An Empirical Research on InfoSec Risk Management in IoT-based eHealth

Waqas Aman, Einar Snekkenes
Norwegian Information Security Lab (NISLab)
Gjøvik University College
Gjøvik, Norway
{waqas.aman, einar.snekkenes}@hig.no

***Abstract*—Enabling the healthcare infrastructure with Internet of Things (IoT) will significantly improve quality of service, reduce the costs and efficiently manage remote and mobile patients. To be efficacious, IoT and eHealth infrastructure essentials as well as their associated security and privacy issues should be thoroughly recognized to effectively manage the InfoSec risks involved. Unfortunately, there has been a potential lack of research comprehensively addressing these issues jointly while InfoSec risk management solutions are devised for IoT-based eHealth. In this paper, we have highlighted the necessary knowledge while approaching InfoSec risk management in IoT-eHealth as per a standard process, assessed it against standard and proposed requirements and identified the current trends and gaps to set directions for future research.**

***Keywords*—Internet of Things (IoT); Remote Patient Monitoring; Risk Management; Security & Privacy; eHealth.**

I. INTRODUCTION

Internet of Things (IoT) is a global internet architecture connecting various wired and wireless technologies designed to meet specific objectives [1]. Beside its anticipated benefits in various private and business domains, enabling IoT in welfare spheres, such as healthcare, will greatly facilitate the society as a whole. A patient can now be monitored remotely in a continuous fashion thus making the health services more mobile, extendable and effective. Though offering a great deal of benefits, IoT is still facing a number of critical challenges such as networking, security and privacy, QoS, standardization, etc., which needs to be sorted out and yet remain open [2]. Among these challenges, the most threatening are the security and privacy concerns. Connecting diverse technologies may lead to new threats with much grander risk of security. These threats become more drastic when considered in the context of a continuous service, such as healthcare, where the concern is not limited to a patient's privacy but, there is a threat to the breach of trust, leading to the exploitation of a welfare service.

Standards, guidelines and good practices concerning InfoSec Risk Management (ISRM), such as ISO 27005, NIST, CRAMM, ISACA RiskIT, etc., recommend to approach ISRM in a methodological fashion, i.e., understand the target business function, service or system, identify the security and privacy (S&P) concerns and threats, analyze the risk faced, and manage the risk to reduce it to an acceptable level. To qualify this process, IoT-driven eHealth as a continuous real-time service will need an intelligent security system that can dynamically predict and estimate the risk faced and mitigating it autonomously to be more resilient and adaptable in the face of changing security threats [3]. A number of architectural designs, security issues, risk management (RM) models and surveys are presented concerning eHealth [1], [2], [4]–[7]. However, such studies are either focused on the mentioned individual topics, target a specific technology or presents abstract modeling. Hence, there is a lack of literature that provides a holistic study of the related topics as per the standard RM process to approach ISRM in IoT-based eHealth.

In this paper, we will highlight IoT-eHealth infrastructure essentials, the associated S&P issues and will explore various ISRM approaches to establish an understanding of how ISRM can be modeled in IoT driven eHealth. Existing literature is evaluated against standard and projected requirements and current trends and gaps are identified. We identified that the current system and S&P modeling are focused only on the primitive requirements and is done in an empirical manner. Whereas vital operations, key system components and necessary S&P services are overlooked. Suitability of various ISRM models and methods is explored and it was concluded that most of them have a subjective influence which makes them difficult to be adopted in a dynamic-real-time environments and lacks intelligent risk analysis and management capabilities, such as context awareness and self-adaptation, which are deemed to be essential for IoT driven eHealth [3]. We strongly believe that this contribution will provide a reference point for future researchers and will enable them to understand the requirements, challenges, options, methods and techniques necessary to consider while approaching ISRM in IoT driven eHealth.

The rest of the paper is organized as follow: In Section II, an overview of the related work will be highlighted. Section III will elaborate the current literature highlighting architectural designs, S&P services, issues and threats and modeling security risks in the perspective of IoT-based eHealth. In Section IV, evaluation of the current literature will be highlighted by aligning them with a set of standard and proposed requirements. In Section V, current trends and gaps will be identified by discussing the evaluated knowledge. Finally, concluding remarks and future research endeavors will be underlined in Section VI.

II. RELATED WORK

A summary of related efforts concerning IoT, remote eHealth, associated security challenges and ISRM modeling are highlighted in this section. The goal is to identify and

 ISBN: 978-1-61208-313-1

converse the reviews which are aligned with the theme of ISRM and related topics in IoT-based eHealth.

A detailed description of networking and architectural characteristics of ubiquitous computing used for remote patient monitoring (RPM) is presented in [8]. Sunil et al. discuss the use of mobile networks and the utilization of their mobility features in RPM. 3G and 4G networks characteristics were compared and it was showed that 4G can provide magnified advantages in terms of QoS. QoS requirements concerning wireless networks were highlighted and respective suggestions were discussed to overcome some of the current shortcomings.

Wireless Sensor Networks (WSNs) play a vital role in remote eHealth setup. They enable the notion of a continuous monitoring in remote patient monitoring systems (RPMS). Murad et al. [9] stressed that preventive security measures are not sufficient for WSNs due to the presence of an internal attacker. They provided a comprehensive survey of different intrusion detection systems (IDS) categorizing rule, data mining, statistical and game theoretic based techniques as detective measures to comprehend internal and network attacks dynamically thus enabling a second layer of defense to preventive measures. Similar work is also done in [10] [11].

Latré et al. [12] discussed the importance of Wireless Body Area Network (WBAN) and its applications in remote monitoring of various diseases. Positioning of the WBAN in a RPMS setup is detailed and it is argued that most of the current research is focused on the extra-WBAN communication. Available MAC and Network layer protocols were highlighted and it was suggested that new MAC layer protocols need to be design to accommodate patient mobility. Latré et al. reasoned the current issues like QoS, usability and security are more studied in the WSN and should also be examined in WBAN being a more healthcare focused technology as compared to WSN. The survey however was more emphasized on the networking protocols.

