IoT MICROSOFT ACCESS BASED DATABASE MANAGEMENT SYSTEM FOR HEALTHCARE AND CLINICAL SETTINGS

SULTAN MAHMUD

FACULTY OF ENGINEERING
UNIVERSITY OF MALAYA
KUALA LUMPUR

2018

IoT MICROSOFT ACCESS BASED DATABASE MANAGEMENT SYSTEM FOR HEALTHCARE AND CLINICAL SETTINGS

SULTAN MAHMUD

RESEARCH REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF ENGINEERING (BIOMEDICAL)

DEAPARTMENT OF BIOMEDICAL ENGINEERING
FACULTY OF ENGINEERING
UNIVERSITY OF MALAYA
KUALA LUMPUR

2018

UNIVERSITY OF MALAYA
ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: **SULTAN MAHMUD**

Matric No: **KGL150008**

Name of Degree: **MASTER OF ENGINEERING (BIOMEDICAL)**

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"):

IoT MICROSOFT ACCESS BASED DATABASE MANAGEMENT SYSTEM FOR HEALTHCARE AND CLINICAL ENVIRONMENT SETTINGS.

Field of Study: **IoT IN HEALTHCARE**

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This Work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge, nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every right in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date:

Subscribed and solemnly declared before,

Witness's Signature Date:

Name:
Designation:

IoT MICROSOFT ACCESS BASED DATABASE MANAGEMENT SYSTEM FOR HEALTHCARE AND CLINICAL ENVIRONMENT SETTINGS

ABSTRACT

The "things" in Internet of Thing can refer to a wide variety of devices – implants, sensors, automobiles, etc. The IoT has a variety of application domains, including health care and clinical environment. The expended sensing and communicational capabilities of these "things" is a harbinger of new business possibilities in the hospital and different health care organizations. The IoT revolution is remodeling recent health care with promising technological, social, and economical prospects. This project advances in IoT-based health care technologies using Microsoft access and reviews the state-of-the-art platforms, applications, and industrial trends in health care solutions. In addition, it analyzed distinct IoT security and privacy features, including security requirements, threat models from the health care perspective and proposes a collaborative security model to minimize security risk. It also discussed how different innovations such as big data, application of access based healthcare platform and artificial intelligence can be leveraged in a health care technology context. Additionally, it addressed different IoT and eHealth regulations and policies to decide how they can facilitate societies and economies in terms of sustainable improvement. Hence, this research involved in organization and collection of sensitive health related data from clinical environments, built health database on Microsoft access, stored and retrieval of data from the cloud for easy access and interpretation of those data whenever required. The results from the interpretations can be used to analyze data to make concise decisions about the patient conditions. After the data storage had built from different sources like hospital and clinics on the access database, payer data, patient responses, consumer health data has been integrated into a unified data structure, the IoT would

show the results of the various health status based on the data input related to the different physical and mental conditions and other associated parameters. Followed by implementation of artificial intelligence, which yield meaningful insights to make predictive recommendations about the patient health conditions, suggest possible treatment plan based on what happened in those other related situations to improve overall patient's experiences and excel health care environments.

Keywords: Internet of Things, Microsoft Access, Healthcare Management, Business Model, Security and risk

INTERNET DARIPADA MICROSOFT ACCESS BASED SYSTEM MANAGEMENT SYSTEM UNTUK PENETAPAN KESIHATAN DAN KLINIKAL PERLINDUNGAN KLINIK

ABSTRAK

"Perkara" dalam Internet of Thing boleh merujuk kepada pelbagai jenis peranti - implan, sensor, kereta, dll. IoT mempunyai pelbagai domain aplikasi, termasuk penjagaan kesihatan dan persekitaran klinikal. Kemampuan mengesan dan berkomunikasi yang dibelanjakan bagi "perkara-perkara" ini adalah perihal kemungkinan perniagaan baru di hospital dan organisasi penjagaan kesihatan yang berbeza. Revolusi IoT adalah pembentukan semula penjagaan kesihatan baru-baru ini dengan prospek teknologi, sosial dan ekonomi yang menjanjikan. Projek ini memajukan teknologi penjagaan kesihatan berasaskan IOT yang menggunakan akses Microsoft dan mengkaji platform, aplikasi, dan trend industri terkini dalam penyelesaian penjagaan kesihatan. Di samping itu, ia menganalisis ciri keselamatan dan privasi IOT yang berbeza, termasuk keperluan keselamatan, model ancaman dari perspektif penjagaan kesihatan dan mencadangkan model keselamatan kolaboratif untuk meminimumkan risiko keselamatan. Ia juga membincangkan bagaimana inovasi yang berbeza seperti data besar, penggunaan platform penjagaan kesihatan berasaskan akses dan kecerdasan buatan boleh dimanfaatkan dalam konteks teknologi penjagaan kesihatan. Di samping itu, ia menangani pelbagai peraturan dan dasar IOT dan eHealth untuk menentukan bagaimana mereka dapat memudahkan masyarakat dan ekonomi dari segi peningkatan yang berterusan. Oleh itu, penyelidikan ini melibatkan organisasi dan pengumpulan data berkaitan kesihatan sensitif dari persekitaran klinikal, pangkalan data kesihatan yang dibina di atas akses Microsoft, menyimpan dan mendapatkan semula data dari awan

untuk memudahkan akses dan tafsiran data tersebut apabila diperlukan. Hasil dari tafsiran boleh digunakan untuk menganalisis data untuk membuat keputusan ringkas mengenai keadaan pesakit. Selepas penyimpanan data dibina dari sumber yang berbeza seperti hospital dan klinik di pangkalan data akses, data pembayar, respons pesakit, data kesihatan pengguna telah disatukan ke dalam struktur data bersatu, IOT akan menunjukkan keputusan pelbagai status kesihatan berdasarkan input data yang berkaitan dengan keadaan fizikal dan mental yang berbeza dan parameter berkaitan lain. Diikuti dengan pelaksanaan kecerdasan buatan, yang menghasilkan pandangan yang bermakna untuk membuat cadangan ramalan tentang keadaan kesihatan pesakit, mencadangkan pelan rawatan yang mungkin berdasarkan apa yang berlaku dalam situasi berkaitan yang lain untuk meningkatkan pengalaman pesakit keseluruhan dan cemerlang dalam persekitaran penjagaan kesihatan.

Kata kunci: Internet Perkara, akses microsoft, Pengurusan Kesihatan, Model Perniagaan, Keselamatan dan Risiko

AKNOWLEDGEMENT

First and foremost, Al-Hamdulillah, all praise to Allah SWT who granted me the health, strength and patience to overwhelm all sorts of difficulties and accomplish this academic achievement.

I would like to express my gratitude to my supervisor, Associate Professor Ir. Dr. Lai Khin Wee for his excellent directions, encouragement, support, suggestions, guidance and motivated me to work harder and achieve this success.

Most of all, I would like to thank my beloved wife Aishath Nadhiya for her encouragement and endless support. I would also like to thanks to staffs of biomedical engineering department for their ultimate support and guidance.

A very special thanks to my dear friends Abdur Rahman, Murad, Asyiqin, Gowri and Farisya without their support thesis would not be accomplished. I would like to thank Abdullah brother and Robin for their support and help. I would like to show appreciation to my all course mate for sharing their knowledge. Lastly, I am deeply indebted to my parents, thank you for the countless times of prayer and encouragement. I would like to thank my sister and brother in law and relatives for their support during the difficult times. To all those who supported me in any aspect to the completion of my research- thank you.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS & ABREVIATIONS

ADA: Active Digital Artefacts

APHM: Association of Private Hospitals

BMO: Business Model Ontology

CPS: Cyber-Physical System

DBMS: Database Management System

EHR: Electronic Health Record

EIS: Enterprise Information System

GLC: Government-linked corporations

HIS: Hospital Information System

Health-IoT : Internet of Things solution for healthcare

ICT: Information and Communication Technologies

IHH: In-Home Healthcare

IoT: Internet-of-Things

ITGC: Information Technology General Controls

KPJ: Kumpulan Pelaburan Johor

LAN: Local Area Network

LoRa: Long range wide area networks

LPWA: Low-power Wide-Area Networks

MAC: Message Authentication Codes

MMA: Malaysian Medical Association

MS Access: Microsoft Access

M2M: Machine-to-machine

NFC: Near Field Communication

ODBC: Open Database Connectivity

PHCFSA: Private Health Care Facilities and Services Act

RFID: Radio-Frequency Identification

SAN: Sensor Area Network

SaaS: Software as a Service

SQL: Structured Query Language

UML: Unified Modeling Language

WAN: Wide Area Network

WSN: Wireless Sensor Network

CHAPTER 1: INTRODUCTION

1.1 Research background

The word "Internet of Things" (IoT) was invented at the early 21st century by the MIT Auto-ID Center with special mention to British technology pioneer Kevin Ashton (Ashton 2009) and David L. Brock (Brock 2001). As a complex cyber-physical system, the IoT Many relevant concepts have been introduced to describe the future healthcare powered by emerging information and communication technologies, such as mobile healthcare (mHealth), pervasive healthcare (pHealth), ubiquitous healthcare (uHealth), electrical healthcare (eHealth), telehealth, teleradiology, telemedicine, etc. (Pawar *et al.* 2012). In this project, we don't aim to distinguish them pedantically and these impressions are looked as another expressions of the Health-IoT. Furthermore, without special state, the Health-IoT more unambiguously refers to the in-home healthcare application of IoT.

Around Internet of Things (IoT) is a concept where smart and exclusively identifiable machines are connected to the internet providing the potential to enhance current business processes and even create completely new way to operate. Most research on the IoT has been focused on the technological aspects of IoT and during the last years more research has been made to analyze different aspects of IoT. Whitmore, Agarwal and Xu (2015) studied the literature on the IoT and found 127 relevant papers consisting from journal articles, conference papers and edited volumes and noted that due to the dynamic state of development of IoT majority of papers focused on the engineering and computer science domains of the IoT paradigm with less attention on the managerial, economical, and social aspects of IoT.

