IOT SECURITY RISK MANAGEMENT MODEL FOR HEALTHCARE INDUSTRY

Fathi Ibrahim Salih[1], Nur Azaliah Abu Bakar[2*], Noor Hafizah Hassan[3], Farashazillah Yahya[4], Nazri Kama[5] and Jalal Shah[6]

[1,2,3,5]Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia

[4]Faculty of Computing and Informatics, Universiti Malaysia Sabah, 88400 Kota Kinabalu, Sabah, Malaysia

[6]Department of Computer System Engineering & Sciences, Balochistan University of Engineering & Technology Khuzdar 89100, Pakistan

Email: i.salih@graduate.utm.my[1], azaliah@utm.my[2]*(corresponding author), noorhafizah.kl@utm.my[3], fara.yahya@ums.edu.my[4], mdnazri@utm.my[5], jalalshah@buetk.edu.pk[6]

DOI: https://doi.org/10.22452/mjcs.sp2019no3.9

ABSTRACT

Internet of Things (IoT) is predicted as one of the biggest emerging environments in the future that creates simultaneous smart communication between machines or a variety of digital devices. Besides improving how data can be controlled, monitored and collected, IoT also allows us to generate revenue through the identifying of new business opportunities and deployment of advanced analytics processes for decision-making purposes. IoT enables us to accelerate changes in the healthcare environment in improving patient engagement and outcome, as well as transforming healthcare from reactive to proactive accessibility. Nevertheless, IoT's expansion brings new vulnerabilities, risk and security challenges for healthcare practitioners and their patients. However, there is still a lack of study focusing on IoT risk management in healthcare. Existing researches tend to focus only on the implementation of IoT peripherals in a healthcare environment and tend to embed the secured applications solution with it. Since healthcare information and data are highly confidential, it is important to ensure that a secured health IoT application is in place. Thus, the aim of this study is to investigate the IoT risk management aspects in a healthcare environment with particular attention to proposing a step-by-step process of an IoT risk management model. The proposed IoT risk management model was developed leveraging on DEMATEL IoT Risk Assessment Procedure. This study was conducted based on a case study of one hospital in Sudan which has recently invested in IoT technologies in their operation. Interviews were conducted with selected respondents from the hospital and findings suggested that the selected case study does not have an established IoT risk management mechanism due to the ad-hoc IoT implementation approach. The case study also lacks of protection for health data and information with several unclear work process. As a solution, this study proposes an enhanced IoT risk management model for healthcare with consideration of three risk categories; 1) Secured Technology, 2) Human Privacy and 3) Trustable Process and Data. The proposed model was then evaluated by three IoT experts and two IT healthcare practitioners based on System Usability Score (SUS) and received Good Usability score which means the model is usable as a healthcare IoT risk management model.

Keywords: ***Security issues, IoT, Model, Risk Management, Healthcare***

1.0 INTRODUCTION

With some analysts suggesting that there will be more than 25 billion internet-connected things by 2020, an increasing number of businesses are using the internet of things (IoT) to streamline the processes and make customer experiences even better. In 1999, the buzzword of IoT was first mentioned by the founder of MIT Auto-ID Centre which identifies technologies in industries to automate, minimize errors and boost efficiency [1]. The vision of IoT is to connect anything, anyone, everywhere and at any time via identification technologies such as bar codes, smart cards, biometrics, sensors and voice recognition which are connected through wired or wireless systems like Bluetooth, Wi-Fi or 3G/4G cellular network[2]. Data collected from the input device will be processed collaboratively, relayed to one another, and react automatically. This will give a different view of the opportunities and challenges that IoT could offer.

Competitive industries such as the military, transportation, manufacturing and healthcare industry are moving forward to implement IoT by leveraging on its advantage to ensure that they are ahead of their competitors.

Healthcare is among the fast-growing industries in IoT with existing various applications ranging from remote monitoring to integrated mobile medication devices. Health-monitoring products enable the patient to monitor their nutrition, blood pressure, pulse, fitness or other vital signs and receive real-time feedback from hospitals, rehabilitation centres, doctors, nurses, the ambulance, assistive devices, etc. These identification devices are embedded with smart healthcare solutions and are linked to a network to collect and transmit patients' data via the internet making it ready to be retrieved by authorized healthcare personnel [3, 4].

IoT healthcare system requires a holistic healthcare ecosystem which involves people, process and technology. According to Venkatramanan and Rathina [5], there are four main components of an IoT Healthcare System which are Data, Devices, People and Process. Data represents all the health information obtained and stored in an IoT Cloud. Devices consist of all medical peripherals and equipment that are built IoT-ready, while People refer to all stakeholders in the healthcare practice such as doctors, patients and all types of medical practitioners. Finally, the Health-related process represents, namely, Care Delivery, Wellness and Preventive Care. Figure 1 represent the idea of how an IoT Platform can bring those elements together in the healthcare environment.

Fig 1: The confluence brought about by the Internet of Things [6]

Since data is transmitted online, protecting the confidentiality and integrity of patients' records are crucial to ensure the right treatments are set for the right patients. As highlighted by Tarouco, et al. [7], there are five main risks of IoT implementation in healthcare. They are; 1) Risk of patients' privacy exposure, 2) Threats of cyber-attacks on privacy, 3) Data eavesdropping and data confidentiality, 4) Identity threats and privacy of stored data and 5) Location privacy. However, distracted by the new features and capabilities of IoT, requirements for security and data privacy aspects have been overlooked [8].

This leaves a large gap in this area which opens to vulnerability in threats which triggered this research question; *"How to manage risk arisen from the implementation of IoT in healthcare?"*. Based on previous studies, it can be summarised that there are growing numbers of studies in IoT for healthcare, but the aspect of IoT risk management in healthcare is barely highlighted by researchers. Therefore, this paper aims to investigate IoT risk management in healthcare with particular attention in developing a step-by-step process of IoT risk management model. The following section will highlight the findings on IoT risk in the healthcare industry, review on existing IT risk management models and discussion on the proposed IoT Risk Management Model.