A systematic literature review on S&P issues in an Electronic Health Record (EHR) system is presented in [13]. Literature appraisal was based on the requirements defined in ISO 27799 standard related to achieving security goals through cryptographic techniques, HR security measures, such as training and awareness, and its alignment with compliance and regulatory requirements. Luis et al. concluded that though most of the studies do explicate security controls but are not really implemented in health sectors.

A detail survey on IoT is given in [2]. Atzori et al. explain IoT from three different perspectives: *Things, Internet and Semantics* and converse its overlapping and diverse nature. Different technologies, such as Middleware, WSN, RFID, etc., are recognized to review their possibilities in enabling effective IoT. Extended opportunities of IoT in different application areas are explored and their benefits are traversed. Furthermore, a list of open issues, such as, security, privacy, networking, standardization, QoS and data integrity was highlighted and suggested to be researched to make IoT a more mature and promising technology.

To perform effective risk analysis, it is a difficult task to select the appropriate Risk Analysis (RA) methodology [14]. Vorster and Labuschagne presented a framework of evaluating RM methodologies to assist the business managers in selecting an appropriate method to conduct RA within an organization. A five-point common criterion was used for the comparison. A similar approach is also taken by [15] where RA methodologies were classified based on the involvement of risk analysts or stakeholders and the execution nature of the steps used in the RA process. RA methodologies can also be classified into two groups based on the approach adopted–*Traditional*: where a methodology have a subjective influence of the stakeholder involved and risk is analyzed by the appraisers; *Contemporary*: where risk is estimated based on the target system behavior by inspecting the events it creates, testing it and validating it with formal methods [16].

III. Approaches, Concepts & Issues

This section presents an overview of the current literature in accordance with the standard ISRM process. The selected literature encompasses systems overview, S&P services and threats and ISRM modeling approaches which are necessary to be understood while impending ISRM in IoT driven eHealth. A depiction of the literature organization in line with the standard ISRM guideline is shown in Table I.

TABLE I. Literature Organization & Standard ISRM Process

Standard ISRM Process	Literature Organization
Scope Identification	**IoT-eHealth Infrastructure** – System Overview & Functions – Key Assets – Comm. Medium
S&P Services/Threats	**S&P Modeling** – Threats & Security Services Modeling
Analyzing & Managing Risks	**Modeling InfoSec Risks** – Methods, Models & Frameworks for handling IoT-eHealth Risks

A. IoT-eHealth Infrastructure

IoT-based eHealth can be referred to as the global internet of wired and wireless technologies placed to monitor remote and mobile patients. Besides monitoring, patients can also be supervised over the internet and response to emergency situations can be made in a timely manner with the required aid. The infrastructure includes wearable sensors which collect various physiological sensed data from the patient as biosignals, forwards it to a smart device, such as a smartphone or tablet. Biosignals are filtered and are sent to a remote hospital site via mobile network or internet where the medical staff further investigate them and prescribe the patient accordingly. This concept is also portrayed in [17] in which Otto et al.explained a heart patient scenario while presenting their RMPS. A similar model is also described in [18] in which the proposed system, Tele Health Care, is used to monitor blood pressure and heart rate of a remote patient. In abnormal situations the patient is alerted with an alarm and a SMS is sent to the corresponding doctor for instant response. Ambulatory and emergency situations are also discussed. However, Rajan et al. did not discuss the notion of false alerts which may cause panic on both the patient and doctor sides.

Suh et al. proposed a RPMS, *WANDA*, for monitoring congestive heart failure patients [19]. The system is composed of three tiers: sensors, web and back end databases. Mobility is provided through the use of a smartphone carried by a patient. Via Bluetooth the biosignals are transmitted to a smartphone

 ISBN: 978-1-61208-313-1

from the sensors and are sent to the second tier through GSM, 3G and/or Internet for further investigations. Health status can be accessed either by using the smartphone or the web services. The database tier is used only for backup and recovery procedures assisted with offline backup schedulers.

Based on the fact that a TV is still the most convenient way of interaction among the older adults, Santos et al. presented a TV based solution, *CareBox*, for RPM [20]. CareBox processes the vital signs only locally. Sensor data is sent to the monitoring unit attached to a TV where the patient can have a look at to his health status displayed on TV. The communication layer of the system is designed to support various protocols and technologies. A VoIP client is used where a patient can connect to a doctor for a video meeting. A survey form is programmed into the TV, which asks health related questions from the patient and can be sent upon submission to the doctor site via an internet connection.

Scacht et al. proposed *Fontane* [21]. In Fontane, medical data sensed by various sensors are transmitted to a home broker via Bluetooth. The home broker, implemented in a smartphone, sends the processed data to a tele-medicine center (TMC) using GSM or UMTS. The live medical data received in the TMC is recorded as the patient's EHR. A J2EE–based SaPiMa module is used at the TMC to ensure EHR interoperability. Medical professionals can access the EHRs via the internet to review health status. Based on specific prioritization rules set by a doctor, the system can review orders for the patients.

Sneha et al. [22] provided a comprehensive set of requirements for RPMS and suggested a three-step framework for RMPS: Sensing the vital signs, Analyzing them and if an anomaly is found, the analysis report is transmitted to the concerned site. A PDA equipped with different agents responsible for various tasks such as location update, collection and processing of vital signs, alarm generation, updating EHR and storage of personal data are utilized. These agents use ontology based on Descriptive Logic (DL) and implements various alerts and alarms as per the patient history. Sneha et al. however, did not discuss the patient-doctor communication within their model.