The term The Internet of Things (IoT) is frequently used to name a set of things that are directly coupled to the Internet using the Internet Protocol (IP) stack. That is the key

difference of wireless sensor networks (WSN) of earlier generation where nodes were organized in a local network area (LAN) with distinct protocols like WirelessHART or ZigBee. The IoT opens the opportunity for global data analysis by connecting the objects to the global network. Home automation (e.g. smart home), personal health monitoring (e.g. measurements of temperature, pulse or heart rate), industrial automation (e.g. control of the electrical grids), building automation (e.g. electrical and ventilation systems of the building, control heating), and smart cities are the usual applications for the IoT.

Typically, a Health-IoT solution includes the following functions:

1. Tracking and monitoring

   Powered by the ubiquitous identification, sensing, and communication capacity, all the objects like equipment, people, medicine, etc. can be monitored and tracked on a 24/7 basis by wearable WSN devices (Alemdar *et al.* 2010).

2. Remote service.

   Healthcare technology and assist living facilities can be delivered remotely through the internet and field devices e.g. emergency detection and first aid, telemedicine and remote diagnosis, health social networking, dietary and medication management, stroke habitation and training, etc.(Plaza et al. 2011, Klasnja and Pratt 2012, Ludwig et al. 2012).

3. Information management.

   All the healthcare information (Diagnosis, medication, recovery, therapy, finance, logistics, management and even daily activity) enabled by the global connectivity of the IoT can be utilized throughout the entire value chain, collected and managed (Domingo 2012).

4. Cross-organization integration.

The hospital information systems (HISs) are prolonged to patients home and can be integrated into greater scale healthcare system that may cover a rural area, town, city or even state (Serbanati et al. 2011, Yin et al. 2009, and Liu et al. 2008).

1.2 Research objectives

The aim for this research is to implement the Internet of Things in the healthcare environment based on Microsoft access database platform to ensure:

a) To have better insights into the patient data, controlling, manipulating and sharing wide range of data remotely from anywhere in the world at any time for easy access by health care and other related professionals.
b) To improve efficiency and workflow for Healthcare, Clinics, Hospitals and other related industries by connecting health care system through the Internet of things based on Microsoft access to perform its function effectively and more conveniently.

CHAPTER 2: LITERATURE REVIEW

2.1 Synopsis

My review of the existing literature is concentrated on four central topics: Internet of Things (IoT), Microsoft access, Business models and health care system in Malaysia.

The internet of things discusses the essential technologies for IoT. This is followed by a definition that contains some key components a system should possess to label it as IoT. An IoT application that fits the definition connects heterogeneous objects that are embedded with intelligence. This allows the autonomous interaction of these objects. The created data is integrated and analyzed by a cloud structure. During this entire process, the focus is on automation. Then some related concepts are compared with IoT: smart devices, machine-to-machine communication and cyber-physical systems a wireless sensor network. An illustration of a future IoT application is given at the end of this section.

Microsoft Access is an information management tool that helps to store information for reference, reporting, and analysis. Microsoft Access helps to analyze large amounts

of data or information and manage related data more efficiently than Microsoft Excel or other spreadsheet applications. Hence the platform used for this project is based on the Microsoft access 2007 version which will be describe later on.

A section on business models is included since this concept is an important topic when introducing new technologies. To describe a company's business model the nine building blocks of the Business Model Ontology by Osterwalder, Pigneur, & Tucci (2005) are used as a framework. This segment starts with an explanation of this framework, followed by the reasoning why this one is chosen. Next, the use of business models for IoT is outlined, based on the current (limited) literature on this topic. Three perspectives are discussed. The business models of companies that will create IoT systems or implement IoT in other companies, the transformation of current business models by the impact of IoT and the creation of completely new business models. To finish this section, three current challenges for IoT are identified: finding the right business model, regulatory restrictions of the government and interoperability of smart objects.

The healthcare section starts with an overview of the health system in Malaysia. Subsequently, some opportunities for IoT in healthcare are described, based on current problems and recent trends in this sector. The lack of business model innovation and the possibility of IoT as a technological enabler to disrupt this sector (Christensen, C. M., Grossman, J. H., & Hwang, 2009) are discussed as a final part of this chapter.

2.2 IoT

2.2.1 The definition and development of IoT

The amount of devices that are connected to the internet is growing and will continue to grow tremendously in the near future. End-users have started to use multiple other devices, in addition to mobile phones, such as iPads, digital TVs, Kindles etc. New

types of devices, that can communicate and offer services via the internet, are being developed. And these devices allow the machines to be connected to each other. (Höller et al 2014: 4).

According to Porter & Heppelmann (2014: 4) the term “Internet of Things” has come about to reflect the increasing number of smart and connected products and underline the new opportunities they can bring. What makes smart and connected products different is not just the internet but the changing nature of them. It is their expanded capabilities and the data they can generate.

The semantic origin of IoT is comprised of two words and two concepts: “Internet” and “Thing”. Internet is defined as “the world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP)”. Thing means “an object not precisely identifiable”. Semantically, IoT means “a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols”. (INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems in co-operation with the Working Group RFID of the ETP EPOSS 2008).

There has been discussion about the idea of IoT already from 1991 when Mark Weiser wrote about the Computer for the 21st Century. In his article he explains how the computer-readable data will be brought to the physical world and machines will be connected to a ubiquitous network. At that time the ubiquitous computing was more local whereas the IoT today is a broader concept.

The phrase “Internet of Things” probably started life in 1999 when it was introduced first by Kevin Ashton of Auto-ID Center. Ashton explained how RFID (Radio Frequency Identification) and sensor technologies make it possible for computers to understand, identify and observe the world, and he suggested that we should empower

the computers to gather information on their own without any restrictions of human-entered data. Then we could count and track everything, reduce cost, loss and waste, and we could know if things needed repairing, replacing or recalling (Ashton 2009). Ashton, who foresaw that RFID would lead to total automation of collecting data, was also quoted in the Forbes Magazine in 2002. He said that "We need an internet forthings, a standardized way for computers to understand the real world" and that might have been the first documented use of the term IoT in literal (Mattern & Floerkemeier 2010: 242-243, Schoenberger 2002).

The IoT represents a vision where the internet stretches to the real world comprising every-day objects and physical items that are connected to the virtual world. The items can physically act as access points to internet services and they can be controlled and monitored remotely (Mattern & Floerkemeier 2010: 242). The internet will no longer be just about people, media and content. It will include all real-world assets creating knowledge, exchanging information, interacting with people and supporting business processes. IoT is not a new internet; it can be seen as an extension to the existing internet. (Höller et al 2014: 14)

The IoT vision is based on the belief that the advances in information technology, communications and microelectronics will continue also in the foreseeable future. Because of the diminishing size, decreasing energy consumption and constantly lowering price communication modules, processors and other electronic components can be integrated into our daily objects already today. Embedded information and communication technology could revolutionize the use of the objects, and that is why smart objects are in an important role in this IoT vision. With sensors they can picture their context and with built-in networking systems they could access internet services, communicate with each other and interact with people. (Mattern & Floerkemeier 2010: 242-243).

The most essential strength of the IoT vision is the substantial impact it will have on many sectors of daily life. Figure 1. represents IoT as a world of connected devices reaching to different sectors of our daily lives. From a private users' perspective, the consequences of IoT introduction will be noticeable in working and domestic fields. Also, from the business users' point of view, the most visible effects will be in fields such as, industrial manufacturing and automation, business and process management, logistics and intelligent transportation of goods and people. (Atzori et al. 2010: 2787).

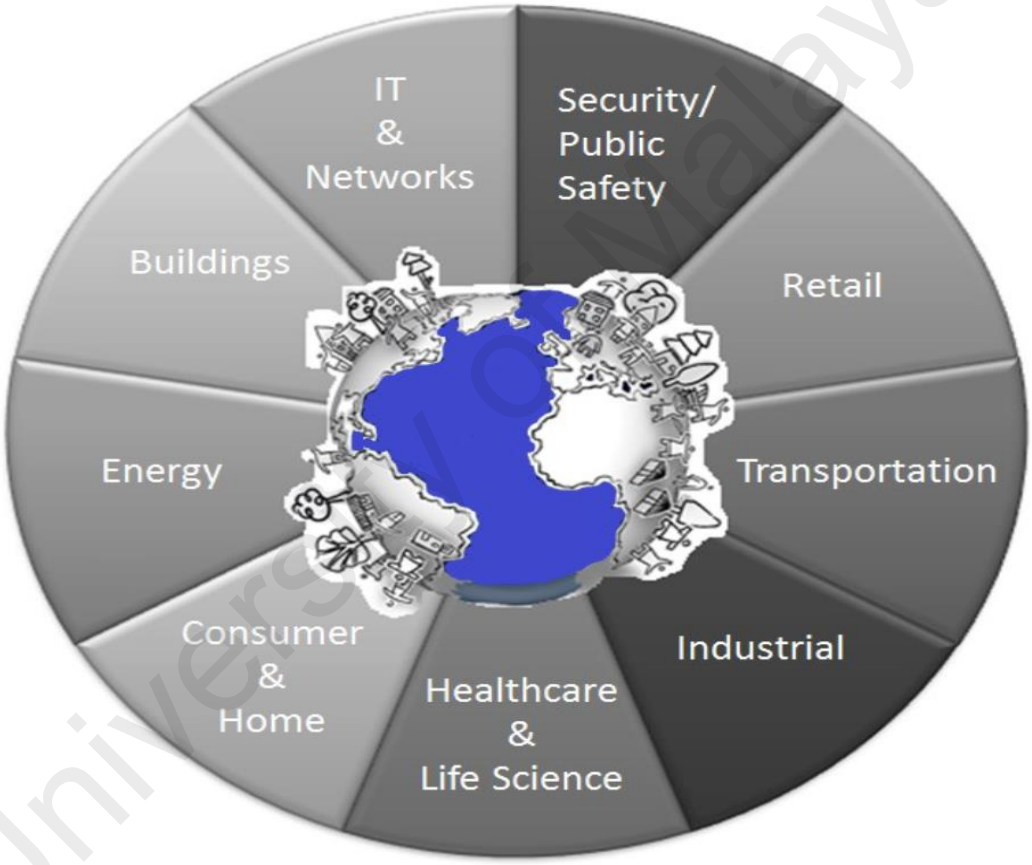


Figure 2. 1: IoT – World of connected devices (adapted from Beecham Research 2011)

The term Internet-of-Things (IoT) is used for a lot of different applications and concepts because there is no strict definition for this term. My personal view on this term is illustrated in the form of a definition to create a common understanding. The following section first includes a basic description of the technologies used for IoT to

get and understanding of how it works. Then the definition is presented, followed by concepts related to IoT and an example of what an IoT application could look like in the near future.

