrics for evaluating performance and uncertainty of Bayesian network models," Ecological Modelling, vol. 230, 2012, pp. 50–62.

[30] K. S. Fuglerud and Ø. Dale, "Secure and inclusive authentication with a talking mobile one-time-password client," IEEE Security and Privacy, vol. 9, no. 2, 2011, pp. 27–34.

[31] S. C. Payne, "A guide to security metrics," SANS Institute Information Security Reading Room, whitepaper, June 2006.

[32] A. Evesti, H. Abie, and R. M. Savola, "Security measuring for self-adaptive security," in Proc. 2014 European Conf. on Software Architecture Workshops, ser. ECSAW '14. New York, NY, USA: ACM, 2014, pp. 5:1–5:7.

[33] R. M. Savola and H. Abie, "Development of measurable security for a distributed messaging system," Intl. Journal on Advances in Security, vol. 2, no. 4, 2009, pp. 358–380. [Online]. Available: http://www.iariajournals.org/security/ [Accessed: 1. Nov 2014].

[34] S. Weiß, O. Weissmann, and F. Dressler, "A comprehensive and comparative metric for information security," in Proc. IFIP Intl. Conf. on Telecommunication Systems, Modeling, and Analysis 2005 (ICTSM2005), Dallas, TX, USA, 2005, pp. 1–10.

[35] S. Jafari, F. Mtenzi, R. Fitzpatrick, and B. O'Shea, "Security metrics for e-Healthcare information systems: A domain specific metrics approach," Intl. Journal of Digital Society (IJDS), vol. 1, no. 4, 2010, pp. 238–245.

[36] R. Kruger and J. H. P. Eloff, "A common criteria framework for the evaluation of information technology systems security," in Information Security in Research and Business, Proceedings of the IFIP TC11 13th International Conference on Information Security (SEC '97), 14-16 May 1997, Copenhagen, Denmark, ser. IFIP Conference Proceedings, L. Yngström and J. Carlsen, Eds., vol. 92. Chapman & Hall, 1997, pp. 197–209.

[37] R. von Solms, H. van de Haar, S. H. von Solms, and W. J. Caelli, "A framework for information security evaluation." Information & Management, vol. 26, no. 3, 1994, pp. 143–153.

[38] R. Savola, "A requirement centric framework for information security evaluation," in Advances in Information and Computer Security, First International Workshop on Security, IWSEC 2006, Kyoto, Japan, October 23-24, 2006, Proceedings, ser. Lecture Notes in Computer Science, H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, and S. Kawamura, Eds., vol. 4266. Springer, 2006, pp. 48–59.

[39] A. Alkussayer and W. Allen, "A scenario-based framework for the security evaluation of software architecture," in 3rd IEEE Intl. Conf. on Computer Science and Information Technology (ICCSIT), vol. 5, July 2010, pp. 687–695.

[40] "The OWASP risk rating methodology." [Online]. Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology [Accessed: 17 November 2014].

[41] C. Shoniregun, K. Dube, and F. Mtenzi, "Towards a unified security evaluation framework for e-healthcare information systems," in Electronic Healthcare Information Security, ser. Advances in Information Security. Springer US, 2010, vol. 53, pp. 151–172.

[42] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," Journal of Biomedical Informatics, vol. 46, no. 3, 2013, pp. 541–562.

[43] "ISO/IEC 27799:2008. Health Informatics–Information security management in health using ISO/IEC 27002". Geneva, Switzerland: International Organization for Standardization, 2008.

[44] B. A. Malin, K. E. Emam, and C. M. O'Keefe, "Biomedical data privacy: problems, perspectives, and recent advances," JAMIA, vol. 20, no. 1, 2013, pp. 2–6.

[45] P. Kierkegaard, "Electronic health record: Wiring europes healthcare," Computer Law & Security Review, vol. 27, no. 5, 2011, pp. 503 – 515.

[46] A. A. Boxwala, J. Kim, J. M. Grillo, and L. Ohno-Machado, "Using statistical and machine learning to help institutions detect suspicious access to electronic health records," JAMIA, vol. 18, no. 4, 2011, pp. 498–505.

[47] M. Peleg, D. Beimel, D. Dori, and Y. Denekamp, "Situation-based access control: Privacy management via modeling of patient data access scenarios," Journal of Biomedical Informatics, vol. 41, no. 6, 2008, pp. 1028–1040.

[48] M. Peleg, S. Keren, and Y. Denekamp, "Mapping computerized clinical guidelines to electronic medical records: Knowledge-data ontological mapper (KDOM)," Journal of Biomedical Informatics, vol. 41, no. 1, 2008, pp. 180–201.