Wu et al. [23] presented an RIFD based Mobile Patient Monitoring System (MPMS) which they claimed to be the first of RFID driven RPMS. The sensor part of the network is composed of wearable ring-type pulse monitoring tags. The sensed data from the tags are sent to a reader where it is delivered to a smartphone via Bluetooth. The smartphone has the ability to process and analyze the data and anomalies are shared with a remote medical station. The smartphone is also equipped with a GPS, which sends out the patient location to the medical station in case of out-door emergencies. RFID is also used in [24] for an out-patient registration. Though, the title reflects a MPMS but is in-fact a model to facilitate the patient's check-in procedure in the hospital. A patient is registered into the system and an RFID bracelet is given to him. The doctor's PDA connects to the RFID server and retrieves the patient information. After the personal information is read, the corresponding patient history is extracted from the health system and advising is done accordingly.

Van et al. proposed *MobiHealth* system experimented in a number of countries [25]. In MobiHealth, the health information was transferred through the next generation wireless networks. Van et al. argued that beside wearable sensors, devices such as actuators and other wearable devices can also be integrated into the system. MobiHealth, however, was prone to major issues of data loss and low bandwidth drawn from the experiments conducted.

Kargl et al. presented a pervasive eHealth monitoring system, *ReMoteCare* [26]. ReMoteCare consists of a local processing and data collection units, which process and collect local data through sensor motes. The data is then forwarded to a remote or local analysis unit over a communication network through a gateway. A PC is used for local analysis from where analyzed data can be sent to a remote processing and collection unit via SNMP for further investigation.

B. Security & Privacy Modeling

eHealth involves critical information exchange and requires a number of security services to make this information reliable, confidential, available and trustworthy. The objective of this section is to understand the threat landscape, S&P issues and how various security services are modeled in remote/mobile patient monitoring.

RPMSs will no doubt greatly improve the quality of healthcare. However, it still have to face a number of challenges concerning S&P. Meingast et al. [5] discussed the issues concerning data access and storage such as authorization, data retention and the type of data to be stored to meet privacy objectives. Regulatory requirements and conflicts among regulations are also highlighted. They stressed that existing controls such as Role Based Access Control (RBAC), Encryption and Authentication mechanisms should be implemented to overcome these issues.

Extending the notion of threats posed in a MPMS, Leister et al. produced a threat assessment report stating the critical threats faced in an MPM environment using various scenarios [27]. Though, the main focus of the assessment is on the WSNs, they have also considered the long range wireless communication infrastructure and the corresponding threats. They also suggested a few countermeasures and security recommendations which can be considered to circumvent these threats.

A comprehensive analysis of threat faced by the WSNs is presented in [4]. The attacks and threats listed by Kalita and Kar are not specific to eHealth but as WSN plays a vital role in RPMS, these threats should be seriously considered when a secure design or risk analysis of RPMS are intended. The attacks identified are categorized in accordance with the TCP/IP network model so that appropriate measure can be taken at the specified layer. Countermeasures are suggested to avoid some of the common attacks.

Lin et al. presented a privacy protection scheme depicting how patient's privacy can be preserved in an MPMS setup [28]. Lin et al. demonstrated how the privacy of the patient medical information is protected from a global adversary trying to eavesdrop on the messages transferred between the patient and the doctor. Furthermore, they explained the preservation of patient's contextual privacy using the proposed scheme showing that an adversary cannot link a patient to a specific

 ISBN: 978-1-61208-313-1

doctor by linking their sources and destinations. They also performed a thorough performance analysis of the proposed scheme demonstrating its efficiency in terms of transmission delays. Ramli et al. [29] provided an insight on four serious privacy issues in pervasive health monitoring systems; eavesdropping, prescription leakages, social implication and abuse of medical information. They argued that these concerns not only affect the health system but also greatly influence patient's life.

Frank et al. described different types of attacks that can be experienced by various network components in RPM as well as the threats corresponding to the information shared between them [26]. They suggested a number of security measures that can be used to prevent internal and external attackers from compromising the confidentiality, integrity and availability of the network components and information. However, privacy and legal issues are just mentioned and are not well elaborated.

Apaporn et al. [30] presented a security framework for eHealth services using two mechanisms: Data and Channel security. Channel security is provided using the SSL on the HTTP layer and data security is provided on the SOAP layer constructed above the HTTP. Apaporn et al. emphasized that RBAC should be used along with multi-factor authentication to ensure proper authorization and authentication. Based on the roles of stakeholders and data sensitivity, communication is divided into different layers where various authentication and encryption settings can be adapted. The framework however dealt only with the web based eHealth services. Multi-factor authentication is also utilized in [31] where Sriram et al. used ECG and accelerometer features from the sensor to perform an activity based biometric authentication.

Elkhodar et al. proposed a Ubiquitous Health Trust Protocol (UHTP) in combination with TLS to authenticate a mobile doctor visiting patients at home [32]. Authentication is performed using three factors based on personal, device and environmental (location) information. During a request to a patient EHR, the doctor uses his smart phone to access the EHR system using his username and password. Beside these personal credentials, the SIM details, IMEI and GPS locations from doctor's phone are validated and access is granted accordingly. The rest of the communication security is ensured as per the TLS negotiated parameters. UHTP, however, doesn't have any application in a continuous RPM orientation.

Simple and secure RPMS is demonstrated in [33]. A mobile set is used as a pulse oximeter where pulse rates are transmitted to a smartphone. The smartphone is equipped with a symmetric cipher and a hashing algorithm to achieve confidentiality and integrity. Shortcomings of this model are ignoring the distribution concerns of the keys and the abstract knowledge of the model, which needs to be detailed.

Timestamps can provide valuable and fresh data for authentication and requires no active involvement of the user [34]. Elmufti et al. used packet timestamps to authenticate a patient/doctor (users) in RPMS. Users are assigned tokens based on timestamps signed by an authenticating server. These stamps are transmitted with individual messages and are compared with a sliding window maintained at the receiving end. User authentication itself is done with digital signature. Elmufti et al. although included sensors in their architecture but did not explore the proposed protocol applications in them.