The Internet of Things is the connection of heterogeneous, (everyday) objects embedded with intelligence (e.g. computing capabilities, a unique identifier and communication abilities (Miorandi et al., 2012)) which allows them to interact and exchange data (Cambridge Advanced Learner's Dictionary & Thesaurus, 2017). This interaction and data exchange may be performed by different communication channels and can be direct. However, at some point, the collected data passes through a cloud structure where it's analyzed. This process is autonomous, thus without human intervention. The process runs in the background and doesn't continuously ask for human confirmation. At the end of the process, information can be communicated to the user in more advanced service applications, but the focus should be on minimizing human input.

The Internet-of-Things (IoT) paradigm is becoming key technologies for innovative products and applications. Smart objects can communicate and interact with each other in a defined IoT enabled environment and make autonomous decisions by appropriate correlation and association of data collected from the environment. The envisioned I-IoT system senses the environment and makes decision to sensed environmental changes dynamically and effectively with optimal resources, low cost and increased convenience.

Today even though IoT has generated excitement among the research community but still there are a number of challenges that need to be emphasized. An Intelligent IoT expects to exhibit intelligent behavior by gathering multiple data and information, data management to avoid collusion, sensor fusion for robust decision, and cloud for

information sharing and so on. In IoT, the gathered data needs to be managed with proper order and classification of data is also a vital part. In the field of IoT, a layer-based data management system is presented in. Due to globalization of IoT systems, it needs Cloud service for information sharing. A Cloud service for IoT architecture has been developed for Vehicular Data Cloud Services. Design of a generic scheme for I-IoT systems need to deal with several challenges and it needs to be able to handle the number of things and objects that will be connected in IoT contextual intelligence is

crucial. Another issue is exchanging and analyzing massive amount of data and the vast amount of data also need to be processed, and presented in a seamless, efficient and interpretable form.

2.2.2 Enabling technologies

The first technology for IoT is often mistaken. Smart devices, devices connected to a network or other devices and have the ability to interact (Wikipedia, 2016). For example, a fridge or a television connected to the internet and had an 'upgrade' with applications that basically offer the same possibilities as a web browser but with a better interface for the user. Stating to these devices as IoT is incorrect because those smart devices are only a minor part of this concept. It's even better to use the term smart things or smart objects and not just devices. Based on the definition of Miorandi, Sicari, De Pellegrini, & Chlamtac (2012); anything with the following characteristics can be used for IoT:

- Can perform basic computations
- Uniquely identifiable
- Able to communicate (can be discovered, receive and reply to messages)

The sensing and/or actuation capabilities (Miorandi et al., 2012) are an optional characteristic. There has been made significant progress in the technology of sensors;

over the last couple of years; they are more economical, easy to install and cheaper than ever. In short, the ideal opportunity to make any object or thing smarter. This is one of the top reasons why IoT became such a popular focus in recent years. However, the sensing capabilities are not a necessary characteristic for smart things when using the definition of Miorandi et al. (2012).

Secondly, the technology that will assist the interaction of the smart objects is a combination of mostly wireless networks: Bluetooth, Wi-Fi, Wireless sensor network (WSN), Near Field Communication (NFC), long range wide area networks (LoRa) or low-power wide-area networks (LPWA) etc. (Gubbi, Buyya, Marusic, & Palaniswami, 2013; Openshaw et al., 2014; Schatsky & Trigunait, 2011).

Radio-frequency identification (RFID) is another useful technology for IoT applications. RFID technology permits the design of microchips for wireless data communication and is actually a great enhancement of the traditional barcode system (Gubbi et al., 2013). The RFID reader can read various tags at once, no line-of-sight contact is required and offer writing capabilities next to the reading capabilities (He & Zeadally, 2015). There is no need of battery installation due to the ability of the RFID reader to provide necessary power to communicate the signal from RFID (Gubbi et al., 2013). These tags can store sensitive information since it automatically identifies the objects. However, a lot of research papers found that improving the security of the RFID tags is still an important subject since it requires some extra fine-tuning. Security and Privacy are more challenging in the IoT context because not only users, but also unauthorized objects could access information (Miorandi et al., 2012).

The cloud computing is the fourth necessary technology to analyze and aggregate all the (big) data. It’s clear this won’t be an easy task. The data from the smart things can be of any kind: physical parameters like temperature, blood pressure, altitude, motion,

proximity to something else, sound, biometrics etc. and the network consists of diverse objects with variable data formats therefore the integration of all this data is one of the biggest challenges for IoT (Davenport & Lucker, 2015).The fundamental part of IoT is the actions required by this technology.

Cloud computing is a platform that allows on-demand network access to computing services (Geng, 2017). This platform works in the background and is used to receive data from the smart things, analyze and interpret this data and provide web-based visualizations for the user (Gubbi et al., 2013). This is a very interesting part for industries because this will generate a market with many opportunities to create value for users of IoT applications. The analysis of this data in the cloud will typically be performed by big data analytics and machine learning algorithms (Geng, 2017). Machine learning is a form of artificial intelligence and allows these algorithms to improve themselves by learning from their data input.

The Big Data has been a hot topic in recent years, but the volumes of data created by IoT applications is even greater. These huge amounts of data first must be transported from various sources and locations over a network, stored in a centralized database, and then analyzed by the cloud (Schatsky & Trigunait, 2011). This will require some time and a significant increase in storage volume. There is already a technology that provides a solution for this time-consuming process, edge computing (Ashton,k 2009). Big companies such as Hewlett-Packard Enterprise, Dell and Cisco have developed devices; mainly gateways, servers and routers that use this technology (Schatsky & Trigunait, 2011). These devices preprocess data such that information is transferred to the cloud instead of data.

IoT uses different interesting technologies, but the technologies mentioned previously are the most important ones today. It is not easy to define IoT as it is a broad

concept, but in my opinion, IoT is a synonym of the following process; The Internet of Things is the connection of heterogeneous, (everyday) objects embedded with intelligence (e.g. computing capabilities, communication abilities and a unique identifier (Miorandi et al., 2012)) which permits them to exchange data and interact (Cambridge Advanced Learner's Dictionary & Thesaurus, 2017). This interaction and data exchange may be performed by different communication channels and can be direct. However, at some point, the collected data passes through a cloud structure where it's analyzed. This process is autonomous, thus without human intervention. The process doesn't continuously ask for human confirmation and runs in the background. The information can be communicated to the user in more advanced service applications, but the focus should be on minimizing human input at the end of the process.

The communication is mainly oriented from devices to the end-user and the Internet is used to connect these end-user devices in the current technology. The focus of IoT, on the other hand, is on the autonomous interaction of smart objects without using humans as an intermediate station (Miorandi et al., 2012). The connected smart objects collect, share data and interact in the background, which in the end creates useful information for an end-user.

My impression about IoT is alike to what British technology pioneer Kevin Ashton said in 1999, when he was the first person to use the term IoT: "Today computers and, therefore, the Internet are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first created and captured by human beings by typing, pressing a record button, taking a digital picture or scanning a bar code.

The problem is, people have limited time, attention and accuracy all of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things using data they gathered without any help from us we would be able to track and count everything and greatly reduce waste, loss and cost. We would now when things needed replacing, repairing or recalling and whether they were fresh or past their best." (Ashton, 2009).

An IoT application needs to use a cloud infrastructure for the analysis of data according to my understanding. However, it's not necessary that every smart object is directly connected to the internet. When this is the case, some authors talk about an alternative interpretation of IoT, the "Intranet of Things" (Holler et al., 2014; Minerva, Biru, & Rotondi, 2015). In my opinion, whether every smart object is directly connected to the internet or not shouldn't determine if something is an IoT application and this condition is not included in my definition.

2.2.3 Components in the Internet of Things

There is a wide variety of architectures that are being leveraged in the IoT paradigm, which has led to a need to reduce the fragmented landscape. As a result, Bauer, Boussard, Bui, Carrez, Jardak, de Loof, Magerkurth, Meissner, Nettsträter, Olivereau, Thoma, Walewski, Stefa & Salinas (2013) proposed an architectural IoT reference model that provides a high-level view with a high degree of abstraction required when discussing the Internet of Things. This model aids in defining building blocks of Internet of Things applications with regard to system modularity, processor architectures, third-party options, and component placement. The common understanding of the IoT architecture provides logic for stakeholders. The high-level view of the model guides discussions and provides a common language for all parties involved. This should allow for the generation and analysis of IoT architectures for

specific systems, identify differences in derived architectures, achieve interoperability, guide design choices, and provide a model for benchmarking.

The model mainly introduces concepts and definitions which allow architectural design and reference. The reference model consists of multiple dimensions in which the domain model is the key model that describes all the concepts relevant in IoT (Bauer & Walewski, 2013). Despite the abundance of technologies that can be applied within the IoT paradigm, it remains unclear which technologies will be applied within a decade. Therefore, it requires abstractions of components within IoT applications. This is represented in the IoT domain model which is displayed in figure 2. It provides a view of entities within IoT environments and the relationships between them. The domain model is constructed using Unified Modeling Language (UML) (Fowler, 2004).