2.0 LITERATURE REVIEW

This section is divided into four, which are the explanation on the IoT characteristics, discussion on the current ICT risk management practice in healthcare, implementation and risk of IoT in healthcare and lastly type of risk of IoT in healthcare.

2.1 Characteristics of IoT

The IoT can be defined as the communication of connected "things" or devices to one or several other IoT devices [9]. The communication enables the IoT devices to communicate with each other and transmit data between the physical and virtual realm often autonomously. IoT devices such as smart devices and wireless sensors operate through the Internet or private network allow actions and services with little or no human intervention. However,

the quality of data is another essential requirement for the adoption of IoT services on a scale. In IoT, there are many connections between physical objects to the Internet that a lot of data needs to be transferred and managed properly and also there is a critical issue relating to security and privacy communication via the Internet [10].

IoT is generally divided into three layers from the aspect of technologies [11] which are; (i) Perception layer also known as sensing layer consists of various sensors, sensors gateways and actuators. It is responsible for identifying things collecting information and controlling things; (ii) network layer includes a variety of private networks, the Internet, mobile networks, the local area networks and wide area network and (iii) application layer is the interface of the IoT service and users. The most widely used IoT technologies are Radio Frequency Identification (RFID), Near Field Communication (NFC), Machine-to-Machine Communication (M2M) and Vehicle-to-Vehicle Communication (V2V) [12].

Basically, there is four types of ways how these IoT devices communicate with each other. The communication models are Device-to-Device, Device-to-Cloud, Device-to-Gateway, and Back-End Data-Sharing model [13].

i) Device- to-Device: The connected IoT devices exchange messages/data using IP networks such as ZigBee, Z-Wave, and Bluetooth

ii) Device-to-Cloud: The connected IoT devices exchange messages/data using the shortest route, connections between devices and cloud services are established using TCP/IP network or Wi-Fi connections

iii) Device-to-Gateway: The connected IoT devices exchange messages/data using application software as a communication link between IoT devices and the cloud. Usually, the apps act as a gateway to transmit data among the devices and cloud services to address the integration issues between new smart IoT devices and legacy systems

iv) Back-End Data-Sharing model: The connected IoT devices exchange messages/data through an authorized layer on the integrated cloud application which facilitates interoperability of IoT devices in cloud environments

2.2 Current ICT Risk Management Practice in Healthcare

In 2016, it is predicted that trust and benefits received from borderless ICT solutions indirectly encourage an individual to share their personal data willingly to health organizations. As a customer who likes to obtain better healthcare services, the public is pushed towards giving away their information to hospitals since it is dealing with life and death situations rather than the safety of information [14]. The advancement of IoT in healthcare is expected to grow as IoT devices have features such as low price, diminishing in size and reduced rate of consumption energy [15]. But how far hospitals are staying obliged to patient's data and the information is still a big question. For example, in 2015 many healthcare providers fell victim to cyber-attacks with a total of over 112 million records [16]. Cyber-attacks such as medical device hijack (MEDJACK), continues to increase gradually from 2016 to 2017 and it is difficult for hospitals to detect and remediate threats without upgraded technologies and implementation of best practices [17]. This caused the IT staffs to be more overstretched with significant control over defenceless medical devices, audits and penalties, action again human interaction devices and the applications used in a healthcare environment.

Exposure of different types of risk every day by healthcare agencies must be alleviated competently. In a highly integrated service environment like hospitals, it is considered as a risky environment, thus the requirement for the risk management guidelines, framework and standards is a must to better governance and control over risks. A study by [18] shows the integration of the risk management process, risk governance, organisational strategy and planning, operation management, reporting processes, policies, values and culture is an early effort to establish a strong risk management lifecycle with the customer and corporate values in the healthcare industry.

2.3 Implementation and Risk of IoT in Healthcare

According to the researchers, there are various types of threats that need to be addressed in a healthcare environment [7, 14, 16]. This issue can be related to hardware, software, application, remote connection and also other technology in use. For example, customization in hardware for IoT design will cater the need to fulfil the intended embedded systems design. Hence, it will be wrong to implement IoT devices using predetermined functions and platforms which are not intended for security purposes [19]. For the best practice, the network switches and devices designed to cater the IoT security needs should be carefully chosen by hospital information security officers instead of other parties [20].

An adequate communication system is vital to mitigate network risk and enhance risk management. Sfar, et al. [21] suggests applying the 6Lowpan adaptation layer, a highly secured technology in the healthcare security framework. Meanwhile, Catarinucci, et al. [22] and Amendola, et al. [23] enhanced the security of their IoT model by integrating sensor classification layers such as radio frequency identification (RFID), ultra-high frequency (UHF) and wireless sensor networks (WSN). Another group of researchers suggested self-monitoring healthcare devices be utilized in hospitals [24-26]. Such a device may use encryption technology in transferring data and securing data with some enhanced security protocols.

However, the advanced technology of IoT in the healthcare industry may lead to the issue of data privacy as it is open to self-remote access and control systems in hospitals [15]. Furthermore, it can also trigger the effect of signals and electromagnetics inside hospitals which might create additional issues for healthcare providers. To resolve this issue researchers [27, 28] suggested that an adaptation of smart and secured technology is a must in a risk management process as it will strengthen internet security, cloud computing security in the IoT environment and indirectly will drop the rate of network risk

2.4 Type of Risk of IoT in Healthcare

Based on the previous discussions, this study grouped IoT risks into three categories mentioned by [21] which are; 1) Secured Technology, 2) Human Privacy and 3) Trustable Process and Data. Following are the detailed discussion of the risk categories mentioned.