QoS and event reporting are important requirements in information system. In eHealth, real-time delivery is a must and health status has to be monitored continuously [35]. Rikitake et al. presented an NGN/IMS based ubiquitous health monitoring system in which they addressed the issues of event notification, real-time transfer and data accumulation. Sensor's data is sent to an IMS Client from where it is sent to the observer's site using Realtime Transfer Protocol (RTP). For event notification a SIP base Subscribe/Notify module is utilized that records incidents in an event server connected to the hospital application server. An XML database management system (XDMS) is used that extracts the events from the event server and stores it in an XML format.

Malhotra et al. used Elliptic Curve Cryptography (ECC) to secure the exchange of medical data using mobile devices [36]. Basic ECC methods are used where encryption is done at the user level with a public-private key pair. User is authenticated through a username/password terminal and access to the data is granted based on the user (patient/doctor) role. ECC based digital signature to ensure non-repudiation while message integrity is provided through a cryptographic hash.

C. Modeling the InfoSec Risk

To detect and prevent accidental events regarding a patient's health, an activity based risk analysis framework is proposed in [6]. Collected vital signs events are matched with the patient's history already stored as EHR and the current situation of the patient is predicted. Based on the prediction, risk is calculated and an alert is generated to cope up with the situation. The proposed architecture, although only address the patient health, can be extended to the information security domain as a reference when modeling InfoSec risk analysis is desired.

There are several studies on general S&P issues in eHealth comprising ubiquitous systems. However, it is quite hard to understand and systematically listing down these key issues and design a risk mitigation strategy for them. Oladimeji et al. [37] proposed a framework to model security and privacy objectives, identifying threats and risks and approaching their mitigation strategies. They also discussed how information sensitivity can be characterized as well as how different administrative policies can be refined to protect the patient's privacy.

The attributes that are used to design IT solutions specifically in eHealth are usually complex and interdependent thus needed to be analyzed and prioritize to produce a reliable and trustworthy solution. In [38], it is discussed how these critical attributes and their inter-dependencies can be assessed to reduce the risk after the solution has been deployed. The study can be used for formulating the requirements of designing an automated or real-time risk analysis model as it discuss both the quality and security issues at the requirement engineering level.

Bønes et al. proposed *ModIMob*, a model which can be used to discover the availability of the health experts where their presence is required for an expert opinion [39]. The Australian and New Zealand standard for RM (AS/NZS

 ISBN: 978-1-61208-313-1

4360:1999) is used to discover the risks associated with the use of IM and mobile services used in a healthcare. Though, the scope of their risk evaluation is limited to a specific domain of instant messaging but it can provide an understanding of conducting a RA process in a RPMS.

Abie and Ilangko proposed a risk based adaptive framework for IoT-based eHealth [3]. They argued that based on the real time data collected from the sensors and recent information history, a risk will be calculated, which will further be used in the decision making process of system adaptation. They also provide a detailed literature on various issue concerning system adaptation and risk management and it is deemed that using context awareness and Game Theory techniques, the faced risk can be effectively estimated and predicted.

To provide an appropriate level of privacy all the assets as well as the stakeholders involved in the target system must be considered [7]. A Privacy Risk Model is demonstrated specifically targeting the Ubicomp systems where risks concerning privacy are identified and analyzed by a series of questions. RM is performed by categorizing the risks analyzed and designing architectural strategies for them.

Maglogiannis et al. presented a detail risk analysis of RPMS. RA is performed through the CCTA Risk Analysis and Management Methodology (CRAMM) by considering a case study highlighting the associated key risks [40]. The results of the RA are used in developing a graph using Bayesian Network technique showing the interaction of various critical events that can cause system failure.

Beside the risk posture of the sensitive information processed by the health information systems, the devices used in healthcare have their own inherited risks. With the introduction of pervasive computing and IoTs this risk has grown rapidly. Zhao and Bai described how Failure Mode and Effect Analysis (FMEA) can help in analyzing and managing the risks associated with these devices to circumvent any potential hazards [41]. They showed that Risk Priority Number (RPN) can be used in the context of FEMA to reduce such potential casualties associated with medical devices.

ENISA, using EBIOS tool, performed a detailed RM process of a diabetes case study basing a RPMS [42]. EBIOS is a tool that incorporates the 5-steps RM process developed by the Central Information Systems Security Division of France. The report described a detailed step-by-step procedure of assessing and managing risks indicating the intended audience how to approach the overall process of risk management in MPMSs.

IoT comprises of a complex architecture composed of a variety of technologies due to which the overall threat faced becomes more drastic. There is a need for a sophisticated risk analysis method to assess the risk faced. Lui et al. proposed a mathematical dynamic risk assessment model, DRAMIA, to cope with the threat situation confronted in the IoT space [43]. Enthused by the Artificial Immune System (AIS) their proposed method consist of two components: a Detection Agent that sense and detect the attack environment and evolve accordingly; and a Dynamic Risk Assessment subsystem that computes the risk associated with the attack detected.

IV. EVALUATION

In this section, an evaluation of discussed literature is depicted. Evaluation is performed by mapping the reviewed articles onto a set of standard and proposed requirements.

A. System Models Evaluation

System models discussed in section III-A are evaluated against a set of functional requirements proposed in [44]. We believe that these are complete set of requirements which should be included in any RPMS and MPMS. However, we have added an important requirement of *mobility* as it is the only component that makes the health service mobile and assist in out-doors ambulatory and activity monitoring needs [22]. Functional requirements are described below whereas system models evaluation against the requirements is shown in Table II. ($\surd$) mark indicates the presence of a specific function whereas an (–) implies that either the function is absent or not explicitly discussed.