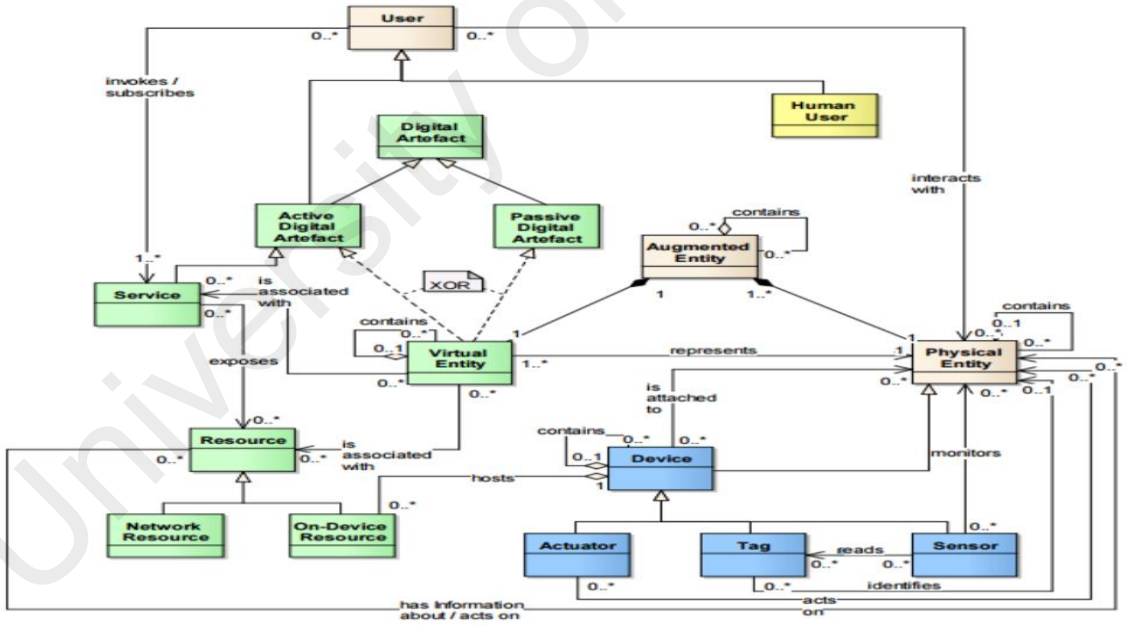


Figure 2. 2: IoT Domain Model (Bauer et. al, 2013)

In the most general form of interaction in an IoT environment, a user, either human or an active digital artefact, wishes to interact with a physical entity. Other forms are direct interactions, such as sending a parcel from location A to location B, but IoT interactions are commonly indirect, by sending or receiving services about the physical

entity. The physical entity can be characterized as an identifiable component of our environment, which can be anything from humans to objects. The physical entities are also digitized in a virtual form, which is the virtual entity. Examples of virtual entities are avatars, database entries, or programmable instances. Virtual entities are characterized by two essential properties:

1. The digital artefact must have a unique reference to the physical entity. This enables identification of the digital artefact in an unambiguous manner. A distinction can be made between active and passive digital artefacts. Active digital artefacts (ADAs) can be seen as streaming data that is used by applications, agents, or services to access other services or resources. Passive digital artefacts (PDAs) can be described as artefacts that are stored in a database, for example, for later reference. In addition, resources can describe the location of objects in the physical world in virtual entities (Dayal, Castellanos, Simitsis, & Wilkinson, 2009).
2. The virtual representations must be synchronized with the physical entities, which means that any changes to parameters in the physical environment should also be reflected in the virtual entity. For example, if a device is activated by a user, then this should also be visible in the digital artefact as a result of the change in the physical entity.

Interactions in the IoT environment can be between human users and machines, but also between two machines. Whenever there is machine-to-machine communication, one of the machines is considered the user consisting of an active digital artefact and a service. The augmented entity is the composition of the physical entity with a digital environment, which is the essence of physical things becoming part of IoT. The hardware which makes this connection possible is presented as the device, which can be an actuator, tag, or sensor. A sensor can provide data or information about the physical

entity that they monitor and can be attached or embedded in the physical entity. This can be referred to as the primary identification of natural features (Roussos & Kostakos, 2009). Secondary identification uses tags to identify physical entities and are commonly physically attached. The identification process is referred to as reading the object, which is done by a specific sensory reader (Roussos et al., 2009). Barcodes are not defined as tags since they are a physical characteristic of an object and do not possess passive computation power (Nikitin, Rao, & Lazar, 2007). A common example of a tag is an RFID chip used to identify an object. An actuator modifies the physical state within the physical environment, for example, turning on a device, or adjusting the functional properties of such a device. To provide a representation in the digital world, some physical entities rely on resources. Hardware used in the devices supporting physical entities must possess a certain degree of processing, communication and storage abilities to support IoT (Madakam, Ramaswamy, & Tripathi, 2015; Wu, Lu, Ling, Sun, & Du, 2010). It is also important to ensure the desired energy consumption properties, since the operational autonomy relies on the energy resources of the device as well as the computational resources available on the device (Fragkiadakis et al., 2014).

Resources can be seen as software to control the hardware linked to the physical entity. This enables the physical entity to process data and provide information as output. There can be an on-device resource which deploys the software locally on the device including the program code for accessing, treating and storage of the sensor information. Common limitations for on-device resources in IoT are the frequent lack of computing power and available storage on the devices (Dar, Taherkordi, Baraki, Eliassen, & Geihs, 2015). This limitation can be overcome by applying network resources which are backed by cloud or fog-based computing resources, for example Services in the IoT environment should provide interfaces to address all necessary functionalities for the interactions with resources and devices linked to the physical

entity. Papazoglou (2007) defines a service as "[a] programmatically available application logic exposed over the Internet". So, Services can be defined as the mechanism by which needs and capabilities within IoT systems are brought together. This means that services serve as the connection between the IoT phases of a system to the application of an information system (Bauer & Walewski, 2013). IoT services need to have sections that control pivotal processes necessary for the communication of tools and devices that are hooked up to the physical entity. Services have become ubiquitous in today's IT infrastructures.

IoT-linked services provide accurate and uniform sections, obfuscating the intricacy of gaining entry into different multifaceted materials. Engagement with a physical entity can be accomplished through different services linked to the analogous virtual entity. This relationship grows into an essential one in the look-up process and detection. An IoT service could well be described as one such service which provides access to communication with the physical world. As stated by Dar et al., (2015) IoT Services can be sectioned in accordance with their rank in abstraction.

Resource-level services display the purpose of a device by gaining entry into its hosted resources. These services point to a single resource. Aside from revealing the resource purpose, they work with the value part such as dependability, security (for example, access control), resilience (for example, availability) and performance (for example, scalability, timeliness). Additionally, resources can also be network resources— so, that the resources is not located on the device itself.

Virtual entity-level services give access to data at a virtual entity level. They can be services linked to a particular virtual entity that allows access to features for reading feature data or for upgrading features for trigger associations. Alternatively, provisions could be made for common virtual entity-level services with interfaces for accessing

attributes of different virtual entities. Integrated services are the outcome of a service configuration of resource-level or virtual entity-level services just like any grouping of both service abstractions.

2.2.4 Related Concepts

Different concepts related to IoT can now be used to compare by the definition presented in the previous section but have some different characteristics. A clear distinction between these concepts allows the proper classification of applications. In the near future the use of IoT could result in a mix of information for the end-user and actions from smart things. If the ultimate objective is the automation of every possible process, including human behavior, applications will directly influence human actions by actuators in the network instead of communicating information to the user (Miorandi et al., 2012). This ultimate objective is more associated with something termed as cyber-physical system (CPS). IoT and CPS are very similar concepts they use the same kind of technology (sensors, cloud computing, wireless network etc.) and are used for the automation of processes. The actuation of objects, controlling physical entities (e.g. logistics and production systems) is the only difference is that for CPS, and when talking about IoT, the focus is on the network structure used for the interaction of objects which allows the collection and integration of data (Minerva et al., 2015). In CPS system, this network structure is needed for the actuation of different objects.

A WSN is a network of autonomous sensors that used to send their data through the network to a central location (Minerva et al., 2015). For the collection of data in a lot of applications an IoT can use a WSN, but not every IoT system will use one since there are many other possibilities. The first step of an IoT system is the collection of data, this data must be analyzed and transformed into valuable information or shared with other objects. The sensors used for the WSN provide the possibility to make any object smart

and the huge progress in these sensors is probably the main innovation that started the IoT evolution.

Wireless Sensor Network (WSN) is a key enabling technology of IoT (Li et al. 2013). It connects a number of sensor and/or actuator3 nodes into a network through wireless communication and integrates this network into a higher level system through a network gateway. The sensor nodes are normally lightweight, inexpensive, easy to deploy and maintain, but the capability and functionality are limited by resources (sensors, processors, memories, energy sources, etc.). Akyildiz et al. (2002) and Yick et al. (2008) have thoroughly reviewed the architectures, applications, protocols and challenges. Among them, the challenges about energy efficiency, communication reliability, and system mobility are emphasized in the design of our WSN platform for Health-IoT.

When the WSN is integrated in an application system of IoT, it is extended to be the Ubiquitous Sensor Networks (USN). According to (ITU-T 2008), the main components or layers of USN are:

1. Sensor Networking: also called Sensor Area Network (SAN), comprising sensor/actuator, processor, communication interface, and power source (e.g., battery, solar power, or passive). The sensors can be used for collecting and transmitting information about their surrounding environment;

2. Access Networking: also called Wide Area Network (WAN), intermediary or "sink nodes" or gateway collecting information from a group of sensors and facilitating communication with a control center or with external entities;

3. Network Infrastructure: likely to be based on a next-generation network (NGN);

4. Middleware: for the collection and processing of large volumes of data;

5. Applications Platform: to enable the effective use of a USN in a particular industrial sector or application.

Many alternative technologies have been developed in recent years for SAN. Some of them have been standardized such as the Bluetooth Low Energy4, IEEE802.15.65, Zigbee 6, WirelessHART 7, ISA100 8, WIA-PA 9, and 6LoWPAN 10. The Zigbee, WirelessHART, ISA100 and WIA-PA are all utilizing the IEEE802.15.411 radio. Some are not open standard but have been widely applied in certain industry such as the ZWave12.

Some are not specifically designed for WSN but are also applied in many cases after certain optimization such as IEEE 802.11 WLAN13 (Ferrari et al. 2006). At the same time, many proprietary technologies are proposed too. Despite the diversity of technical details, all these alternatives are commonly featured by low power consumption, short range communication, flexible networking capacity, and light weight protocol stack. These are the key features required by WSN.

The aim of USN Access Networking is to connect the small area WSN to the wide area internet. It has many alternatives and they can be grouped into two types. One type is wired WAN such as the IEEE 802.3 Ethernet 14 and broadband power line communication15. Another type is wireless WAN such as IEEE 802.11 WLAN, 3GPP wireless cellular communication (GSM, GPRS, EDGE, UMTS, LTE, LTE-A, etc), and satellite. One common feature of these technologies is the infrastructure dependency. Different access types are quite diverse in terms of connectivity, mobility and cost (as shown in Table 2.1).

