VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Jnana Sangama, Belgavi-590018

A TECHNICAL SEMINAR REPORT

On

"IOT Security Risk Management Model for Secured Practice in Healthcare Environment"

Submitted in partial fulfilment of the requirement for the degree of

BACHELOR OF ENGINEERING

In

COMPUTER SCIENCE & ENGINEERING

Submitted by

SREELEKHA PASIKANTI (1RG16CS096)

Under The Guidance of

Mrs. Geetha Pawar

Asst Professor, Dept of CSE

RGIT, Bengaluru-32

Department of Computer Science & Engineering

RAJIV GANDHI INSTITUTE OF TECHNOLOGY

Cholanagar, R.T.Nagar Post, Bengaluru-560032

2019-2020

RAJIV GANDHI INSTITUTE OF TECHNOLOGY

(Affiliated to Visvesvaraya Technological University)

Cholanagar, R.T.Nagar Post, Bengaluru-560032

Department of Computer Science & Engineering

CERTIFICATE

This is to certify that the seminar report titled **"IOT Security Risk Management Model for Secured Practice in Healthcare Environment"** is a bonafide work carried out by **Ms. Sreelekha Pasikanti (USN 1RG16CS096)** in partial fulfillment for the award of **Bachelor of Engineering** in **Computer Science and Engineering** under **Visvesvaraya Technological University, Belagavi**, during the year **2019-2020.** It is certified that all corrections/suggestions given for Internal Assessment have been incorporated in the report. This technical seminar report has been approved as it satisfies the academic requirements in respect of technical seminar work prescribed for the said degree.

Signature of Guide	Signature of HOD
Mrs. ……	**Mrs. Arudra A.**
Asst. Professor	Head Of Department
Dept. of CSE,	Dept. of CSE,
RGIT, Bengaluru	RGIT, Bengaluru

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Jnana Sangama, Belgavi-590018

RAJIV GANDHI INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DECLARATION

I hereby declare that the technical seminar report entitled **"IOT Security Risk Management Model for Secured Practice in Healthcare Environment"** submitted to the **Visvesvaraya Technological University, Belagavi** during the academic year **2019-2020**, is record of an original work done by me under the guidance of **Mrs. Geetha Pawar,** Asst Professor, Department of Computer Science and Engineering, RGIT, Bengaluru in the partial fulfillment of requirements for the award of the degree of **Bachelor of Engineering** in **Computer Science & Engineering.** The results embodied in this technical seminar report have not been submitted to any other University or Institute for award of any degree or diploma.

Sreelekha Pasikanti (1RG16CS096)

ACKNOWLEDGEMENT

I take this opportunity to thank my college **Rajiv Gandhi Institute of Technology, Bengaluru** for providing me with an opportunity to carry out this technical seminar report work.

I express my gratitude to **Dr. Nagaraj A M**, Principal, RGIT, Bengaluru and to **Dr. D G Anand**, Rector, RGIT, Bengaluru for providing the resources and support without which the completion of this seminar would have been a difficult task.

I extend my sincere thanks to **Mrs. Arudra A**, Associate Professor and Head, Department of Computer Science and Engineering, RGIT, Bengaluru, for being a pillar of support and encouraging me in the face of all adversities.

I would like to acknowledge the through guidance and support extended towards me by **Mrs. Geetha Pawar**, Assistant Professor, Dept of CSE, RGIT, Bengaluru**, Mrs. Pragathi M,** Assistant Professor, Dept of CSE, RGIT, Bengaluru. Their incessant encouragement and valuable technical support have been of immense help. Their guidance gave me the environment to enhance my knowledge and skills and to reach the pinnacle with sheer determination, dedication and hard work.

I also want to extend my thanks to the entire faculty and support staff of the Department of Computer Science and Engineering, RGIT, Bengaluru, who have encouraged me throughout the course of the Bachelor's Degree.

I want to thank my family for always being there with full support and for providing me with a safe haven to conduct and complete my technical seminar. I will be ever grateful to them for helping me in these stressful times.

Lastly, I want to acknowledge all the helpful insights given to me by all my friends during the course of this technical seminar.