- **Collection and Processing**: Collection and processing of vital signs from the body sensors by a Patient Cluster Head (PCH) or a wireless base station (BS)
- **Real Time Delivery**: PCH or BS should be able to deliver the processed data in real time for analysis to specified destination such a remote hospital site or a smart device.
- **Alarm generation**: The investigating node, a server at hospital or the smart device, should be able to generate alarms based on the real time data received both locally and remotely at hospital.
- **Interpretation**: Local and remote investigating nodes should be able to diagnose and interpret processed vital sign.
- **Correlation**: Local and remote investigating nodes should be cable of correlating various vital sign such as heart rate, diabetes level and blood pressure to diagnose the correct health status
- **Data Request**: Patient health history should be made available whenever requested
- **Communication Interface**: A communication interface should be incorporated locally to enable expert supervision for a remote patient.
- **Actuation**: To assist elder patients or on demand basis sensors or actuators should be able to saturate the essential medicine or trigger the required action.
- **Mobility**: The system should be able to support mobility services to the patient. This includes tracking the location and service availability while the patient is moving.

B. Evaluating S&P Modeling

S&P service modeling literature reviewed in section III-B is evaluated against the networking and communication requirements standardized by the U.S Health Insurance Portability and Accountability Act (HIPAA) of 1996 specified in [45].

 ISBN: 978-1-61208-313-1

TABLE II. IOT-BASED EHEALTH SYSTEMS EVALUATION

Function/ Reference	[19]	[26]	[20]	[17]	. [25]	[18]	[21]	[22]	[24]	[23]
Collection & Processing	√	√	√	√	√	√	√	√	√	√
Realtime Delivery	√	√	√	√	√	√	√	√	√	√
Alarm Gen.	–	√	–	–	–	√	–	√	√	√
Interpretation	√	√	√	√	√	√	√	√	√	√
Correlation	–	–	–	√	–	–	–	√	–	√
Data Request	√	–	–	–	√	√	–	–	√	–
Comm. Interface	–	–	√	–	–	–	–	–	–	–
Actuation	–	–	–	–	√	–	–	–	–	–
Mobility	–	√	–	–	√	–	–	√	–	√

Besides, ensuring health insurance coverage and simplification of administrative policies, HIPAA aims to standardize S&P mechanisms for electronic health information exchange. Requirements stated by HIPAA are: Data Access, Confidentiality, Integrity, Availability, Alarm Generation, Identity Management, Privacy Preservation, Authentication, and Event Reporting. Table III depicts the requirement(s) covered by each study as per HIPAA security requirements and how they are approached in individual study.

C. InfoSec RM Models Suitability

IoT-based eHealth is a continuous service in which response to an adverse situation should be made in a dynamic fashion. Hence, it requires an ISRM solution that can estimate and predict the security risk faced in real time and adapts appropriate security setting accordingly [3]. To capture the requirements of a real time RM in IoT-eHealth below we devise a fitness criteria, which we believe should be met by a given ISRM model in order to fulfill the operational needs of IoT-eHealth and efficiently manage the risk faced.

- **Operational Nature:** The time at which an ISRM process is executed. This can be *on-demand* basis where the process is activated when required. For instance, ISACA Risk IT method can be executed bi-annually or quarterly by an enterprise. ISRM can be performed in a *dynamic* manner where security risks are analyzed in a real-time fashion such as in military setups. For IoT driven eHealth the operational level should be dynamic in order to be in line with the continuous monitoring theme.
- **Context Awareness:** It corresponds to the understanding of an adverse situation in a given time. In most cases, risks are analyzed individually however; in real computing environment, risk can be seen as a combination of different adverse events. These events and risks need to be correlated to understand a given situation otherwise low impact risks might be tagged as critical leading to false positives and unwanted situations.
- **Analysis Complexity:** It should be taken care of that risk analysis method is lightweight and fast in response to facilitate the theme of real time service [3]. RA solutions having low computational complexity can also be integrated in devices with limited resources.
- **Self-Adaptation:** For IoT-eHealth to be dynamic and self-adaptive, an ISRM should have the ability to react to an adverse situation and manage security autonomously. Self-adaptation refers to the autonomous effective reaction of a system to minimize the effect of a risky situation [3].

In Table IV, we evaluate the suitability of the studied ISRM approaches against the above mentioned metrics to see how they address these metrics in order to be implemented in IoT-based eHealth.

V. TRENDS AND GAPS

Key elements of ISRM concerning IoT-eHealth are reviewed in this paper as system, S&P and InfoSec risk modeling and are evaluated as per projected requirements. The objective was to understand and recognize the essential operations, S&P challenges and methodologies for effective ISRM in IoT driven eHealth. A brief discussion on the evaluated knowledge corresponding to individual domains is conferred below to reflect the current trends and gaps in the existing literature.

– System Models

A total of 10 models are studied and analyzed according to the required features in a RPMS or IoT driven eHealth. Some of the models reviewed are focused on monitoring generic vital signs such as ECG, Blood pressure and heart rate [21], [25] while a few targets specific heart [17], [19] and chronic diseases such as diabetes [22]. Systems corresponding to [17], [19], [21], [22], [25] emphasized the use of cellular network (GPRS, GSM and UMTS) for the transmission of sensed data to the hospital site through the use of smart phones. However, simultaneous transmissions on cellular networks can cause performance degradation and may affect continuous monitoring in critical situations [25]. Except for [22], the importance of local analysis of sensed data is ignored in the rest of the models, which enable a patient to view his health status locally and schedule the daily routines accordingly. Similarly, actuation of medical infusions is also overlooked. A vital functionality of RPM is to diagnose the patient at home to save the time and energy spent in regular checkups, i.e., the provisioning of communication interface between a doctor and patient however, an absence is experienced of this feature in most of the systems reviewed. Those who support this functionality did not explicate it in detail. Santos et al. [20] on the other hand fairly explained a patient-doctor communication over a VOIP client, which can also be used in calling the health facilities in case of emergencies as well. Alarm generation is merely explored, except for [22] who detailed each alarm as per the assigned agent's responsibilities.