Table 2. 1: Comparison among USN Access Networking Types

Access Type	Cost	Coverage		Mobility
		Indoor	Outdoor	
Ethernet	Very Low	High	Very Low	Very Low
Power Line	Low	Medium	Very Low	Very Low
WLAN	Very Low	High	Low	Medium
3GPP	Medium	High	High	High
Low Orbit Satellite	Very High	Very Low	Very High	High

The ambient intelligence; is another concept related to IoT, an environment with sensing and computing abilities, which can interact with humans. This concept is different from IoT since it only supports some predefined capabilities in a closed environment (e.g., a room, a building), is focused on human interaction and the used objects don't necessarily have to be connected to each other (Miorandi et al., 2012). This is different from IoT because an important aspect of IoT is minimizing human input.

A simplified version of IoT is the Machine-to-machine (M2M) communication. The focus of M2M is on connecting devices and provide the possibility to remotely access data from these devices. This data is processed in a service management application to achieve productivity gains, increase safety or security and reduce costs (Holler et al., 2014). The data isn't integrated into other processes, only takes place on the level of the machines because the machines don't necessarily have to be connected to a cloud platform. It's more a direct, one-way form of communication. Data in IoT applications comes from heterogeneous objects in different formats and is then integrated without human intervention, this is different in M2M applications. IoT can support the same services as M2M but has much more capabilities because data in IoT applications can be used for other purposes thanks to the web-based technologies (Holler et al., 2014).

A schematic overview of all the different concepts is provided in Figure 2.3.

- An IoT system uses Cloud computing and edge computing technology.

- An IoT system uses smart objects. This isn't the same as smart devices, these are just devices connected to the internet and equipped with an interface for some predefined capabilities to interact. However, a smart object can offer the same capabilities as a smart device so that's why the structures overlap in the overview. When the used objects are sensors connected to the internet, this is called a WSN. These structures also overlap because not every smart object is a WSN. Smart objects don't necessarily have sensing capabilities as mentioned by Miorandi et al. (2012).
- The same explanation applies for ambient intelligence and M2M. An IoT system can offer the same capabilities as these concepts but IoT is more than that.
- IoT and CPS are two different concepts but there is an overlap. A CPS application will use IoT technology in most cases, for the collection of data and the interaction of smart objects. But the focus of CPS is on the actuation of objects, which isn't the case for IoT.

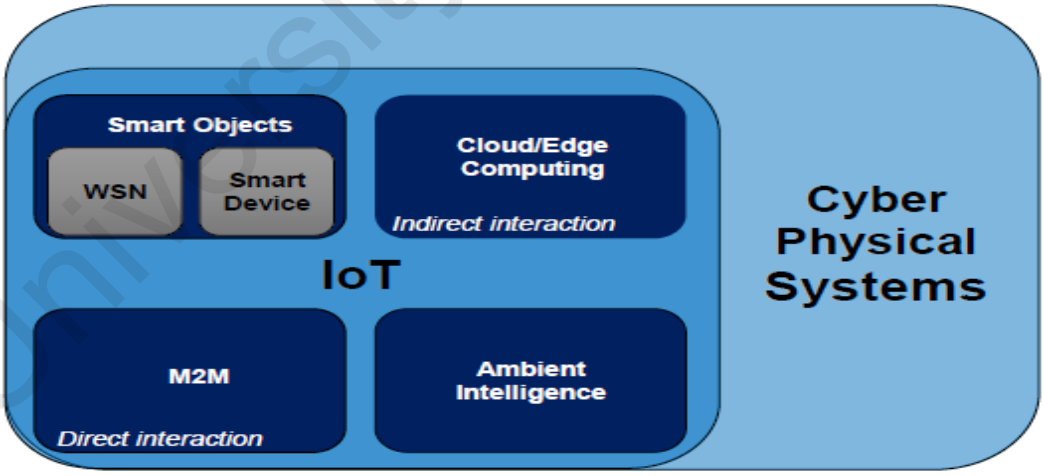


Figure 2. 3: Concepts related to IoT

2.2.5 Functional Approach to the Internet of Things

The key layers which allows the IoT to function are the device layer, the communication layer, the middleware layer, and the application layer (Alam et al.,

2011; Aloul, & Zualkernan, 2016). The IoT functional model shows the possible interactions between the functional layers. In addition, the model represents two managerial layers, which refer to the role of controlling the risks in the application and role of managing the IoT application. The middleware layer in the functional model has multiple dimensions, namely IoT service organization, Virtual entity, IoT process management and IoT service.

IoT process management is concerned with the conceptual mixture of the business value creation methods and the associated information systems. The main objective of IoT process management is the creation of operative concepts that are essential to conceptually align the customary features of the IoT services with the business execution (Dar et al., 2015). An essential component in IoT process management is its ingrained relation to organizational systems. IoT process management is the stage at which business objects and procedures merge with IoT. More importantly, the process modelling procedure has to consider the features of the IoT domain, including the particularities of the underlying business logic (Bauer et al., 2013).

The service organization component acts as the function between the IoT service, process management, applications, and the virtual entity. Service Organization is responsible for resolving and orchestrating IoT services, as well as dealing with the composition and choreography of services. Service composition helps combine basic services in order to answer requests at a higher level of service abstraction. Service choreography is a concept that supports the brokering of services so that services can subscribe to other services available in the system. Service Organization enables (business) processes or external applications to find and bind services that can be used to execute process steps or can be otherwise integrated with external applications. The service organization acts as an essential enabler for IoT process management.

Communication is an important layer since interoperability within the IoT is required. This function encompasses the sets that allow devices to interact with other entities in the IoT domain model. The communication stack exists of different layers that are based on the ISO OSI 7 layer model. However, the traditional model is not suitable for the IoT since it is not associated with device heterogeneity. A device needs to be connected to an IP address without the constraints of the hardware technology of the IoT device, such as ZigBee or Lorawan. According to Bauer (2013), the main aspects of communication within IoT communication involve the following stacks:

- The physical layer deals with the tangible characteristics of the communication technologies used in the system. It employs the adopted technologies as a premise to replicate the leftovers of the system.
- The link layer tackles the heterogeneousness of networking technologies denoted in the IoT field. This should be done by implementing interaction arrangements and security solutions. Hence, this layer requires a high level of abstraction due to the large variety of functions that allow communication.
- Networking and the ID layer merge the two communication aspects by connecting to an IP address and linking the functions of the IoT application to a specific destination. Therefore, this layer makes two systems addressable from one to another.
- End-to-end layers deals with reliability, issues in transport, functionality of data translations, proxy and gateway support, and parameter configuration when the communication crosses different networking environments.

2.2.6 Security and Risks in the Internet of Things

The security aspects of IoT are challenging, as its framework spans the physical environment to the virtual Internet. The constant complexity and distribution of IoT

applications makes the level of security even more difficult. Increased security demands for a certain IoT service will depend on certain applications and circumstances to standard security characteristics. Key challenges in IoT systems management research are security issues for ensuring access control, confidentiality and authentication. Privacy and the management of trust in IoT are additional main points of research. (Fei & Santos, 2012; Jing et al., 2014; Miorandi et al., 2012; Neisse et al., 2015; Sicari et al., 2015). This impacts many aspects that need to be considered for the governance of IoT applications. Some examples of these considerations are the importance of confidentially, identity management through access control and authentication, the need for data anonymization and privacy by design, and the context awareness of the system. In many cases, these considerations are particularly challenging due to the necessary scalability and heterogeneity of IoT devices (Perera, Zaslavsky, Christen, & Georgakopoulos, 2014).

Due to sensitive data that IoT services might contain, this information must be kept confidential. This can be achieved with encryption, such as symmetric and asymmetric schemes that will guarantee high levels of security. The selection of a specific encryption is very dependent on the application and the device (Sicari et al., 2015). Data integrity should be maintained since IoT services exchange important data with other services along with third parties, such as service providers and control centers. Therefore, there is a high demand to prevent stored or transmitted data from being tampered with, either accidentally or deliberately. It is critical that design protection be reliable and dependable for sensor data. This can be achieved with identity management, for example, Message Authentication Codes. Choosing the MAC technique should depend on the application and the device's capability (Alam et al., 2011). Furthermore, it is important for some IoT services to be continually available from anywhere and at any time in order to provide information such as measured data.

There is no specific security behavior that can do this, but different measures can be taken to guarantee constant availability. Authentication is needed in IoT because the data is used to make various decisions and to motivate different actions. Service providers and service consumers need to know that a given service is accessible to authentic users and that the service is provided by an authentic source. Significant authentication components need to be redistributed in order to prevent imitations. Enforcing any component requires a registered user identity and IoT resource, which poses a strict restriction for enabling a certain authentication (Atzori et al., 2010a; Borgohain, Kumar, & Sanyal, 2015). Then, the control of access—allowing only authorized users access to the resources—should be managed. Enforcement is usually based on the decisions for access control. IoT is the all-present privacy issue that has become a major concern. Imagine a home that is provided power using an IoT service; without proper access control, it could lead to the disclosure of a user's information, such as when someone would be home. It could interfere with a user's activities within the home. Therefore, it is critical that user information only be provided to authorized people. There are applications that are very sensitive, such as those for healthcare services that need to assess the trustworthiness of various entities. From the perspective of IoT applications, assessing the trustworthiness of sensors and data is extremely important. Malicious sensor nodes and non-trustworthy sensor data can lead to a complete safety disaster. Non-trustworthy behavior could come from intentional harm or unintentional errors (Alam et al., 2011; Borgohain et al., 2015).