Sreelekha Pasikanti (1RG16CS096)

ABSTRACT

The emerging of Internet of Things (IoT) technologies for unified and interconnected medical devices and sensors has changed the scenario in the healthcare with the ‘openness’ of the and distributed environment and medical devices ,IoT will be the point of breach where attackers are able to identify vulnerabilities and subsequently launch their attacks.This becomes high risk to the health care environment which may cause a big impact on security measure . Nonetheless the benefits of IOT solution in health care is undeniable. To address this issue, this study proposes an IoT Security Risk Management Model for Secured Practice in Healthcare Environment. This study reviewed all IoT risks from related works and has selected one Malaysian government hospital as a case study. From the findings, a model was formulated which consist of three parts, the Healthcare IoT Risk Management, the Hospital Performance Indicator for Accountability (HPIA) and the implementation phases. As a result, a priori model was successfully developed and yet to be validated by the case study participants in the next stage.

CONTENTS

Acknowledgement i

Abstract ii

List of Figures iv

List of Tables v

CHAPTER	TITLE	PAGE NO
1	**INTRODUCTION**	**2**
1.1	Internet of Things (IoT)	2
1.2	IoT and Healthcare	3
2	**IoT HEALTHCARE COMPONENTS AND ITS RISKS**	**5**
2.1	RFID and WSN	6
2.2	IoT Middleware and Cloud Computing	7
3	**IoT APPLICATIONS AND RISK MANAGEMENT**	**10**
3.1	IoT Applications	10
3.2	COBIT5 Framework for IoT Risk Management	11
4	**RESEARCH METHODOLOGY**	**14**
4.1	Planning	14
4.2	Design	14
4.3	Prepare	15
4.4	Collect	15
4.5	Analyse	15
4.6	Sharing	16
5	**FORMULATION OF IoT SECURITY MODEL FOR HEALTHCARE**	**18**
5.1	COBIT IoT Risk Management	19
5.2	HPIA	19
5.3	Implementation Phases	20
	CONCLUSION	**22**
	REFERENCES	**24**

LIST OF FIGURES

FIGURE NO.	FIGURE NAME	PAGE NO
Figure 2.1	WSN with IoT connected Healthcare Platform	5
Figure 3.1	COBIT5 Framework for IoT Risk Management	12
Figure 5.1	Proposed model of IoT Security Risk Management for Healthcare Practice	18

LIST OF TABLES

TABLE NO.	TABLE NAME	PAGE NO
Table 3.1	IoT Risk Factors in Healthcare Environment	11

INTRODUCTION

CHAPTER 1

INTRODUCTION

The emerging of Internet of Things (IoT) technologies for unified and interconnected medical devices and sensors has changed the scenario in the healthcare industry. However, with the 'openness' of the distributed environment and medical devices, IoT will be the point of a breach where attackers are able to identify vulnerabilities and subsequently launch their attacks. This becomes high risk to the healthcare environment which may cause a big impact on its security measure. Nonetheless, the benefits of IoT solution in healthcare are undeniable. To address this issue, this study proposes an IoT Security Risk Management Model for Secured Practice in Healthcare Environment. This study reviewed all IoT risks from related works and has selected one Malaysian government hospital as a case study. From the findings, a model was formulated which consist of three parts, the Healthcare IoT Risk Management, the Hospital Performance Indicator for Accountability (HPIA) and the implementation phases. As a result, a priori model was successfully developed and yet to be validated by the case study participants in the next stage.

1.1 Internet Of Things (IOT)

The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IOT is a latest technology epitome that its emergence is intended to connect machines, devices and applications via the network. It is based on the idea that internet connection will not be restricted to laptop, desktops and tablets as in previous decades but any physical devices that is embedded with electronics, software, sensors, actuators, and connectivity will be able to connect and exchange data within theirs . Lists of hardware and applications generally become smarter by having more data accessibility and network expansion opportunities. The IoT's major significant trend in recent years is the explosive growth of devices connected and controlled by the Internet. The wide range of applications for IoT technology mean that the specifics can be very different from one device to the next but there are basic characteristics shared by most. The IoT creates opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions.

1.2 IOT and Healthcare

Recently various IoT applications are being developed based on healthcare platform. One of the purposes of developing IoT devices is to help the healthcare personnel in diagnostic activities of patients. Given the increasing importance of quality performance indicators in current health policy, the World Health Organization (WHO) emphasize all countries establish various assessments and metrics to measure that performance. In addition, the impact of the existence of healthcare quality key performance indicators (KPI) is proven by studies worldwide. In Malaysian government hospital, the KPI aims to measure and monitor the achievement of service quality in government hospitals. This is achieved by the establishment of Hospital Performance Indicator for Accountability (HPIA). Ever since the HPIA was launched in 2014 there are now 38 indicators of HPIA and 239 indicators for Clinical Medical Program which covers all aspects including Community Environmental Support, Technical, Internal Business Process, Learning and Growth, Employee Satisfaction, Financial, Customer Focus, and Office Management.