i. Secured Technology

To monitor a patient with chronic disease at home, there are several usages of sensing devices for a home telemonitoring system such as Wi-fi IP camera for patient movement detection, body scale and blood pressure monitor [7]. These devices are connected via Wi-fi to transmit data and the patient's personal data should be protected against unauthorized access because once the sensitive data is disclosed, it is irrevocable. These mobile devices are potential targets for malicious attacks that might steal patient's information, attack device resources and shut down some applications during operation. This refers to the fact that the device used by the end-user that can connect to the LAN and PAN over the Internet can easily be stolen and accessed by a malicious user [29]. The healthcare industry is working hard to overcome security issues but because of no system in the world is 100% guaranteed secure, therefore, a certain degree of acceptable risk must be defined [15].

ii. Human-Patient Privacy

Patient's information needs to be safeguarded to fulfil privacy requirement due to the risk of technology being abused by legitimate or illegitimate users [21]. Even though the patient agrees to share some information pertaining to their health condition, it is still subject to patient privacy with limited access. The information must be kept confidentially, with integrity and authenticity. The authorities need to have a definable legal action to protect patient privacy [15].

iii. Trustable Process and Data

Trust is another vital area of concern in the IoT of healthcare. This is referring to the validity of transmitted data which is then used to make life and death decisions for a patient [15]. The data might be corrupted and altered by malware during transmission via the internet. A study by [21] also mentioned the issue of trusting sensing devices whether it really makes the right assessment and produces reports accordingly to the authorized recipient. Accidental failures such as medical device malfunction might cause fatal consequences which could jeopardize trust in IoT technology [30]. Another reason for this is due to a lack of understanding and unawareness of the underlying risks of the various IoT components involved in a human being healthcare environment [28].

Table 1: Current Security Risk Effort in IoT for Healthcare

REF	Security Risk Effort in IoT for Healthcare	IoT Risk Category Sfar et al. (2018)		
		Secured Technology	Human Privacy	Trustable Process & Data
[18]	Reduce the IoTs vulnerability to attacks; since communications are mostly wireless, unattended things are usually vulnerable to physical attacks.	✓		
[19]	Customization in IoT hardware to strengthen the security	✓		
[19]	Able to tackle issues of lost signals, battery drain or loss, timing complications, programming bugs causing unresponsive behaviour	✓		
[19]	Must provide sufficient training in how to properly account for safety and reliability of new designs			✓
[20]	Secured design of network switches and devices in hospital	✓		
[21]	Implement highly secured technology in healthcare IoT implementation	✓		
[21]	The information must be kept confidentially, with integrity and authenticity		✓	
[21]	Ensure the trust of the sensing device if it really makes the right assessment and produces report accordingly to the authorized recipient.			✓
[24]	Adaption of smart and secureD technology for internet security, cloud computing security in the IoT environment	✓		
[22]	Enhance the IoT model by integrating sensor classification layers such as radio frequency identification (RFID), ultra-high-frequency (UHF) and wireless sensor network (WSN).	✓		
[25]	Use encryption technology in transferring data and securing data with some enhanced security protocol for self-monitoring healthcare devices to be utilized in hospitals a device may	✓		
[15]	The authorities need to have a definable legal action to protect patient privacy for any IoT devices that opens to self-remote access and control system in hospitals		✓	
[15]	Ensure the validity of transmitted data which then used to make life and death decision of a patient			✓
[29]	Protect the stored sensitive data in IoT devices and provide secure storage tools in the context of IoT to avoid physical attacks	✓		
[29]	Effective authentication technology should take to prevent illegal user involvement			✓
[30]	Establish a control mechanism whereby the user must make sure not to transmit unencrypted information across open networks that could bring loss to billing and medical information.			✓
[30]	Avoid any accidental failures such as medical device malfunction might cause fatal consequences which could jeopardize trust in the IoT technology			✓
[30]	The manufacturer must aware and learn more about the equipment's security capabilities, risks and real consequences	✓		
[30]	Patients and their families have a deep and personal understanding of how IoT device could affect their quality of life			✓
[28]	Increase the understanding and awareness of people on the underlying risks in the new IoT healthcare environment.			✓
[28]	Tighten the physical security controls; the fact that the device used by the end-user that can connect to the LAN and PAN over the Internet can easily be stolen and accessed by a malicious user	✓		
[7]	Strengthen the security for sensing devices for a home telemonitoring system are potential targets for the malicious attack that might steal patient's information, attack device resources and shutting down some applications during operation	✓		

REF	Security Risk Effort in IoT for Healthcare	IoT Risk Category Sfar et al. (2018)		
		Secured Technology	Human Privacy	Trustable Process & Data
	TOTAL	**12**	**2**	**8**

3.0 METHODOLOGY

This study methodology comprises of three steps which are i) Investigation of the current research by conducting literature analysis; ii) Model formulation based on the findings from literature and the selected case study and iii) Model evaluation by the IoT experts and Healthcare IT Officer based on System Usability Score (SUS).

IoT in the healthcare environment has become a new disruptive technology as it has changed the normal linear process to an integrated mesh process. As many scholars agreed that this contributes to healthcare process optimization, it also tends to invite new kinds of ICT security threats [18, 24, 29, 31]. To analyse this phenomenon, this study begins by reviewing related works in IoT in Healthcare. A search string of *"IoT"* AND *"healthcare"* AND *"security risk"* were used for the searching process in the research database, particularly IEEE, Web of Science, Elsevier and Scopus. In brief, there were 81 articles focusing on these topics, which later after a thorough filtration to *"risk management process"*, only 22 articles as shown in Table 1 are taken into consideration. Based on the findings, the initial idea of IoT risk model started to be conceptualised.

To enrich the model formulation process, this study selected a hospital with IoT implementation as a case. RC Hospital is a private hospital located in Khartoum, Sudan. The hospital was established in 2010 by Sudanese founders, providing multi-disciplinary healthcare ranging from advanced general health care services up until a healthcare research centre. To date, RC hospital has partially implemented IoT infrastructures to cater to customer needs. One of the recent projects is the installation of IoT connection directly from the ward to the lab to transfer patients' test results. This is done via a lab information system with specific modules of patient result tracking, patient registration and lab result processing. At this moment, the IoT infrastructures are only limited within the hospital perimeter.