2.2.7 Internet of Things Risk Ontology

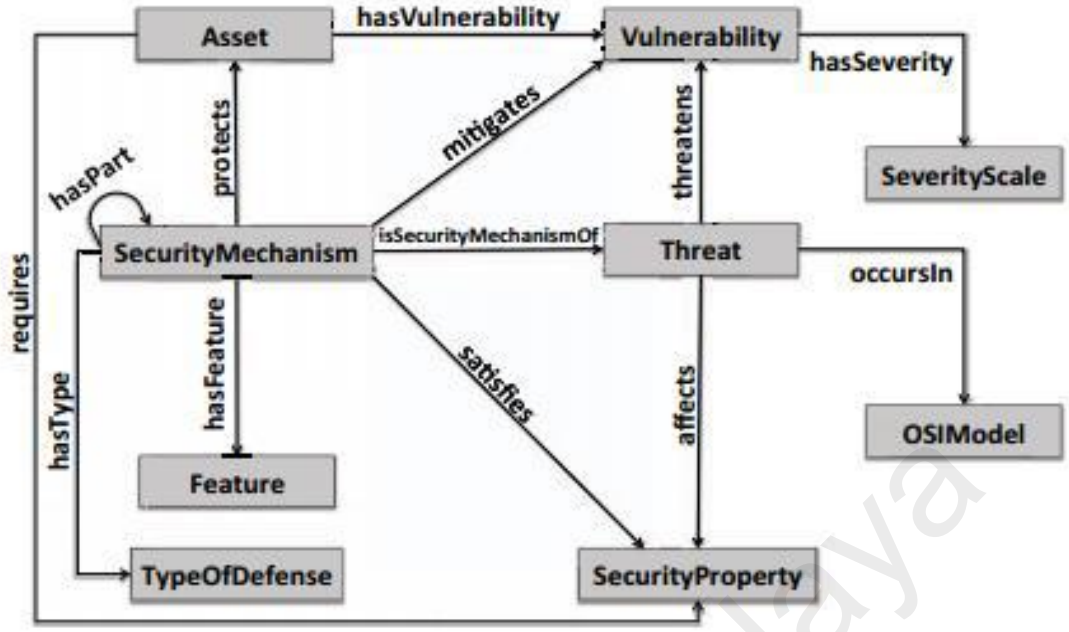


Figure 2. 4: IoTsec Ontology (Mozzauarto & Jardim-Goncalves, 2015)

2.2.8 Risk Controls

If auditors obtained information about the risks in the IoT environment, they can assess to what degree an enterprise has controls in place in accordance with their risk tolerance and risk appetite within their IoT environment. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines risk tolerance as "the degree of risk, on a broad-based level, that a company or other organization is willing to accept in pursuit of its goals. Management considers the organization's risk appetite first in evaluating strategic alternatives, then in the setting of objectives aligned with the selected strategy, and in developing mechanisms to manage the related risks" (COSO, 2004). And they define risk appetite as "the acceptable level of variation relative to the achievement of objectives. In setting specific risk tolerances, management considers the relative importance of related objectives and aligns risk tolerances with its risk appetite" (COSO, 2004). Risk management entails processes and methods to seize the opportunity and manage risk in attaining the company's objectives (ISACA, 2009). It usually starts with recognizing circumstances or specific events that are crucial to the company's objectives such as securing the danger of data breaches, intensely checking

them in terms of magnitude and likelihood of the effect (ISACA, 2009; Peltier, 2004). For example, if the inherent risk of a data breach is rated high and the dangers of such breach is also rated high, then make sure there is an appropriate response to the breach. If an organization explicitly addresses its risk and opportunities, it would be in the best position to create value for its stakeholders. So, risk management will help provide insight into the important risks for the entire organization. This can be used to determine audit priorities, set up project activities, and form tolerance and risk appetite. When there is a risk management process in place, it can be used to assess how an organization will deal with the risk. It can accept the risk, eliminate the risk, share the risk, or control the risk.

Information Technology General Controls (ITGC) are used to control risks of system data, processes, or components of a particular system environment or organization. Some common controls include user management, resource management, IT governance, IT operations, application maintenance and development, risk management, backup and recovery, change management, physical security, logical security and business continuity. Some common controls are related to business while others are technological in nature (for example, system software controls and network software controls) and they relate to the underlying infrastructure. Common IT controls are reviewed by auditors, because the controls form the foundation of internal control (van Praat & Suerink, 2004).

Application controls relate to the application systems or scope of individual business processes and involve controls within application input, processing, and output. Also included in the application controls are segregation of business functions, data edits, error reporting, transaction logging, and balancing of processing totals. The performance of a control application is related to the evaluation of its effectiveness and design (van Praat & Suerink, 2004). Controls are assigned according to the risk levels,

where required. From a general perspective controls can be classified as detective, preventive, or corrective measures (Peltier, 2004). Detective controls detect incidents or errors that evade preventive controls. For instance, the detective control may recognize accounts that have been selected for monitoring of suspicious activities or inactive accounts. Detective controls can also include analysis and monitoring to determine events or activities that violate known patterns in data or exceed authorized limits that may show illegal manipulation. Detective controls can demonstrate that a sender cannot be authenticated, or the message has been corrupted (Peltier, 2004).

Preventive controls prevent security incidents, omissions, or errors from occurring. For instance, dynamic and complex technical control such as intrusion prevention systems, firewalls, antivirus software; access controls that guide sensitive system resources or data from unauthorized individuals; simple data entry edits that obstruct alphabetic characters from being entered into the numeric field (Peltier, 2004). Corrective control correct omissions, errors, or incidents once they've been detected. They differ from just correcting wrong data entry to removing and identifying illegal users or software from networks or systems to recover from disruptions, incidents, or disasters (Peltier, 2004).

Other familiar categorization of controls is by the group accountable for ensuring they are maintained and implemented correctly. For the assessment of responsibilities and roles, this guide mainly classifies management, IT controls of governance, application, and technology. However, management and governance are the most relevant to the scope of the guide. It may also be helpful to know how higher-level controls are specifically developed within the application IT and technical infrastructures (GTAG, 2012). Figure 2.5 shows an overview of it.

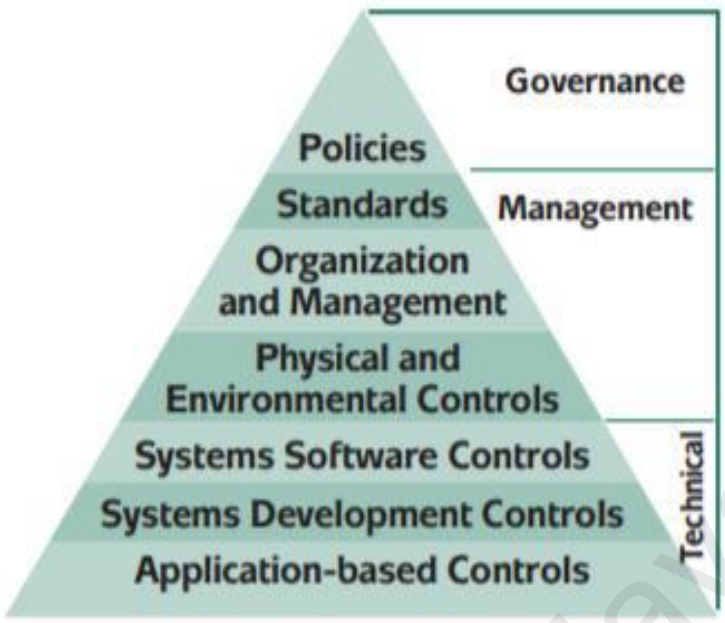


Figure 2. 5: IT Risk Controls (GTAG, 2012)

IT governance controls—The main role for internal control oversight stays with the board in its task as keeper of the governance framework. Information technology control at the level of governance includes monitoring active information principles, processes, policies, management, ensuring that they are in place and performing correctly. IT governance controls are attached to the concepts of governance, which are controlled by both the organizational strategies and goals and by external bodies like the regulators (GTAG, 2012).

Management controls explains responsibilities for internal controls which mainly includes sensitive information, reaching into every area of the company with particular attention to operational functions and critical assets. Management must ensure that the IT controls they need to attain the company's defined objectives are applied, reliable, and are a continuous process. Management controls are deployed as an effect of intentional actions by management on the risks to the company, assets, and its procedures (GTAG, 2012).

Technical controls often make up the logic behind management's control framework. The entire control framework is affected if the technical controls are not active, for

instance, by guiding against illegal intrusion and access, technical controls lay the foundation for reliance on information security including its evidence of all changes and authenticity. Technical controls are the technologies in use within a company's IT infrastructures (GTAG, 2012). Some examples of these controls are logging, database controls, encryption and operating system controls.

2.3 Business models

The importance of business models for new technologies can be illustrated by a quote of Chesbrough. "A mediocre technology pursued within a great business model may be more valuable that a great technology exploited via a mediocre business model" (Chesbrough, 2010). Since the foundation of IoT is the use of different technologies, this statement also applies for IoT.

2.3.1 Business models in academic literature

At the moment, there still does not exist a consensus on a framework for business models. Every framework has a certain level of detail and focusses on different aspects. In their review of academic literature on business models; Massa, Zott, and Amit (2010) explain that researchers still haven't reached an agreement on a definition for a business model since it's used for different concepts:

"Throughout our review, we have seen that the business model has been used to address different concerns in different contexts and in different management areas. Scholars have used the same term (i.e., business model) to explain and address different phenomena such as value creation or value capture by firms, e-business types, and how technology innovation works." (Massa et al., 2010). However, Massa et al. (2010) did also conclude business models are now widely recognized as a tool for analyzing how firms do business and business models try to explain the value creation and capturing of a company. So business models can be useful to examine how firms do business and

create value but it's important to make sure the business model framework addresses the right concept in the context it is meant for.

2.3.2 Business Model Ontology

One of the papers reviewed in the research of Massa et al. (2010) is 'The business model ontology—A proposition in a design science approach', by Osterwalder (2004). The Business Model Ontology (BMO) (Osterwalder, Pigneur, & Tucci, 2005) was the theoretical basis used to create the Business Model Canvas (Osterwalder & Pigneur, 2010), the most famous and widely used technique for the representation of a business model. In the review, Osterwalder's BMO is classified as a business model for e-Business. This means the use of information technology in organizations and internet-based business. Since IoT fits this classification, this technique is applied in the right context to describe the business model of companies that use IoT. Osterwalder's definition for business models is the following: "A business model is a conceptual tool that contains a set of elements and their relationships and allows expressing the business logic of a specific firm. It is a description of the value a company offers to one or several segments of customers and of the architecture of the firm and its network of partners for creating, marketing, and delivering this value and relationship capital, to generate profitable and sustainable revenue streams." (Osterwalder et al., 2005)

2.3.3 Impact of the Internet of Things on business models

There are three ways to look at IoT and business models. On the one hand, are the companies that will implement IoT in other companies or intervene somewhere in the creation of IoT systems. They solely use IoT technology as their main value proposition and IoT is used to create straightforward applications (e.g. predictive analytics). On the other hand, they are currently using business models. These will be transformed by the impact of IoT. The creation of completely new business models is the third perspective.