Despite the recent advancement of IoT in healthcare, there is an alarming concern on the security and privacy aspect of the health data shared through these IoT devices. This also caused a healthcare data at risk, which means immediate action should be taken to ensure patients data are not being jeopardized while medical practitioners can still leverage on the IoT solutions in assisting their daily operations. For this reason, this paper examines the IoT security, privacy and risk factors in the healthcare sector and the practitioners in order to provide a secured Healthcare IoT environment with compliance to the existing quality performance indicators. Hence, comparative studies are conducted to analyses the related works together with a case study of a Malaysian government hospital that implements the IoT solution. Following this, the study will develop an IoT Security Risk Management for healthcare practitioner as a base principle for the safe use of IoT solution in a healthcare environment.

IOT HEALTHCARE COMPONENTS AND ITS RISKS

CHAPTER 2

IOT HEALTHCARE COMPONENTS AND ITS RISKS

As many healthcare enabled technologies are developed based on IoT, innovations in healthcare are becoming more versatile and reasonable in cost. This includes identification technology, communication and location technologies, sensing technologies and service-oriented architecture . One of the examples of healthcare IoT implementation is the OpenAPS, the open source solution for the open artificial pancreas system to help diabetes sufferers whereby it provides continuous glucose monitoring (CGM). A wireless system sensor sends glucose data to the smart transmitter that is worn on the upper arm over the sensor insertion site then the data and alerts are sent simultaneously to the smartphone to help identify patterns and provide necessary information. Another study by also highlights the used of IoT during cancer treatment whereby patients will wear the tracker for a week prior to treatment and continued for certain period over the course of multiple treatments.

Apart from assisting diagnosis, IoT healthcare devices are also developed to ensure health treatment adherence. By connecting the devices to the mobile apps, it will allow the patients to get reminders for self-adherence monitoring. In addition, Doukas and Maglogiannis stated that inhalers for chronic obstructive pulmonary disease (COPD) that are connected to the digital platform via a sensor can passively record and transmit the required data. Hence, this will allow patients, families and physicians to monitor the medication ingestion and adherence pattern in real time.

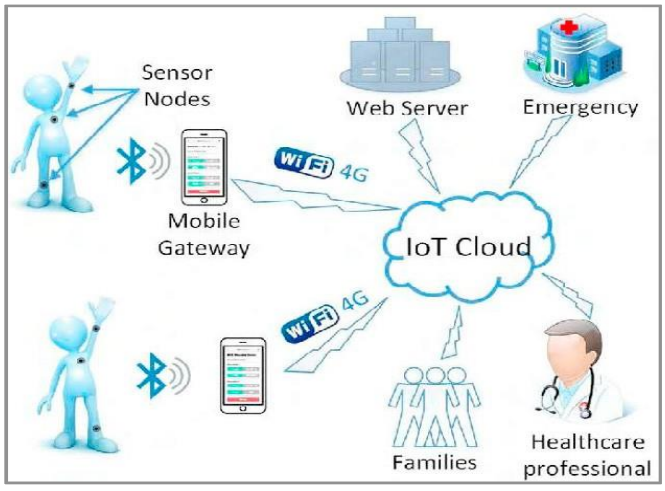

Fig 2.1 Wireless sensor network with IoT connected healthcare platform

Fig. 2.1 describes how IoT can be implemented on the healthcare platform by using Wireless Sensor Network. The diagram illustrates how IoT Cloud is functioning as a platform in integrating all parties, which are the patient itself equipped with all sensor nodes, healthcare professional, the patient families, and the emergency department. The dependence of healthcare on IoT is generally to improve access to care, increase the quality of the care and reduce the cost of care. Despite the rise of many healthcare applications based on IoT, the excitement around these applications far outdoes the reality. Furthermore, there is a risk that excessive leveraging on IoT technologies will disassociate caregivers from patients, potentially causing in a loss of caring. In more specific, resource constraints that have to reduce IoT capabilities are often comprised of limited computation performances, energy supply and memory capacity. These limitations made applicability onto the conventional security solutions are less feasible. Following subsections will discuss IoT components and their potential risk.