It can be seen that most of the system models are focused on the basic functionalities of collection, processing and delivery of vital signs to the remote hospital site. Analysis and correlation of various bio-signals are limited to the server side, which is needed to be shifted to the patient side to increase

TABLE III. MAPPING S&P REQUIREMENTS ONTO HIPAA

Author	Data Access	Confidentiality	Integrity	Availability	Alarm Gen.	Identity Mgt	Privacy	Authentication	Event Rep.
Lin et al. [28]	–	Symmetric Encryption	Hash	–	–	PKI based on Patient IDs	Symmetric Encryption & Pseudo ID	Shared Key	–
Apaporn et al. [30]	RBAC	Symmetric Encryption	–	–	–	–	–	Muliti-factor	–
Elkhodar et al. [32]	–	–	–	–	–	–	–	Multi-factor	–
Mona et al. [33]	–	Symmetric Encryption	SHA–1	–	–	–	–	Message Authentication Code(MAC) based on a Secret key	–
Khalid et al. [34]	–	–	–	–	–	–	–	User: Digital Signatures Message: Timestamps	–
Koichiro et al. [35]	AAA over NGN/IMS	–	–	Realtime Transfer Protocol (RTP)	–	–	–	AAA over NGN/IMS	SIP Event Subscribe/Notify Framework
Sriram et al. [31]	–	–	–	–	–	–	–	Multi-modal Biometrics	–
Malhotra [36]	RBAC	ECC	SHA-1	–	–	–	–	ECC based Digital Signatures	–

TABLE IV. ISRM APPROACHES SUITABILITY IN IOT-BASED EHEALTH

Author	Artifact	Analysis Method	Operational Nature	Context Awareness	Complexity	Self Adaptation
Don et al. [6]	Framework	Quantitative Analysis of patient activities	Dynamic	Event Correlation		No
Croll et al. [38]	Framework	Qualitative Investigation of Quality, Usability, Privacy and Safety (QUPS) Attributes	Dynamic & OnDemand	Investigating interdependent critical attributes and events		No
Hong et al. [7]	Model	Qualitative Assessment based on a questionnaire	On-Demand	No		No
Liu et al. [43]	Method	Quantitative RA based on attack detection in network packets using Artificial Immune System	Dynamic	No	Attack detection & RA are done by specific agents	Adaptation is performed only to enhance the detection capabilities.No mechanism of adapting a RM strategy
Maglog et l. [40]	Case Study	Threat Identification is performed using Bayesian Network Modeling whereas CRAMM is used as a RA method	On-Demand	Event dependencies are used to build the context of a specific threat	Unclear to evaluate the actual computation complexity just on the graphical model presented	No
Nes et al. [39]	Case Study	Methodology: Australian & New Zealand Standard for RM ASNZS 43601999. Qualitative Approach is used in the RA process	On-Demand	No		No
Abie et al. [3]	Framework	Monitor, Analyze & Adapt loop.	Dynamic	Game Theory & Context Awareness		Yes
Zhao et al. [41]	Model	Methodology: FMEA . Risk (RPN) is analyzed using Severity, Occurrence & Detection (SOD) values	On-Demand	No	Low: RPN = SxDxO	No
ENISA [42]	Case Study	Qualitative 5-Step EBIOS RA Methodology: Formulating Risk, Asset Valuation, Probability Calculation, Impact Valuation & Prioritizing Risk Levels	On-Demand	No	Low- Risk Calculation: Risk = (Threat x Vulnerability x Impact)	No

patient satisfaction. Mobility features should be well designed to support both in and out door patient and to facilitate ambulatory services [22]. Security and safety alarms are needed to be designed intelligently to support critical patient monitoring. Communication interface and GUIs needed to be constructed in order to enrich a patient-doctor relationship and trust.

– Security & Privacy

Among the HIPAA required services for secure remote and mobile patient monitoring systems, the most addressed are the confidentiality and authentication. However, none of them addresses all the HIPPA requirements. Our objective here is not to criticize this fact but to recognize how these requirements can be approached and to identify the current focus of S&P modeling and the necessary issues to be explored in future.

In most of the literature, Symmetric encryption is used to attain confidentiality [28] [30] [33]; however, asymmetric encryption using ECC is also explored [36]. Multi-factor authentication is used in a few studies where passwords, SIM credentials, GPS location, ID cards [30], [32] and vital signs (as biometrics) such as ECG and heart beats are used as various factors of authenticating patients and doctors [31]. Digital signatures are also used in authentication [34], [36]. Message authenticity is achieved by using packet timestamps and message authentication code [33], [34]. Hashing remained the only method of ensuring message integrity however, discussed by only a few [28], [33], [36]. Anonymity is only discussed in [28], where pseudo patient IDs are used to ensure identity privacy against global eavesdropping. Authorization through RBAC are conversed in [30], [36] but are not explicitly defined.

Some of the security services in a continuous RPM such as

event reporting, alarm generation and availability are yet to be researched. These are the services which are used in real-time delivery and emergency situations and are the key attributes of RPMS. Most of the literature summarized targets the extra-Body Area Network (Ex-BAN) security, which includes traditional web services and back end database resources in eHealth. As per our knowledge, there is a very limited literature available on securing inter-BAN communication specific to medical information exchange. Research is necessary to be done to secure these networks as they are the core producers of the medical information in an IoT-based eHealth or RPM. Also, the resources used in such networks have limited capabilities thus there is a need to design lightweight cryptographic solutions as discussed in [36] to be aligned with sensors computational competencies.

– InfoSec RM Models

Managing InfoSec risk in IoT-based eHealth is a tough task because of the diverse nature of technology utilized in it. The evaluation of the studied literature in context of ISRM reveals that almost all of them can be used in an On-Demand basis most of which are analyzing the risk on qualitative grounds [7], [39]–[42]. This is because of the subjective influence in RM process which makes it stiffer to be adapted in a dynamic environment. Those that can be executed in dynamic setups are suggested frameworks [3], [38] and still needs a keen and defined method of quantitative risk analysis. Liu et al. [43] on the other hand provide an effective method for analyzing the risk in a real time manner on a quantitative basis, which make it easier to program and usable for IoT-based eHealth. It also includes intelligent agents to adapt its attack detection capabilities and requires fewer resources as the threat detection and analysis is performed by specific agents. However, the suggested techniques are based on the inputs from signature based IDS, which makes it to generate false positives [9]. Self-adaptation as a risk management strategy is completely absent and needed to be designed intelligently to make IoT-eHealth an autonomous technology.