These three perspectives are comparable to the three phases in a study of the McKinsey Global Institute on IoT.

The authors predict three phases for suppliers in the IoT technology market, in comparison with the evolution of personal computers and the Internet in its earlier days (Manyika et al., 2015). The first phase is characterized by the domination of companies that produce infrastructure and hardware, the building blocks of the technology. For IoT, this means sensors, data storage, cloud computing, connectivity infrastructure, etc. The next phase involves the creation of core services and software that use a broad platform. In the personal computer and internet evolution, this meant Google and Yahoo's search engine. In the third phase, new business models based on the technology will dominate the market. Examples from the personal computer and internet evolution include companies like Amazon, Uber, and Airbnb. Where each transition to the next phase involves an increase in the total value of the IoT market (Manyika et al., 2015).

According to Manyika et al. (2015), we are currently located between the first and the second phase. Nevertheless, in these early phases, IoT already offers great opportunities to create value. Maciej Kranz, vice president Strategic Innovations Group at Cisco and previously general manager of the Connected Industries Group at Cisco, a business unit focused on the Internet of Things, has already seen the following paybacks for companies deploying IoT at this stage (these companies were mostly situated in the B2B area) (Kranz, 2016):

- New insight into product usage and customer information
- Development of new product and service delivery options
- Reduction in costs
- Design and creation of new business models

- Revenue generation
- Implementation of new go-to-market strategies
- Increased uptime
- Speedier service and delivery
- Streamlined business processes
- More efficient ways to service and support customers

Now focusing on (one of) these paybacks could already offer different possibilities for companies to create interesting value propositions. For companies that succeed in building a complete business model to support these value propositions, IoT technology could turn out to be a lucrative opportunity. This is the so-called first phase.

Based on the research of Gassmann et al. (2013) on business model patterns; Fleisch, Weinberger, and Wortmann (2014) identified two business models patterns that could be commonly used alongside the usage of IoT technology when the IoT technology market evolves to phase two. These business model patterns are based on the existing business model patterns of Gassmann et al. (2013). The digitally charged products business model pattern is quite basic. Digital services are linked to physical products to create new value propositions. Fleisch et al. (2014) define six transformed business models based on the idea of the digitally charged products (e.g. Add-on, Freemium, Pay per Use, etc.). It's mainly one smart object with a fixed digital service offered in different forms. The type of service determines the business model. This is quite superficial and in my view, not the true value of IoT. These are business models for smart devices, with applications that provide an interface for the user, to make use of services for the device.

The second business model pattern is called Sensor as a Service. The collected data from products can be sold to external interested parties. The value proposition isn't a

service or product, but the data itself. This business model is based on the existing Software as a Service (SaaS) business model. The provider in this model offers on-demand information processing services to the user (Ma, 2007). This business model results from the use of cloud computing in applications. Instead of merely selling the software, the provider offers the use of its hardware, IT infrastructure, and all associate support services (e.g. Security, maintenance, data backup, installation) to deliver applications on demand for the user through a network (Ma & Seidmann, 2008; Mell & Grance, 2011). For the use of this service the user only pays a fee.

Based on the seven laws of information from Moody and Walsh (2002), Bucherer and Uckelmann (2011) present four exemplary business model scenarios for the Internet of Things. The value proposition for the business models is always based on information as a value creator (raw data as well as aggregated or processed data). These four business model scenarios are similar to the pay-per-use model, the Sensor as a Service business model pattern and two of the specific digitally charged products business models (Remote Usage and Condition Monitoring; and Product as Point of Sales). It is clear it's already difficult to predict the impact of IoT on business models. Since IoT itself is still in such an early phase it's not possible to predict in the near future which new business models will be created.

2.3.4 Challenges for IoT

Now that IoT and business models are discussed sufficiently in the previous sections, the challenges concerning this topic can be explained. There are three main challenges that still must be conquered for IoT to be successful. The first challenge is a technical one. The interoperability of smart objects, the main feature of IoT, still needs to be worked out. All connected objects from different manufacturers should operate fluently to be valuable, this is also important for the exchange of data. This will require open standards and industry-wide interoperability (Kranz, 2016). It's clear this will take some

time, but in the words of Maciej Kranz: “The industry knows how to do it; we did it for the first stage of the Internet and for the cloud. The current task at hand is even bigger and more complex, but I know that the IoT community is up for the challenge.” (Kranz, 2016).

There are a lot of possibilities with IoT but this concept can’t completely prove its value until the objects can properly interact with each other. Most companies will possibly try to avoid the collaboration with other companies for as long as possible. IoT hasn’t proven its value yet and collaboration on interoperability poses the risk of sharing trade secrets and other intellectual property. However, as mentioned by Kranz (2016) collaboration and partnerships will be imperative for IoT to succeed.

The role of the government is the second challenges. Government regulations are obviously needed in some areas, but too much regulatory restrictions have to be avoided to leave some space for companies to innovate their business model (Kranz, 2016). The problems with Uber and the taxi sector have shown it’s not always easy to find the right balance between new business models and regulations from the past (Schellevis, 2014). The government also has a role to play for concerns about privacy and security. As mentioned, security in an IoT environment will be a difficult assignment since there is a trade-off between the fluent interaction of different smart objects and preventing unauthorized access of these objects to sensitive data. On the other hand, privacy and security are still a concern today in the world of social media, smartphones, and other applications while these industries seem to operate quite profitably.

IoT is an interesting technological evolution, but it is only relevant if it provides value for its users. This is a big technological change with a lot of opportunities, but it’s not easy to find a good value proposition and the right business model to support it. Big

Data for example is a concept that's been around for some time now and companies are still having some difficulties trying to figure what to do with it.

2.4 Health Care

The delivery model of healthcare in the coming decades, will transform from the present hospital-centric, through hospital-home-balanced in 2020th, to the final home centric in 2030th (Koop et al. 2008). The future healthcare system should be organized in a layered structure, e.g. from low to high comprising the personal, home, community, and hospital layer; and the lower layer has lower labor intensity and operational cost, higher frequency of usage for chronic disease, and lower frequency of usage for acute disease (Poon and Zhang 2008). So the in-home healthcare (IHH) service enabled by the IoT technology (the so-called Health-IoT) is promising for both the ICT industry and the traditional healthcare industry. The Health-IoT service is personalized and ubiquitous and will speed up the transformation of healthcare from career-centric to patient-centric (Liu et al. 2011, Klasnja et al. 2012, Plaza et al. 2011).

The latest improvements in e-Health and the advent of the Internet of Things pointed towards a fourth paradigm of health data sources can range from body sensor networks to physician analysis and diagnosis and are aggregated into a unied model (FHCR or EHCR) of human health. This focuses on how the Internet of Things can be a suitable framework for e-Health communication and especially how low-cost and low-power devices can enhance the quality of life of people during emergencies and suffering from chronic diseases. In addition, we advocate the importance of using open standards based communication solutions for e-Health applications, since allowing heterogeneous hardware and services to seamlessly interact with one another is the cornerstone for

removing the operational barriers and creating a holistic health care system on the Internet.

The health care is a complex sector without any doubt. There are a lot of different stakeholders with their own objectives and the structure differs in every country since it's mostly determined by extensive government regulations (De Cleyn et al., 2015). Since there are such big differences between health systems, only the health system in Malaysia is discussed; followed by general trends and problems in health care and the use of business models in health care

.

2.6 The Health Care System in Malaysia

Malaysia currently has a dichotomous public-private system of health care services. Since the time of independence it was largely a government-led and funded public service enterprise, the healthcare service has over the decades, transformed into a buoyant dual-tiered parallel system, with a sizable and thriving private sector. But the country has not approached a unified system that is a declared national healthcare policy of offering universal access to every citizen. There appears to be strong ambivalence as to whether to fully tap into the free market system for healthcare provision and funding or to resort to a single payer publicly controlled system where universal healthcare access is assured. At the current moment some mix of these two disparate systems seems to be in play.

There has always been an overarching concern for the common citizen, especially the poorer segment of Malaysian society on the other hand, where there is an implied social contract and acknowledged 'right'. There is a deep-seated commitment of the Malaysian government to develop human capital and eradicate poverty. It is expected that the government guarantees a comprehensive provider function at greatly subsidized rates or

at token sums—that taxes and other contributions should provide adequately for most if not all its citizens, with the government taking up the shortfalls for unexpected costs due to catastrophic or chronic ailments. On the other hand however, there appears to be a covert if unannounced shift in thinking that eventual corporatization of the public sector facilities and services should be allowed to unfold, where market forces dictates the price, extent and quality of the services offered. The ultimate aim is that the government should play only a regulatory, monitoring and facilitator role to safeguard the welfare of its citizens, while at the same time encouraging growth of the less-bureaucratic, better-run and more competitive private sector.

Thus, despite public dissent, over the past 20 years or so, there have been sporadic if partially successful attempts to privatize or corporatize various components of the public health sector, e.g. the government's drug procurement and distribution centre (to UEM's subsidiary Southern Task, later renamed as Remedi Pharmaceuticals, then as Pharmaniaga); and the divestment of its support services (biomedical engineering maintenance, cleaning, linen, laundry, clinical waste management,) to Faber Mediverse, Pantai Medivest, and Radicare.

Also, there has been full and implicit encouragement of the private healthcare sector to flourish with differing modes of financing and capital injection. Government-linked corporations (GLCs) such as the Sime Darby groups, KPJ (Kumpulan Pelaburan Johor) and latterly the Ministry of Finance investment arm, Khazanah, have been pushed to become major players in modernizing and extending the reach of the private health care services in Malaysia and beyond.