2.1 Radio Frequency Identification (RFID) and Wireless Sensor Network (WSN)

There are varieties of IoT applications in the healthcare domain based on **Radio Frequency Identification (RFID)**. For example, it serves the authentication process, blood transfusion medicine, medication safety and patient tracking. In user authentication, besides identifying and validation of staff, the healthcare sector has incorporated RFID functionality in medical assets tracking and validation, patients where-about, newborns identification, medical treatments tracking, procedure management in the wellness center, and surgical process management.

There is a concern about location privacy and scalability when applying IoT in healthcare. Jing, Vasilakos, Wan, Lu and Qiu emphasize that in safeguarding healthcare data integrity, the tag nor the reader can be forged or impersonated. If tampering, then the forgeability will be a hindrance in the successful adoption of IoT. In addition, as discussed by the RFID must be able to protect patients' data that contain patients' treatments and location for privacy protection. Despite its potential advantage in this sector, related applications require sophistication with the purpose of security preservation and data privacy while the cost of maintaining RFID must be affordable; which is yet to be achieved.

Wireless Sensor Network (WSN) also gaining interest as one of the major IoT components. It offers low cost, low power monitoring and successfully reduce devices dependency on wires or cable. Originally WSN was developed for the military application and nowadays it is being widely applied into various solution such as environmental monitoring, smart monitoring, agricultural monitoring and healthcare applications. For example WSN attached to the patient's body will enable medical monitoring, memory enhancement, medical data access, and communication with the healthcare provider in an emergency via SMS or GPRS. The monitoring process can be continuously done using a wearable, clothing-embedded transducers and implantable sensor networks. This will assist in the detection of patients' emergency condition along with the growth in a wireless sensor network.

However, the lack of available bandwidth is the main concern whereby the IoT for health monitoring may not be feasible and the accuracy of data transmission from patients to healthcare providers is hard to achieve. Packet losses during data transmission through wireless is also critical for IoT in healthcare. Apart from data losses, sensors that capture patients' health conditions and transmit to the clinicians via hospital servers are vulnerable to message hijacked and modifications. Hence, healthcare providers get the falsified information that contributes to a disastrous treatment plan and jeopardize the patients' lives.

2.2 IOT Middleware and Cloud Computing

Middleware in IoT is a key technology as an intermediary between IoT devices and its applications. According to Billure, Tayur and Mahesh, this layer of IoT is crucial as its interoperability between new and existing legacy infrastructure. Different middleware approach is targeted to fulfil functionalities such as efficient software installation and data aggregation. However, as indicated by Yang, Li, Geng and Zhang, there are also risks faced in the IoT middleware layer such as hardware resources; where sensor nodes must accomplish three (3) basic operations which are sensing, data processing and communication. Thus, it must able to deliver a mechanism to manage the processor and memory use efficiently while maintaining a lower power communication. Additionally, this layer must capable to perform failure reporting and run automatic corrective measure or take alternative actions to maintain network operations until the failure is fixed.

Cloud computing in healthcare institutions requires more than just easy access to electronic medical records (EMR), but also claims, medications, laboratory data and overall hospital management systems including billing. However, Chauhan and Kumar prove that to have a useful cloud computing application, the institutions must ensure data is feed properly, in a complete manner and timely. Thus, in a hospital that relies mainly on paper-based and manual charting and it will be a painful approach to take. Additionally, devices such as smartphones and tablet PCs that primarily must be used in assisting medical staffs and patients might be a challenge to the financial constraint to mass- acquire of equipment. Besides the financial resources constraint, non-acceptance of technology by doctors and consultants, unawareness among healthcare community in the institution and lack of proper supporting IT infrastructure become contributing factors of failure or slowness in adopting cloud computing approach in the healthcare sector.

IOT APPLICATIONS AND RISK MANAGEMENT

CHAPTER 3

IOT APPLICATIONS AND RISK MANAGEMENT

3.1 IOT Applications

Along with the growth of IoT applications, however, there exist technological problems; taking instances like electromagnetic radiation effect and signal strength problem in the hospital. With the vast implementation of IoT in healthcare institution like a hospital, loss of privacy can be a part undesirable effect; as certain private information must remain confidential. The challenge is assuring privacy while providing high-quality care based on data generated through lists of IoT devices. Apart the loss of trust in data transmission; that data might be 'hijacked' and modified during data transmission, nurses must be able to balance between optimizing technologies for better factual assessment, surveillance and treatment while maintaining contact with the patient. In summary, IoT risk factors in the healthcare environment can be divided into six categories as depicted in the following table.