IoT-based eHealth needs quantitative methods for predicting and estimating threats in a dynamic fashion and should be capable of understanding and analyzing the threat situation and transforming the system security autonomously [3]. Some of the methods and framework discussed such as [3], [6], [43] can be utilized as a reference point to design the desired InfoSec RM methods for IoT driven eHealth.

VI. Conclusion and Future Work

In this paper, we have explored the existing literature in the context of approaching InfoSec risk management in IoT-based eHealth. A common knowledge of RMPSs, S&P issues, security and risk management modeling was established in the light of a standard risk management process. System models are evaluated against a set of required functionalities, models pertaining to security services are aligned with the standard HIPAA requirements and existing RM approaches in the context of IoT driven eHealth are weighed against a fitness criteria. An overall analysis is discussed and current trends and gaps are identified.

Our future work includes devising lightweight real-time InfoSec RM methods for IoT-based eHealth with the abilities of context awareness and self-adaptation. An adaptive security model will be developed that will address the mentioned InfoSec RM requirements. Security metrics and options necessary for the adaptation will be explored. To analyze the foreseen risk, Game and Utility theory will be used to model the dynamic and expected behaviors of adversaries and a comprehensive case study will be formulated to validate the model.

Acknowledgments

The work presented in this article is a part of the ASSET (Adaptive Security in Smart IoT in eHealth) project. ASSET (2012-2015) is sponsored by the Research Council of Norway under the grant agreement no: 213131/O70. Wishing thanks to the project colleagues and anonymous reviewers for their valuable suggestions and comments.

References

[1] R. H. Weber, "Internet of things: New security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23 – 30, 2010.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010.

[3] H. Abie and I. Balasingham, "Risk-based adaptive security for smart iot in ehealth," in *Proceedings of the 7th International Conference on Body Area Networks*, ser. BodyNets '12. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 269–275.

[4] H. K. Kalita and A. Kar, "Wireless sensor network security analysis," *International Journal of Next-Generation Networks (IJNGN),*, vol. 1, pp. 1–10, December 2009.

[5] M. Meingast, T. Roosta, and S. Sastry, "Security and privacy issues with health care information technology," in *Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE*, 2006, pp. 5453–5458.

[6] S. Don, E. Choi, and D. Min, "A situation aware framework for activity based risk analysis of patient monitoring system," in *Awareness Science and Technology (iCAST), 2011 3rd International Conference on*, 2011, pp. 15–19.

[7] J. I. Hong, J. D. Ng, S. Lederer, and J. A. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems," in *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*, ser. DIS '04. New York, NY, USA: ACM, 2004, pp. 91–100.

[8] S. Kumar, K. Kambhatla, F. Hu, M. Lifson, and Y. Xiao, "Ubiquitous computing for remote cardiac patient monitoring: a survey," *Int. J. Telemedicine Appl.*, vol. 2008, pp. 3:1–3:19, Jan. 2008.

[9] M. A. Rassam, M. Maarof, and A. Zainal, "A survey of intrusion detection schemes in wireless sensor networks," *American Journal of Applied Sciences*, vol. 9, no. 10, p. 1636, 2012.

[10] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, 2003, pp. 113–127.

[11] D. Christin, P. S. Mogre, and M. Hollick, "Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives," *Future Internet*, vol. 2, no. 2, pp. 96–125, 2010.

[12] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wirel. Netw.*, vol. 17, no. 1, pp. 1–18, Jan. 2011.

[13] J. L. Fernndez-Alemn, I. C. Seor, P. ngel Oliver Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *Journal of Biomedical Informatics*, no. 0, pp. –, 2013.

 ISBN: 978-1-61208-313-1

[14] A. Vorster and L. Labuschagne, "A framework for comparing different information security risk analysis methodologies," in *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*, ser. SAICSIT '05. Republic of South Africa: South African Institute for Computer Scientists and Information Technologists, 2005, pp. 95–103.

[15] P. L. Campbell and J. E. Stamp, "A classification scheme for risk assessment methods," last Accessed On: 13-Sept-2013. [Online]. Available: http://prod.sandia.gov/techlib/access-control.cgi/2004/044233.pdf

[16] E. Paintsil, "Taxonomy of security risk assessment approaches for researchers," in *Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on*, 2012, pp. 257–262.

[17] C. Otto, A. Milenković, C. Sanders, and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *J. Mob. Multimed.*, vol. 1, no. 4, pp. 307–326, Jan. 2005.

[18] R. S. Rajan, S.P. and S. Vijayprasath, "Design and development of mobile based smart tele-health care system for remote patients," *European Journal of Scientific Research*, vol. 70, p. 148158, 2012.

[19] M.-K. Suh, C.-A. Chen, J. Woodbridge, M. K. Tu, J. I. Kim, A. Nahapetian, L. S. Evangelista, and M. Sarrafzadeh, "A remote patient monitoring system for congestive heart failure," *J. Med. Syst.*, vol. 35, no. 5, pp. 1165–1179, Oct. 2011.

[20] A. Santos, R. Castro, and J. Sousa, "Carebox: A complete tv-based solution for remote patient monitoring and care," in *Wireless Mobile Communication and Healthcare*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, B. Godara and K. Nikita, Eds. Springer Berlin Heidelberg, 2013, vol. 61, pp. 1–10.

[21] A. Schacht, R. Wierschke, M. Wolf, M. von Lowis, and A. Polze, "Live streaming of medical data - the fontane architecture for remote patient monitoring and its experimental evaluation," in *Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW), 2011 14th IEEE International Symposium on*, 2011, pp. 306–312.

[22] S. Sneha and U. Varshney, "Enabling ubiquitous patient monitoring: Model, decision protocols, opportunities and challenges," *Decision Support Systems*, vol. 46, no. 3, pp. 606 – 619, 2009.