From the preliminary interview with their Head of IT Department, one of the reasons for IoT area restriction is due to some security issues and no IoT Security Risk Management Plan exists in their ICT Security Policy. As a result, the management decided that RC hospital need to establish the IoT Security Risk Management plan first before further implementing the IoT solution.

To understand the phenomenon in this case study, a series of interviews were conducted with the IoT development team which consisted of the Head of the IT Department, the Senior IT Manager and the IT Security Officer. The interview questions were in an open-ended format consisting of the following questions:

i) Does this hospital have any IT Security Management Plan? If yes, what is it? / If No, why?
ii) Is there any formalized process of managing IoT and its risk?
iii) How well is the acceptance of IoT implementation among the healthcare practitioners and patients of this hospital?
iv) Have this hospital encounters any security threat with this IoT implementation?

The responses were analysed using thematic analysis [32] whereby all themes were categorized accordingly based on Sfar, et al. [21] risk management categorization, namely i) Secured Technology, ii)Human Privacy and iii)Trustable Process & Data. The results were then used in the formulation of a new model for IoT risk in healthcare. The newly formulated model was then evaluated by three IoT experts and two IT healthcare practitioners. This study applied a modified System Usability Scale (SUS) questionnaire [33] to evaluate the proposed model. SUS is a simple questionnaire, which is easy to administer and it provides reliable results even with a small sample size [33]. It is used by researchers in many different systems, frameworks or model, and able to demonstrate the differentiability between usable and unusable systems [34]. The hypothesis in the study was that the proposed IoT Risk Management Model is useful and able to assist the IoT implementation process in the healthcare environment.

SUS scale consists of simple subjective evaluation with ten items measured on a Likert scale from 1 (strongly disagree) to 5 (strongly agree). To calculate the SUS score, the score contributions from each item are first summed. Each item score contribution ranges from 0 to 4; for odd items, the score contribution is the scale position minus 1, and for even items, the contribution is 5 minus the scale position. The sum of the scores is multiplied by 2.5 to obtain the overall value of the SUS, and the total score ranges from 0 to 100%. Since this study is evaluating a model, not a 'system', the questionnaire was modified by changing the word 'system' with 'model', and 'functions' to 'criteria', as follows.

1. *I think that I would like to use this model frequently*
2. *I found the model unnecessarily complex:*
3. *I thought the model was easy to use:*
4. *I think that I would need the support of a technical person to be able to use this model*
5. *I found the various criteria in this model were well-integrated*
6. *I thought there was too much inconsistency in this model*
7. *I would imagine that most people would learn to use this model very quickly*
8. *I found the model very cumbersome to use*
9. *I felt very confident using the model*
10. *I needed to learn a lot of things before I could get going with this model*

A SUS score above 68 would be considered above average and anything below 68 is below average [33]. Meanwhile, according to Bangor et al. [34], it is passable to have SUS scores above 70, with better scoring in the high 70s to upper 80s. A truly superior score should be better than 90. Scores of less than 70 should be considered candidates for increased scrutiny and continued improvement and should be judged marginally at best. Figure 2 explains how the SUS score is tabulated based on scores by quartile of the acceptability adjective ratings of the average SUS score.

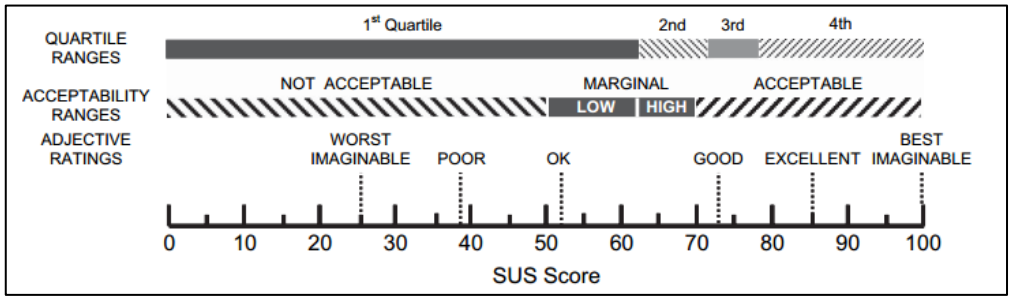

Fig 2: System Usability Scale (SUS) scores by quartile [34]

4.0 RESULTS AND DISCUSSIONS

The result and discussion section comprise of two subsections, first is the literature analysis of existing IoT Risk Management Models and the second is the findings from RC Hospital's IoT implementation and its associated risk. The outcome of these results is the proposed IoT Security Risk Management Model in Healthcare which will be discussed further in Section 5.

4.1 Review on Existing IoT Risk Management Model

As per described by Maksimović, et al. [35], there is an IoT communication framework requirement in healthcare applications such as:

i) Interoperability of different things to collaborate to deliver service
ii) Bounded latency and reliability especially in emergency situations
iii) Authentication, privacy and integrity are compulsory in exchanging sensitive data across the network.

Despite the conveniences of IoT in service delivery for the community, this technology handles huge security threats and the most challenges are from security and privacy issues. [36] describes four aspects of security and privacy

issues in IoT which are 1) data authentication, 2) resilience to attack, 3) access control and 4) client privacy. This indicates that risk assessment and management are very crucial in addressing and handling those security issues [32]. It is commonly understood that risk assessment is the third process in risk management lifecycle. Risk assessment means assessing security incidents from two dimensions, firstly the likelihood and secondly the adverse impact of an incident. Then after the risk management plans are implemented, there is a need for follow-on actions as part of a comprehensive assessment and continuous [37].