IOT Risk Category	IOT Risk Factor
Data and Application	• Manual data feed
User and Change Management	• Loss of caring for patient caregivers • Non-acceptance of technology medical practitioner • Unawareness of IoT among the healthcare community in the institution
Security and Privacy	• Loss of data privacy • Hijacked and modified data • Location privacy • Genuine authentication on medical/clinical procedure • The attack on Server Security
Infrastructure	• Slow Middleware performance

	• Slow Sensor performance • Slow data processing • Lack of proper supporting IT infrastructure
Network and Physical Environment	• Lack of bandwidth • Packet loss • Intermittent communication
Financial	• Financial constraint • 3rd party suppliers and vendors

Table 3.1 IoT risk factors in the healthcare environment

3.2 COBIT5 Framework for IoT Risk Management

As the IoT adoption continue to grow, there are also number of IoT related reference architecture, frameworks, guidelines, platforms and standards being developed by researchers. This study will explain the relevancy of choosing **Control Objectives for Information and related Technology (COBIT 5)** to aid the formulation of the risk management model for healthcare IoT proposed by Latifi and Zarrabi. By using COBIT 5, a safe monitoring system can be created for machine tools using IoT devices. COBIT5 provides best practices in the area of risk perspective, risk components, using risk scenarios for Governance of Enterprise IT (GEIT) as well as its relationship with other standards. Basically, this framework covers most of the important elements in the organization as well as IoT. It provides insights on how to increase the efficiency and effectiveness in dealing with IoT risks, and at the same time reduce the cost, time and hard work in achieving it. This model also clearly stated the influence elements in managing the IoT risk in an organization. The following figure shows the COBIT5 model discussed.