[23] Y.-C. Wu, P.-F. Chen, Z.-H. Hu, C.-H. Chang, G.-C. Lee, and W.-C. Yu, "A mobile health monitoring system using rfid ring-type pulse sensor," in *Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on*, 2009, pp. 317–322.

[24] I. Korkmaz, C. Atay, and G. Kyparisis, "A mobile patient monitoring system using rfid," in *Proceedings of the 14th WSEAS international conference on Computers: part of the 14th WSEAS CSCC multiconference - Volume II*, ser. ICCOMP'10. Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society (WSEAS), 2010, pp. 726–732.

[25] A. T. van Halteren, R. G. A. Bults, K. E. Wac, D. Konstantas, I. A. Widya, N. T. Dokovski, G. T. Koprinkov, V. M. Jones, and R. Herzog, "Mobile patient monitoring: The mobihealth system," *The Journal on Information Technology in Healthcare*, vol. 2, no. 5, pp. 365–373, October 2004.

[26] F. Kargl, E. Lawrence, M. Fischer, and Y. Y. Lim, "Security, privacy and legal issues in pervasive ehealth monitoring systems," in *Mobile Business, 2008. ICMB '08. 7th International Conference on*, 2008, pp. 296–304.

[27] W. Leister, H. Abie, A.-K. Groven, T. Fretland, and I. Balasingham, "Threat assessment of wireless patient monitoring systems," in *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, 2008, pp. 1–6.

[28] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," *Selected Areas in Communications, IEEE Journal on*, vol. 27, no. 4, pp. 365–378, 2009.

[29] S. P. Ramli Rusyaizila, Zakaria Nasriah, "Privacy issues in pervasive healthcare monitoring system: A review," *World Academy of Science, Engineering & Technology*, vol. 72, p. 741, 2011.

[30] A. Boonyarattaphan, Y. Bai, and S. Chung, "A security framework for e-health service authentication and e-health data transmission," in *Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on*, 2009, pp. 1213–1218.

[31] J. C. Sriram, M. Shin, T. Choudhury, and D. Kotz, "Activity-aware ecg-based patient authentication for remote health monitoring," in *Proceedings of the 2009 international conference on Multimodal interfaces*, ser. ICMI-MLMI '09. New York, NY, USA: ACM, 2009, pp. 297–304.

[32] M. Elkhodr, S. Shahrestani, and H. Cheung, "An approach to enhance the security of remote health monitoring systems," in *Proceedings of the 4th international conference on Security of information and networks*, ser. SIN '11. New York, NY, USA: ACM, 2011, pp. 205–208.

[33] M. Kamel, S. Fawzy, A. El-Bialy, and A. Kandil, "Secure remote patient monitoring system," in *Biomedical Engineering (MECBME), 2011 1st Middle East Conference on*, 2011, pp. 339–342.

[34] K. Elmufti, D. Weerasinghe, M. Rajarajan, V. Rakocevic, and S. Khan, "Timestamp authentication protocol for remote monitoring in ehealth," in *Pervasive Computing Technologies for Healthcare, 2008. Pervasive-Health 2008. Second International Conference on*, 2008, pp. 73–76.

[35] K. Rikitake, Y. Araki, Y. Kawahara, M. Minami, and H. Morikawa, "Ngn/ims-based ubiquitous health monitoring system," in *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*, 2009, pp. 1–2.

[36] K. Malhotra, S. Gardner, and R. Patz, "Implementation of elliptic-curve cryptography on mobile healthcare devices," in *Networking, Sensing and Control, 2007 IEEE International Conference on*, 2007, pp. 239–244.

[37] E. A. Oladimeji, L. Chung, H. T. Jung, and J. Kim, "Managing security and privacy in ubiquitous ehealth information interchange," in *Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication*, ser. ICUIMC '11. New York, NY, USA: ACM, 2011, pp. 26:1–26:10.

[38] P. R. Croll and J. Croll, "Investigating risk exposure in e-health systems," *International Journal of Medical Informatics*, vol. 76(5-6), pp. 460–465, 2006.

[39] H. E. S. T. Bnes E, Hasvold P, "Risk analysis of information security in a mobile instant messaging and presence system for healthcare," *International Journal of Medical Informatics*, vol. 76(9), pp. 677–687, 2007.

[40] I. Maglogiannis, E. Zafiropoulos, A. Platis, and C. Lambrinoudakis, "Risk analysis of a patient monitoring system using bayesian network modeling," *J. of Biomedical Informatics*, vol. 39, no. 6, pp. 637–647, Dec. 2006.

[41] X. Zhao and X. Bai, "The application of fmea method in the risk management of medical device during the lifecycle," in *e-Business and Information System Security (EBISS), 2010 2nd International Conference on*, 2010, pp. 1–4.

[42] ENISA, "Being diabetic in 2011 - identifying emerging and future risks in remote health monitoring and treatment," Technical Publication on ENISA website, 2009, last Accessed On: 13-Sept-2013. [Online]. Available: http://www.enisa.europa.eu/publications/archive/being-diabetic-2011/

[43] C. Liu, Y. Zhang, J. Zeng, L. Peng, and R. Chen, "Research on dynamical security risk assessment for the internet of things inspired by immunology," in *Natural Computation (ICNC), 2012 Eighth International Conference on*, 2012, pp. 874–878.

[44] G. Paliwal and A. Kiwelekar, "A comparison of mobile patient monitoring systems," in *Health Information Science*, ser. Lecture Notes in Computer Science, G. Huang, X. Liu, J. He, F. Klawonn, and G. Yao, Eds. Springer Berlin Heidelberg, 2013, vol. 7798, pp. 198–209.

[45] D. A. Tribble, "The health insurance portability and accountability act: security and privacy requirements," *American Journal of Health-Systems Pharmacy*, vol. 58, pp. 763–770, 2001.

 ISBN: 978-1-61208-313-1