From the analysis conducted, events that are likely to impact the organization will be identified and treated accordingly. There are several steps in risk assessment such as identifying, estimating, and prioritizing information security risks and these steps vary according to risk management models [38]. Listed below are six risk management models identified from the literature.

i) Information Security Risk Assessment (ISRA): aim to protect the security of asset from vulnerability and threat, and to ensure the information confidentiality, integrity and availability.
ii) Fuzzy Comprehensive Evaluation Method (FCEM): mature assessment method used to resolve difficult quantification (fuzzy)
iii) Analytic Hierarchy Process (AHP): expected to be independence from risk assessment families
iv) Privacy Security Risk Assessment (PSRA): an immature model that helps early risk detection for IoT system.
v) Bayesian Network (BN): compute the probability of risk level and analyses threat propagation
vi) Decision-Making Trial and Evaluation Laboratory (DEMATEL): analyse relationships between factors and convert the relationships into a comprehensible structure model

Above all of the risk management models mentioned earlier, this study opts to discuss on the new Privacy Security Risk Assessment (PSRA) model which is based on the Decision-Making Trial and Evaluation Laboratory (DEMATEL) and Bayesian Network (BN) [22]. The DEMATEL process was applied in various risk assessment fields such as oil and gas construction projects [39]; smart cities [40], cargo ship management [41], software project management [42] and electronic supply chains [43]. This model was chosen as it is able to provide early risk detection in IoT application, thus it supports the IoT risk management process. There are four stages in DEMATEL starting from Stage 1: Assessment Preparation; Stage 2: Elements Identification; Stage 3: Risk Analysis and Calculation and Stage 4: Risk Management. Figure 3 describes the detail process in DEMATEL.

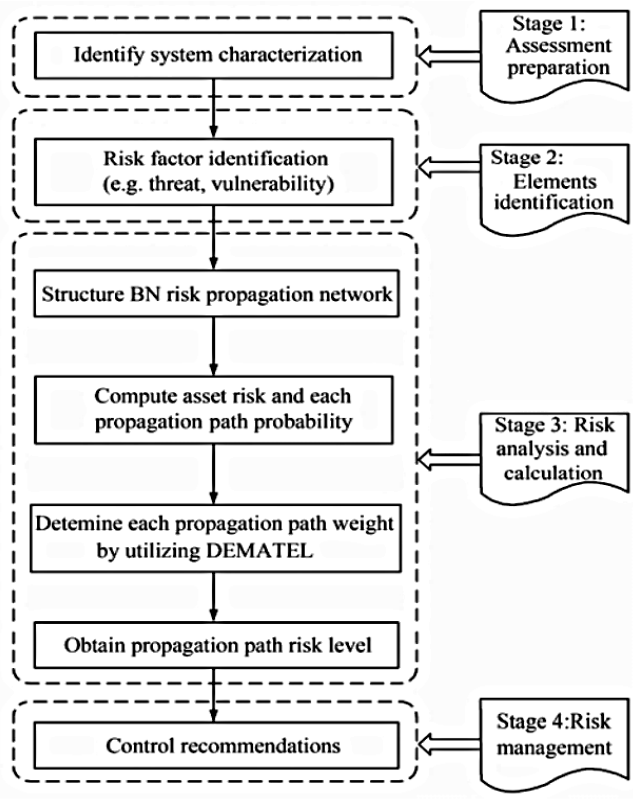

Fig 3: DEMATEL IoT Risk Assessment procedure

DEMATEL process started off with identifying the system characterisation meaning that understanding the as-is environment of the system, then set the goal, scope and aim for the assessment. Then followed by risk factor identification whereby all the possible risk elements (risk, likelihood and vulnerability) are listed accordingly. Only then all elements will be structured according to BN risk propagation network which leads to the computation of risk probability. Next, DEMATEL will analyse each propagation path weight and path risk level, then finally recommends the appropriate risk control.

4.2 Case Study Findings

Findings from the RC Hospital shows that this hospital has an IT Security Management Plan but not centralised in governance. The infrastructure pertaining to medical technology such as health analysers, heart rate machines, x-ray and scanner machines is maintained and monitored by every departments' authority. Some are still maintained by third party contractors. Initial findings show that most of their risk management relies on staffs' daily monitoring activities. This leads to loose control of data security and information privacy protection. However, records show that RC hospital is audited internally and externally every year. During the auditing process, some risks were identified and managed but more on the non-IT risks rather than the IT and IoT infrastructure. To date, their IoT practice is well accepted by all healthcare practitioners and patients. They also never encounter any security threats literature this IoT technology since its implementation. Overall, it can be concluded that their IoT implementation is more on ad-hoc actions and there is no IoT risk management plan existing yet in RC Hospital, even though they have successfully implemented IoT in their daily healthcare operation.

5.0 PROPOSED IOT RISK MANAGEMENT MODEL FOR HEALTHCARE

Based on the literature analysis and RC Hospital's case study findings, this study proposes an IoT Security Risk Management Model for Healthcare with consideration of three categories of risk which are 1) Secured Technology, 2) Human Privacy and 3) Trustable Process and Data. The newly proposed model concentrates more on ensuring that state of the art and upgraded IoT technology infrastructures are in place. The following sections describe the process of model formulation and later the model evaluation.

5.1 Model Formulation

The proposed IoT Security Risk Management Model for Healthcare was derived from the DEMATEL procedure with a focus on IoT Healthcare for patient safety which comprises of processes, secured technology, human privacy and trustable process and data. In this model, each phase is designed such that information of patients are safeguarded in the new technology wave. This model will help IT security officers to enhance and improve their current IoT architecture and mitigate technology risks such as cyber-attacks, medical device hijack and ransomware in hospitals

This 5-steps model was formulated based on the 4 stages of DEMATEL IoT Risk Assessment procedure and was modified as per case study suitability. DEMATEL Stage 1: Assessment Preparation was updated to Setting Goals; DEMATEL Stage 2: Element Identification was updated to Technology Risk Evaluation; DEMATEL Stage 3: Risk Analysis and Calculation was updated into two steps reassure improvement and innovation, and facilitating transformation; finally DEMATEL Stage 4: Risk Management ("Controlled Recommendation") becomes Common Process. The justification is based on the feedback received from the respondents that this stage is referring to how the existing healthcare process should be operated as a common process but with an awareness of that IoT risk control and countermeasure are in place. The complete model was shown in Figure 4.