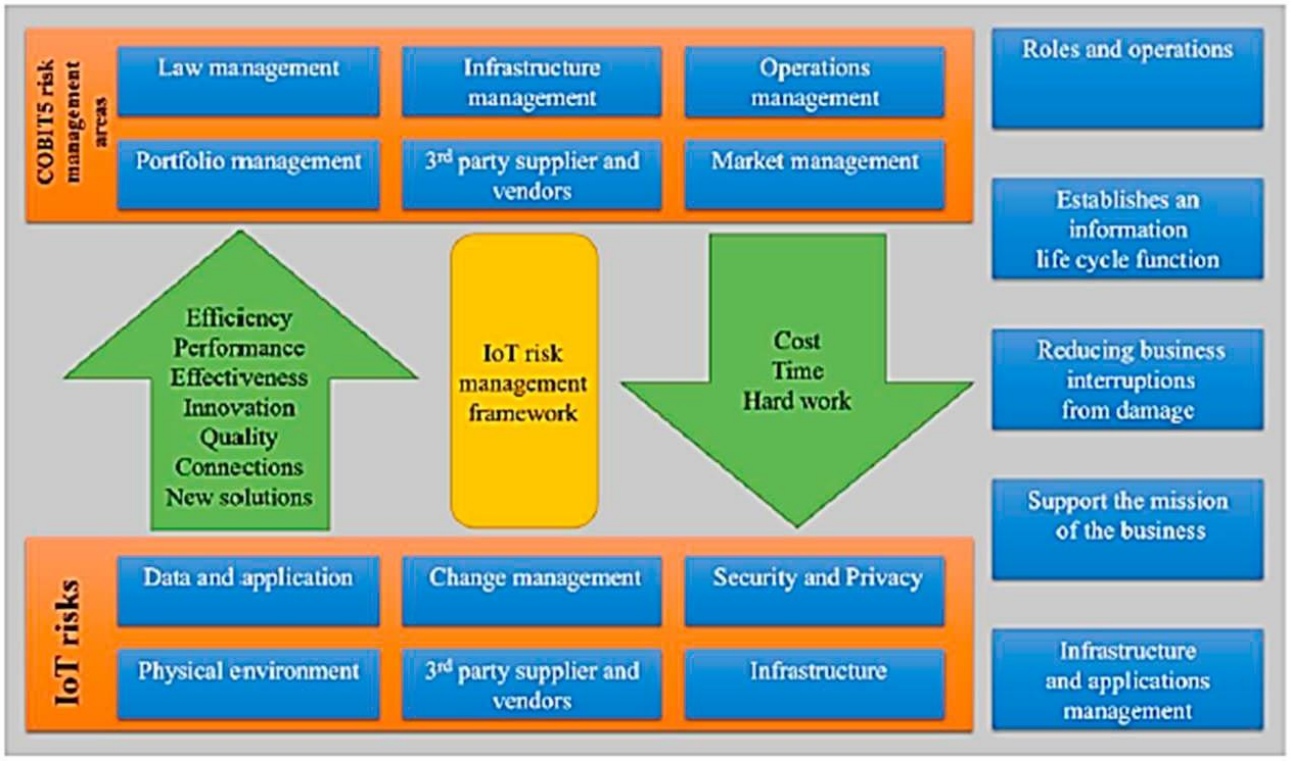

Fig 3.1 The chosen COBIT5 framework for IoT risk management

RESEARCH METHODOLOGY

CHAPTER 4

RESEARCH METHODOLOGY

This study adopted a case study approach by Yin which outlines six processes which are :

1) Plan

2) Design

3) Prepare

4) Collect

5) Analyse

6) Share.

4.1 Planning

The planning stage focuses on identifying the research questions or justification for conducting a case study based on its strengths and limitations. For this study, the aim is to identify the IoT risks in a healthcare environment and to propose an IoT Security Risk Management Model for its Secured Practice. The case study method is justifiable for this study because we do not aim to generalise to populations (the healthcare industry) because every healthcare setting is different in nature, but rather than to generalise to theory, which in this study we propose to utilise on COBIT5 Framework for IoT Risk Management.

4.2 Design

Next is the design stage which aims on describing the unit of analysis, classifying the underlying issues of the anticipated study and developing procedures to maintain case study quality. Hospital Kuala Lumpur (HKL) is selected as a case study as it the Malaysia largest government hospital and a benchmark hospital for many pilot implementation projects ranging from medical health until technological infrastructure. HKL consists of 53 different departments; including the clinical departments and clinical support services, pharmaceutical department, training and research. The hospital maintains its standards of service delivery by adhering to the Hospital Performance Indicator for Accountability (HPIA). The HPIA

indicators consist of internal business process, customer focus, employee satisfaction, learning and growth, financial and office management and environmental support.

4.3 Prepare

Later is the prepare stage which aims on developing skills as a case study investigator, developing a case study protocol, conducting a pilot case, and gaining any relevant approvals. Our team consist of experienced researchers who are familiar with the case study approach and a case study protocol was designed to ensure the study reliability. Since one of our researchers previously worked in HKL and the study scope only on the technology aspect without involving any medical or patient data, we manage to get the study approval without further dispute.

4.4 Collect

Next is the collect stage which involves the execution of case study protocol, using multiple sources of evidence, forming a case study database, and maintaining a chain of evidence. For our case study, we have conducted series of the interview (semi-structured) with the IT Officers and healthcare practitioners of HKL to get the overview of HKL operations and also the current state of their IoT implementation. The aim is to better understand the current scenario of IoT implementation and what are the associated risks.

4.5 Analyse

Next is the analyse stage that relies on theoretical propositions and other strategies, in order to explore rival explanations, and interpretations of the findings. This study is an enhancement of theoretical propositions by COBIT5 Framework for IoT Risk Management and HPIA strategies. Hence, explanation building analysis is applied because of it is able to analyse the case study data by constructing an explanation about the case and explain how and why things happened about the IoT risk in the healthcare setting. The interview transcript is then coded according to those two theoretical propositions.

4.6 Sharing

Finally, is the sharing stage whereby the textual and visual materials are composed, enough to display the evidence to reach the conclusion for the study. In this study, the final output is shared by proposing a Model of IoT Security Risk Management for Healthcare Practice whereby the COBIT5 Framework for IoT Risk Management and HPIA strategies are included plus the phases on how to achieve it. Ideally, this study suggests seven iterative phases that must be in placed in order to create a secured IoT practice in a healthcare environment.

FORMULATION OF IOT SECURITY MODEL

CHAPTER 5

FORMULATION OF IOT SECURITY RISK MANAGEMENT MODEL FOR HEALTHCARE PRACTICE

Healthcare IoT solution is not yet robust but continues to develop. Therefore, it is difficult to identify and predict all possible risks, vulnerabilities and threats associated with the IoT healthcare domain. Nonetheless, for the security preparedness action, there is a necessity to develop a risk management model prior to any security disaster happened. This study adopted the Control Objectives for Information and related Technology (COBIT5) due to its ability to synergize with another standard in a seamless way. COBIT5 focus on the enterprise level and the solution is not just limited to the IT domain. Hence, its suits HKL case very well with its organizational complexity in nature. The model consists of three parts, which are Healthcare IoT Risk Management, HPIA alignment and COBIT5 implementation phases. The following figure shows the proposed model as described.