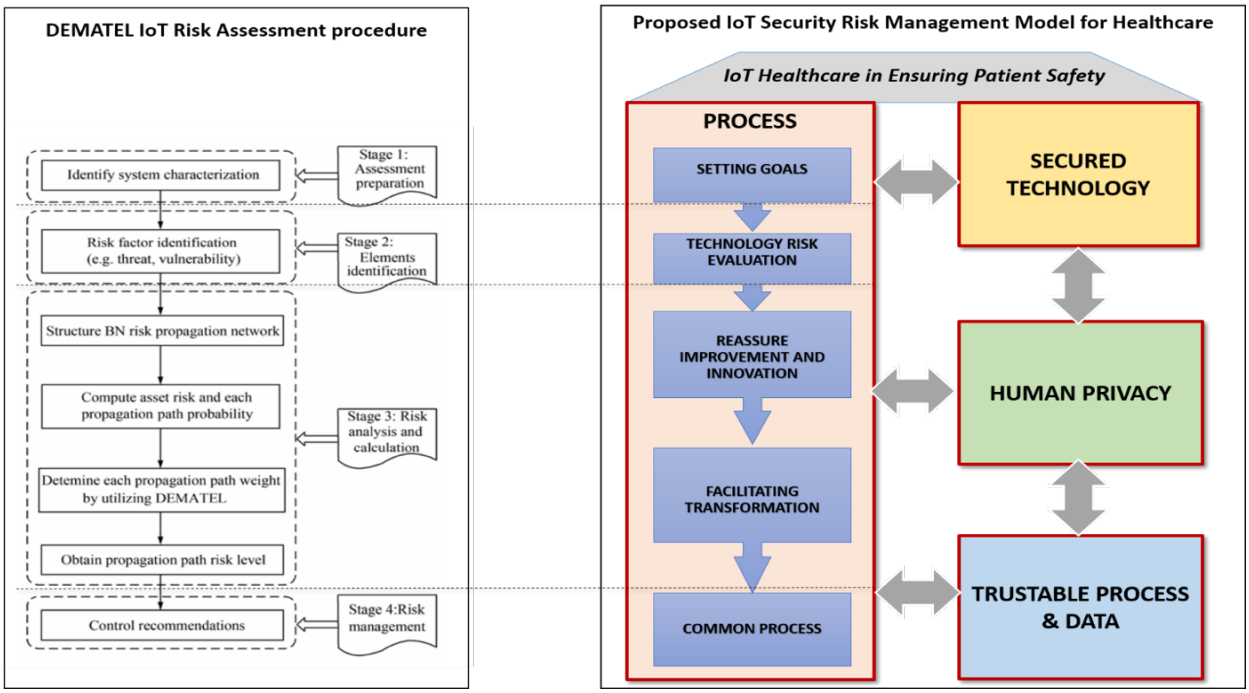

Fig 4: The formulation of IoT Security Risk Management Model for Healthcare based on DEMATEL procedure

To understand how this model works, the following section will describe all the activities involves in each step and the justification.

Step 1: Setting Goals

It is important for a healthcare organization to set clear goals before implementing IoT. These objectives will help them get a clear view of what they going to achieve by implementing IoT infrastructures in the organization. Without goals, the implementation of IoT could go wrong, because it may lead to possessing the unwanted infrastructures and wasting the cost of implementation. Goals also help to estimate some of the risks before implementation which may help in cost saving. At this level, hospitals may plan efficiently their IoT implementation and utilization of new technologies to achieve their targeted objective. A careful plan and documented goals may help to create a proper set of IoT infrastructures design as efficient infrastructure is one of the crucial elements in guarding the patient's information and hospitals assets.

Step 2: Technology Risk Evaluation

Technology risk evaluation will be different from the normal risk evaluation. This evaluation only caters to technology risk connected to IoT infrastructure focusing on the healthcare domain. Hence it will be more specifically evaluated from the IoT infrastructures in hospitals and possible risk identified associated more towards patient safety. Once the goals are finalized, the organization may conduct a technology risk evaluation. This is an important level in risk management as all technologically related risk will be identified and listed. Subsequently, many hospitals fall short in technologies at this level, whereby it will guarantee their IT infrastructures safety. Also, for IoT implemented hospital, existing infrastructures is evaluated, and risk is identified at this level.

Step 3: Reassure improvement and innovation

Then, the identified risk in the previous step will be analyzed. The purpose is to apply countermeasure which related to the improvement of IoT infrastructure and innovation implementation. The rapid development of IT may lead to an outdated system or devices, which may cause more danger to hospitals. Therefore, continues improvement and updating IoT infrastructures is important as well as upgrading it to the more advanced system in order to create durable security. This innovative step will assist in implementing efficient IoT with minimal cost and higher security in healthcare.

Step 4: Aiding transformation

Performing transformation in a healthcare environment is a challenging process. This is because it is hard to interrupt a hospital process which is on-going since it is strongly associated with human life and critical services. Often this is an obstacle for the healthcare environment whenever they require changes or improvement to the current infrastructures. Therefore, a carefully planned transformation must exist to ensure any changes is at low risk to the hospital's operations. Transformation not only in technology but also can be applied to a human resource (people) and also hospital work process. Hospital staff need to be trained in the latest ICT technology apart from medical skills only. The aim is to manage IT devices and educate other staffs on cyber threats awareness and so on. With this exposure, it may help medical staff in taking appropriate action during threats and they do not have to fully dependent on support from IT staffs only.

Step 5: Common Process

This is the final step, which is 'Common Process'. This is the uniqueness of this model since another model normally does not consider this as a crucial step in risk management. Other models are more on protection approach whereby this model consist both by allowing the prevention in place. This step allows IT security office to utilize the other common process which is relevant in mitigating healthcare risk. This includes normal steps as controlling and applying countermeasures. These steps allow the officer to prioritize the risk management process which suits best for the healthcare environment and alleviate the unwanted process. This is because some of the processes are not relevant to healthcare and may relevant to other organization, therefore it is important to study which activities are important to hospitals and IoT infrastructures in healthcare and prioritized that particular processes. This will help to design a risk management activity which is more competent to hospitals.

5.2 Model Evaluation

The Healthcare IoT Risk Management Model was evaluated for its usability based on the System Usability Scale (SUS) questionnaire [33]. The evaluation was conducted by three IoT experts and two Healthcare IT Practitioners. The result shows that average SUS score for all participants was 72.54, thus this model was perceived to have 'good usability' which corresponds to the adjective scale presented by Bangor et al [34] in Fig 2 which means the evaluated model is acceptable. Figure 5 depicts the mentioned score.

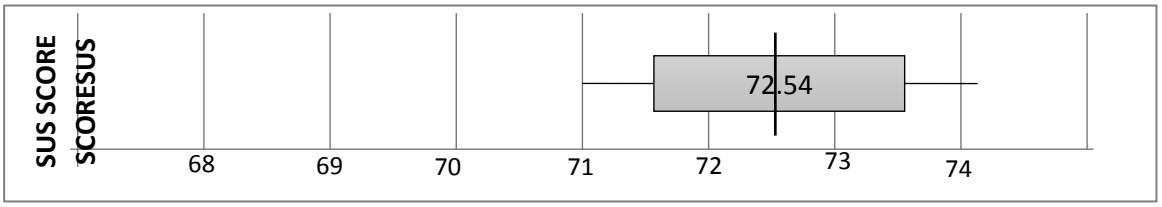

Fig 5: Box plot of average Healthcare IoT Risk Management Model SUS scores

This indicates that the evaluation scores from these agencies are above average based on SUS Score (*score above 68 would be considered above average)*. Apart from the SUS score, we also interviewed the evaluators these three questions.

i) What is your opinion regarding this Healthcare IoT Risk Management Model?
ii) Does it help and guide the IoT implementation process?
iii) What is your suggestion to improve this model?

These are the feedback received from the evaluators, which can be categorised into two aspects. Firstly, is the benefits of healthcare IoT risk management model. All participants agreed that this model is useful to assist the implementation of IoT from the risk management perspective. Participants also suggested that this model should be extended to other healthcare agencies that will implement IoT as a solution. Secondly is on the applicability of healthcare IoT risk management model in the real environment. From the interviews, evaluators suggested two best occasions to utilize this model which are 1) Prior the implementation of any IoT project in order to identify and manage the anticipated risk and 2) Post IoT project implementation, with the aim to assess the occurring risks and how to manage it.

6.0 CONCLUSION

Risk can be defined as a state of increased awareness approach in the organization. Nevertheless, there are hospitals yet to implement a complete risk management system. Implementing and maintaining risk management in a healthcare environment requires continuous observation. Security administration teams need to be formed to protect each level of the risk management process and ensure countermeasures are being adhered. Critical services in hospitals often slow down upgrading and innovation processes. But it is the effort of a risk management team to continue their task efficiently without interrupting the service. In addition to dealing with immediate crises, auditing can point out weaknesses in technology controls and help the administrator understand changes that need to be made to preserve the necessary risk management within the environment.

To increase the effectiveness of the risk management process, it is significant to use technologies high in cybersecurity and also protected IoT infrastructures. In a big organization such as a hospital, it is impossible to deploy IoT infrastructures efficiently through the security officer alone, thus a team of IT experts are required to work together to achieve this aim. In addition, the team can invest in deploying specific risk management software to the healthcare industry. Lastly, above all, a well-defined healthcare business process is the key to any risk management plan. The IoT Security Risk Management Model for healthcare that we proposed comprises of 1) Secured Technology, 2) Human Privacy and 3) Trustable Process and Data. In short, this model has analysed and proposed a holistic risk management solution for the healthcare industry since the element of technology, human, process and data are in place. Therefore, looking at the inclusiveness of this model we hope that it can strengthen the healthcare industry in regard to risk management in IoT implementation.

ACKNOWLEDGEMENT

The research is financially supported by Universiti Teknologi Malaysia (UTM) PAS Grant Q.K130000.2738.03K32.

REFERENCES

[1] M. Elkhodr, S. Shahrestani, and H. Cheung, "The Internet of Things: vision & challenges," in IEEE 2013 Tencon-Spring, 2013, pp. 218-222: IEEE.

[2] Y.-K. Chen, "Challenges and opportunities of internet of things," in 17th Asia and South Pacific design automation conference, 2012, pp. 383-388: IEEE.

[3] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," Future Generation Computer Systems, vol. 78, pp. 659-676, 2018.

[4] P. Kaviya, "Intelligent Healthcare Monitoring in IoT," International Journal of Advanced Engineering, Management and Science, vol. 4, no. 6, 2018.

[5] P. Venkatramanan and I. Rathina, "Healthcare leveraging internet of things to revolutionize healthcare and wellness," IT Services Business Solutions Consulting, 2014.

[6] P. Venkatramanan and I. Rathina, "Healthcare Leveraging Internet of Things to revolutionize Healthcare and Wellness," IT Services Business Solutions Consulting2014.

[7] L. M. R. Tarouco et al., "Internet of Things in healthcare: Interoperatibility and security issues," in Communications (ICC), 2012 IEEE International Conference on, 2012, pp. 6121-6125: IEEE.

[8] MCMC, " INTERNET OF THINGS (IOT) TECHNICAL REGULATORY ASPECTS & KEY CHALLENGES," Malaysian Communications and Multimedia Commission2018.

[9] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015, pp. 336-341: IEEE.

[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer networks, vol. 76, pp. 146-164, 2015.

[11] P. Sethi and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," Journal of Electrical and Computer Engineering, vol. 2017, 2017.

[12] J. H. Nord, A. Koohang, and J. Paliszkiewicz, "The Internet of Things: Review and theoretical framework," Expert Systems with Applications, 2019.

[13] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, "The application of internet of things in healthcare: a systematic literature review and classification," Universal Access in the Information Society, pp. 1-33, 2018.