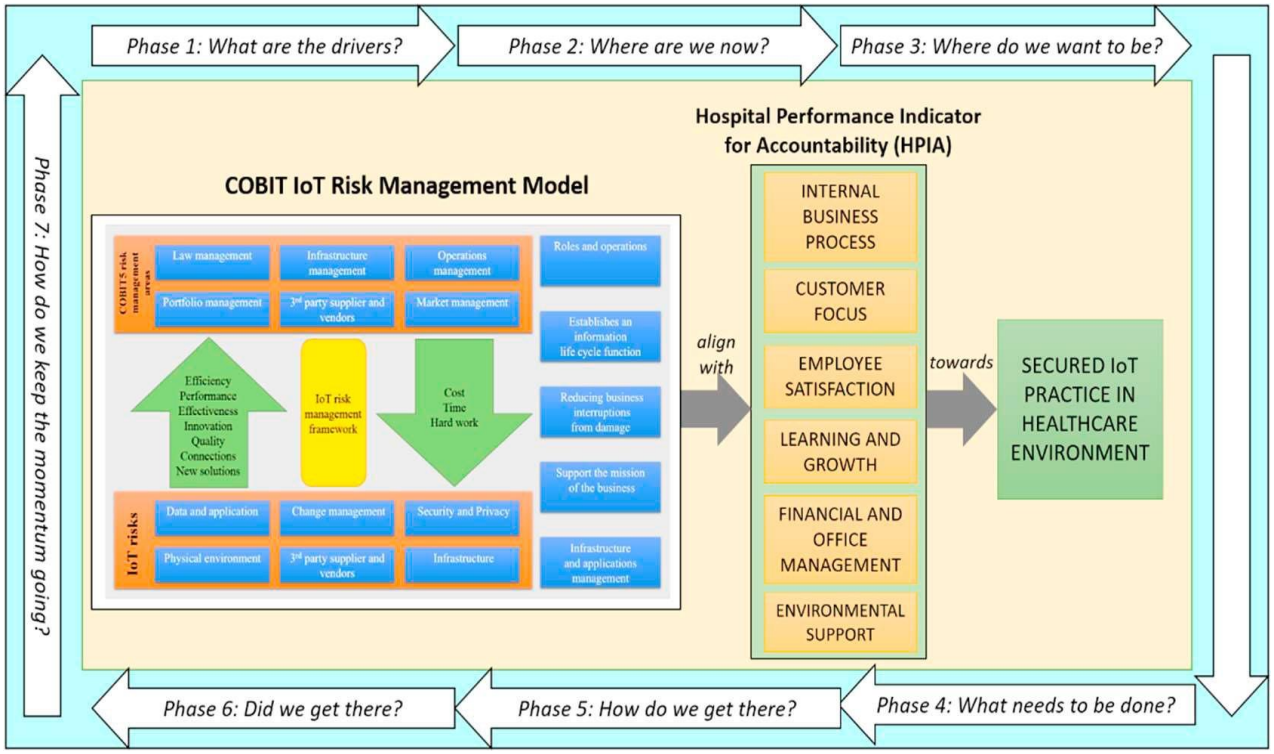

Fig. 5.1 Proposed model of IoT security risk management for healthcare practice.

5.1 COBIT IoT Risk Management

The first part of the model is the COBIT IoT Risk Management which is formulated based on the IoT risk category such as 1) data and application, 2) user change management, 3) security and privacy, 4) physical environment, 5) 3rd party supplier and vendor, and 6) infrastructure. The other part is COBIT 5 management areas which consist of 1) law management, 2) infrastructure management, 3) operation management, 4) portfolio management, 5) 3rd party suppliers and vendor, and 6) market management. For this case study, we found out that all infrastructures pertain to medical technology such as an analyzer, heart rate machine, x-ray and scanner machines are maintained and monitored by each department authority themselves which may be resulted varies risk issue once IoT is implemented widely. The main reason is no centralised IoT security and risk control mechanism. Therefore, by having this model, we are proposing to reduce the risk because everything associated with IoT solution now can be centrally monitored. This will lead to better efficiency, performance, effectiveness, innovation, connection quality, and portrays a new solution idea. This also will eventually reduce the cost, time and operational tasks. Other supporting elements in this model are, the establishment of clear roles and operations, establishment information life cycle function, reduction of business process interruption, support for the business mission and management of infrastructure and application management. In overall, the findings from the case study agree that the criteria from this model are relevant to the healthcare context as well. For example, data and application are the major risks in healthcare when it involves IoT. Therefore, to manage this risk, law management needs to be in place.