[14] H. K. Patil and R. Seshadri, "Big data security and privacy issues in healthcare," in Big Data (BigData Congress), 2014 IEEE International Congress on, 2014, pp. 762-765: IEEE.

[15] Y. Yuehong, Y. Zeng, X. Chen, and Y. Fan, "The internet of things in healthcare: An overview," Journal of Industrial Information Integration, vol. 1, pp. 3-13, 2016.

[16] D. Munro, "Data breaches in healthcare totaled over 112 million records in 2015," New York, NY: Forbes, vol. 31, 2015.

[17] M. Hills, "Beyond simple human threats to cybersecurity: the need for strong proactive measures and resilient responses to cyber risk," Cyber Security Review, no. 2015, pp. 26-30, 2015.

[18] 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, 2012, pp. 269-275: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[19] P. A. Wortman, F. Tehranipoor, N. Karimian, and J. A. Chandy, "Proposing a modeling framework for minimizing security vulnerabilities in IoT systems in the healthcare domain," in Biomedical & Health Informatics (BHI), 2017 IEEE EMBS International Conference on, 2017, pp. 185-188: IEEE.

[20] O. Mavropoulos, H. Mouratidis, A. Fish, and E. Panaousis, "Apparatus: A Framework for Security Analysis in Internet of Things Systems," Ad Hoc Networks, 2018.

[21] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," Digital Communications and Networks, vol. 4, no. 2, pp. 118-137, 2018.

[22] L. Catarinucci et al., "An IoT-aware architecture for smart healthcare systems," IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515-526, 2015.

[23] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, "RFID technology for IoT-based personal healthcare in smart spaces," IEEE Internet of things journal, vol. 1, no. 2, pp. 144-152, 2014.

[24] J. Pacheco and S. Hariri, "IoT security framework for smart cyber infrastructures," in Foundations and Applications of Self* Systems, IEEE International Workshops on, 2016, pp. 242-247: IEEE.

[25] G. Banda, K. Chaitanya, and H. Mohan, "An IoT protocol and framework for OEMs to make IoT-enabled devices forward compatible," in 2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), 2015, pp. 824-832: IEEE.

[26] P. Mvelase, Z. Dlamini, A. Dludla, and H. Sithole, "Integration of smart wearable mobile devices and cloud computing in South African healthcare," in eChallenges e-2015 Conference, 2015, pp. 1-10: IEEE.

[27] M. N. Alraja, M. M. J. Farooque, and B. Khashab, "The Effect of Security, Privacy, Familiarity and Trust on Users' Attitudes Towards the Use of IoT-based Healthcare: The Mediation Role of RiskPerception," IEEE Access, 2019.

[28] S. Ahmed, "BYOD, Personal Area Networks (PANs) and IOT: Threats to Patients Privacy," arXiv preprint arXiv:1902.06462, 2019.

[29] W. AL-mawee, "Privacy and security issues in IoT healthcare applications for the disabled users a survey," 2012.

[30] J. Healey, N. Pollard, and B. Woods, "The healthcare internet of things: Rewards and risks," Atlantic Council, 2015.

[31] C. Thota, R. Sundarasekar, G. Manogaran, R. Varatharajan, and M. Priyan, "Centralized fog computing security platform for IoT and cloud in healthcare system," in Exploring the convergence of big data and the internet of things: IGI Global, 2018, pp. 141-154.

[32] C. Braun and R. Winter, "A comprehensive enterprise architecture metamodel and its implementation using a metamodeling platform," 2005.

[33] J. Brooke, "SUS-A quick and dirty usability scale," Usability evaluation in industry, vol. 189, no. 194, pp. 4-7, 1996.

[34] A. Bangor, P. T. Kortum, and J. T. Miller, "An empirical evaluation of the system usability scale," Intl. Journal of Human–Computer Interaction, vol. 24, no. 6, pp. 574-594, 2008.

[35] M. Maksimović, V. Vujović, and B. Perišić, "A custom Internet of Things healthcare system," in Information Systems and Technologies (CISTI), 2015 10th Iberian Conference on, 2015, pp. 1-6: IEEE.

[36] R. H. Weber, "Internet of Things–New security and privacy challenges," Computer law & security review, vol. 26, no. 1, pp. 23-30, 2010.

[37] J. A. Lewis, Managing risk for the internet of things. Center for Strategic & International Studies, 2016.

[38] L. Liang, W. Ren, J. Song, H. Hu, Q. He, and S. Fang, "The state of the art of risk assessment and management for information systems," in 2013 9th International Conference on Information Assurance and Security (IAS), 2013, pp. 66-71: IEEE.

[39] G. Dehdasht, R. Mohamad Zin, M. Ferwati, M. Abdullahi, A. Keyvanfar, and R. McCaffer, "DEMATEL-ANP risk assessment in oil and gas construction projects," Sustainability, vol. 9, no. 8, p. 1420, 2017.

[40] T. G. Rad, A. Sadeghi-Niaraki, A. Abbasi, and S.-M. Choi, "A methodological framework for assessment of ubiquitous cities using ANP and DEMATEL methods," Sustainable cities and society, vol. 37, pp. 608-618, 2018.

[41] A. Mentes, H. Akyildiz, M. Yetkin, and N. Turkoglu, "A FSA based fuzzy DEMATEL approach for risk assessment of cargo ships at coasts and open seas of Turkey," Safety science, vol. 79, pp. 1-10, 2015.

[42] A. K. Sangaiah, O. W. Samuel, X. Li, M. Abdel-Basset, and H. Wang, "Towards an efficient risk assessment in software projects–Fuzzy reinforcement paradigm," Computers & Electrical Engineering, vol. 71, pp. 833-846, 2018.

[43] R. Rajesh and V. Ravi, "Analyzing drivers of risks in electronic supply chains: a grey–DEMATEL approach," The International Journal of Advanced Manufacturing Technology, vol. 92, no. 1-4, pp. 1127-1145, 2017.