5.2 HPIA

The model then incorporates the HPIA categories which are Internal business process, Customer focus, Employee Satisfaction, Learning and growth, Financial and Office Management and finally Environmental Support. This is in line with the healthcare quality KPI as explained by the case study participants HPIA is mandatory rules to be followed. From the interviews, it is found out that the IoT adoption is currently in the infancy stage. Their current risk management practice relies on staffs' daily monitoring activities by own Head of Department while IT-related security risks are monitored by the IT Department.

5.3 Implementation Phases

The model then proposes seven phases of implementation originated from COBIT5 to guide the implementation process of IoT from the beginning. The phases are :

- **Phase 1: What are the drivers?** –which aim to identify and confirm on the need for IoT implementation.
- **Phase 2: Where are we now?** –where it need to define the scope of the implementation using COBIT's mapping of enterprise goals to IT- related goals.
- **Phase 3: Where do we want to be?** –means that once an improvement target is set, it should be followed by more detailed analysis using COBIT's guidance to identify gaps and potential solutions.
- **Phase 4: What needs to be done?** –Refers to practical solution in defining projects supported by justifiable business case.
- **Phase 5: How do we get there?** –refers to proposed solutions that need to be implemented in day-to-day practices in this phase.
- **Phase 6: Did we get there?** –refers to how the sustainable operation of the new or improved enablers are conducted.
- **Phase 7: How do we keep the momentum going?** -In this phase, the entire success of the IoT implementation is reviewed with the need for continual improvement is reinforced.

CONCLUSION

CONCLUSION

The objective of healthcare IoT which are to increase access to care, upsurge the quality of the care and yet reduce the cost of care. This is attainable with the successful and secured implementation of IoT Security Risk Management Model for Healthcare Practice. COBIT 5 shall provide a standard accepted principles, practices, tools and models to help increase the trust and value from all healthcare practitioners. In ensuring the effectiveness of the adoption, the willingness of the enterprise's management team in IoT technology is crucial. The higher IoT adoption level by doctors and consultants, awareness among healthcare community in the institution and proper supporting IT infrastructure become contributing factors of successful or swift and smooth adoption in cloud computing for the healthcare sector. For future work, this model will be evaluated by the IoT experts in on the relevancy of the proposed components as well as the feasibility and usability evaluation which will be conducted by the healthcare practitioners.

REFERENCES

REFERENCES

[1] Patel, K.K., and S.M. Patel. (2016) "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges." *Int J Eng Sci Comput* **6**.

[2] Bevan, G., A. Evans A, and S. Nuti. (2019) "Reputations Count: Why Benchmarking Performance is Improving Health Care Across the World." *Health Economics, Policy and Law* **14**: 141-61.

[3] Cheon, O., M. Song, A.M. Mccrea, and K.J. Meier. (2019) "Health Care in America: The Relationship Between Subjective and Objective Assessments of Hospitals." *International Public Management Journal*. pp. 1-27.

[4] HKL. (2016) "Hospital Kuala Lumpur: Hospital Performance Indicator For Accountability (HPIA)." in *Lumpur HK*, (ed.)

[5] Yuehong, Y., Y. Zeng, X. Chen, and Y. Fan. (2016) "The Internet of Things in Healthcare: An Overview." *Journal of Industrial Information Integration* **1**: 3-13.

[6] Chakrabarty, A., S. Zavitsanou, T. Sowrirajan, F.J. Doyle III, and E. Dassau. (2019) "Getting IoT-ready: The Face of Next Generation Artificial Pancreas Systems." *The Artificial Pancreas*. pp. 29-57.

[7] West, D.M. (2016) "How 5G Technology Enables the Health Internet of Things." *Brookings Center for Technology Innovation* **3**: 1-20.

[8] Swan, M. (2012) "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0". *Journal of Sensor and Actuator Networks* **1**: 217-53.

[9] Rohokale V.M., Prasad N.R., and Prasad R. (2011) "A Cooperative Internet of Things (IoT) for Rural Healthcare Monitoring and Control", in *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*, IEEE. pp. 1-6.

[10] Islam, S.R., D. Kwak, M.H. Kabir, M. Hossain, and K-S. Kwak. (2015) "The Internet of Things for Health Care: A Comprehensive Survey." *IEEE Access* **3**: 678-708