2.6.1 Rural Health Service

The rural health service is one of the largest sectors in the services department whereby the government provides almost all the infrastructure and the human resources. Throughout the country doctors, pharmacists, dentists, nurses and other allied healthcare workers are employed and deployed by the Minister of Health to various healthcare centres: from rural clinics to district hospitals to tertiary specialist hospitals.

The MMA (Malaysian Medical Association), through its Section Concerning House Officers, Medical Officers and Specialists (SCHOMOS) has been arguing for more structured deployment planning, such that even with these incentives, there should be detailed contractual undertakings that these personnel would be re-deployed to bigger centres of their choice once they have completed their 'hardship' service in the interior.

2.6.2 Tertiary Healthcare Services

In the beginning of 1980s, Tertiary Care Hospitals have made its presence felt in the Malaysian public healthcare sector, with the expansion and privatisation of the University of Malaya Specialist Centre (Petaling Jaya), and the building of the Universiti Kebangsaan Malaysia Medical Centre (Bandar Tun Razak, Kuala Lumpur), and the renowned National Heart Institute (Institut Jantung Negara, IJN), along Jalan Tun Razak. These have delivered excellent specialist care for many highly specialized medical disciplines such as neurology, nephrology, cardiology, cardiothoracic surgery, nephrology, cancer care, and some infectious diseases. These however cater predominantly to Malaysian civil servants, pensioners and their dependents, but long waiting times are now the norm due to facility constraints.

2.6.3 Private Health Care Sector

On the other hand the private sector, has always attracted both general and family physicians who had opted out by opening individual clinics or by joining more established group practices; while specialists join the better-paying more personalised care practices in urban private medical centres. During the Mahathir Mohammad premiership in the 1980s, private healthcare expansion began in earnest, where private hospital beds increased nearly 10-fold (from 1171 to 10405 between 1980 to 2003), and the private sector's share of hospital beds increased from 3.9-5.8% to 23.4-26.7%(MOH).

2.6.4 Private Medical Centers & Hospitals

Hospital care through well-equipped emergency departments (EDs) is now the expected practice for more serious illness and injuries. These medical emergencies are previously offered only at larger public sector general or district hospitals. These days however, most private medical centres boast of state-of-the-art emergency care at more luxurious settings and costs. Personal and more attentive specialist care are now demanded and offered at many of these private EDs, where many neurosurgeons and orthopaedic surgeons now practice privately. However, private medical centres are not simply for emergency and/or trauma care. Most are now developed as competitive consumer-driven full-fledged healthcare facilities to cater for the more discerning public who would pay more to obtain perhaps better, faster, more personalised, faster and possibly more comfortable and/or luxurious medical care. Together with the Association of Private Hospitals (APHM), there has been a move to expand the services toward attracting foreign medical tourists, which is targeted to raise to 30% in 2008, and nearly 1 billion ringgits as of 2005.

2.6.5 Recent trends in health care

Continuous rise in health expenditure is the most common topic regarding the health-care system in Malaysia, but also in the US, UK, etc. This is due to a variety of factors. The health-care sector is characterized by significant improvements in terms of treatment, medical technology etc. However, the cost aspect of these improvements remains a serious problem in this sector. In 2018, Malaysia's government set aside approximately US 6.75 billion or 10.4% of the annual national budget for public healthcare.

The IoT can have the biggest impact on the three problems areas which are the increase in patients with a chronic disease (e.g. asthma, diabetes, obesity, etc.); aging population, and the general continuing inefficiency of this system.

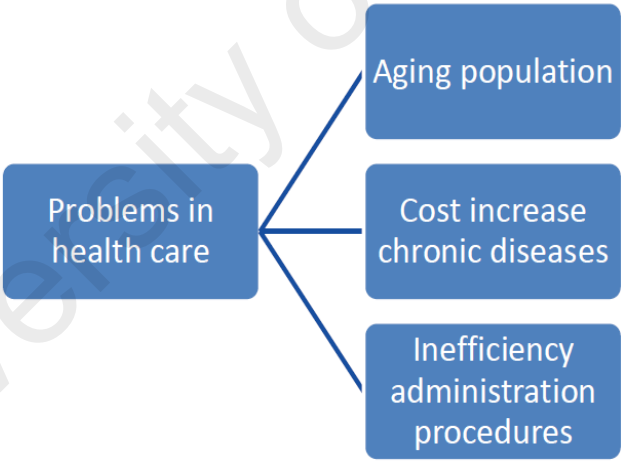


Figure 2. 6: Problems in health care

Islam et al. (2015) discuss the use of IoT for remote health monitoring of patients with a chronic disease with frequent follow-ups for their condition. Decreasing the need for face-to-face visits in the doctor's office is one way of opposing this rise in medical costs. Doctors can check-up on patients by simply looking at the data of their patient's vitals by using IoT applications. Another similar application can be used to support the elderly. By monitoring senior citizens and providing emergency notification systems, it

permits them to live at home independently for longer periods (Geng, 2017). Another way of reducing costs can be reducing the number of admissions in home.

Increase efficiency is value-based health care is the third popular trend in the health-care industry. Sickness funds in many countries are trying to shift the basis for reimbursement from the type and number of procedures to the quality of care delivered. However, this variation is happening slowly due to the reducing volume (and increasing value) cuts into short-term profits of the health-care providers (Kaiser & Lee, 2015) and this requires significant organizational changes. Another trend that illustrates the ongoing concerns in health care includes the focus on prevention instead of treatment and a holistic approach to treating patients. The relevant trends in health care that offer opportunities for IoT are summarized in Figure 2.7.

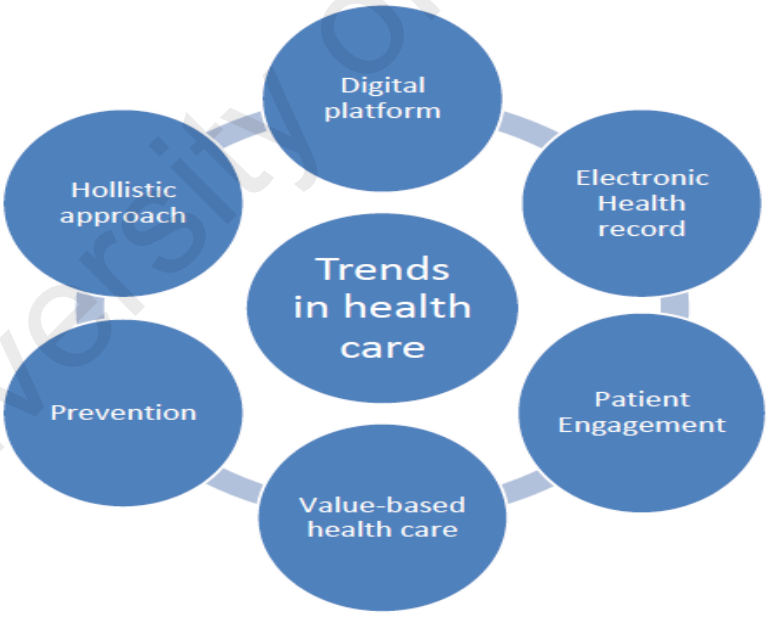


Figure 2. 7: Recent trends in health care

2.7 Business models in health care

The patient engagement and the value-based health-care concept can be used as a starting point towards business model innovation, but so far, companies in this sector have failed to implement it successfully. According to Christensen, C. M., Grossman, J.

H., & Hwang (2009); there are two important factors that could explain this phenomenon. Namely the reimbursement system and the extensive regulations of the complex health-care sector. Van Limburg et al. (2011) share the same view on this subject, a lagging legislation and financial difficulty are mentioned as reasons why this sector is so resistant to change. Other reasons mentioned by van Limburg et al. (2011) are a deficiency of publications that illustrate how business models can be created in health care and the lack of business-like thinking in general. This is a challenging topic in this sector. They specifically focus on the significance of using businesses models when developing technologies in the health care industry, in their research. The authors believe this is the main reason why currently, new technologies often create extra side processes instead of replacing old processes characterized by inefficiency.

2.8 IoT in health care

One of the current challenges for IoT is the finding the right business model for IoT applications, this challenge becomes more difficult when combined with health care. IoT is still an unknown area and health care is a complex sector with many government involvements, which creates business model innovation in this sector difficult. However, if companies can successfully create business models to support their IoT application, two of the three enables for disruptive innovation are present (Christensen, C. M., Grossman, J. H., & Hwang, 2009). IoT is a technological enabler and business model innovation is the second enabler. The third enabler is a value network and defined by the authors as "a commercial infrastructure whose constituent companies have consistently disruptive, mutually reinforcing economic models" (Christensen, C. M., Grossman, J. H., & Hwang, 2009). Of course, one company alone cannot completely disrupt health care. A good interaction with the different care providers and the insurers is needed such that a value network exists through which care is delivered. This is also called a commercial ecosystem by the authors, which corresponds to the

need for an IoT ecosystem. So again, the partner network building block will be an important aspect when developing a business model for companies with an IoT application in health care. Besides these three elements, the authors mention the need for regulatory reforms and new industry standards to facilitate change in the new disruptive industry.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Microsoft Access

Microsoft Access, often abbreviated "MS Access," is a popular database application for Windows. Access allows users to create custom databases that store information in an organized structure. The program also provides a visual interface for creating custom forms, tables, relationship and SQL queries. Using either visual forms or a basic spreadsheet interface data can be entered into an Access database. The information stored within an Access database can be searched, browsed, and accessed from other programs, including Web services.

While Access is a proprietary database management system (DBMS), it is compatible with other database programs as it supports Open Database Connectivity (ODBC). This allows data to be sent to and from other database programs, such as Oracle database, MS SQL, FoxPro, and FileMaker Pro. This compatibility also enables

Access to serve as the back end for a database-driven website. In fact, Microsoft FrontPage and Expression Web, as well as ASP.NET have built-in support for Access databases. For this purpose, websites hosted on Microsoft Windows servers often use Access databases for generating dynamic content.

In Microsoft Access a database consists of one single file. The file contains all the tables of the database, the relationships, queries (computed tables), forms (user windows), Macro and many other things. As a systems developer we will design tables and user windows. As a user we will enter data into the tables (usually through user windows) and get data out of the tables, for instance through the same windows or through printed reports. In Access it is very easy to switch between the developer role and the user role. As a developer we will typically design some tables, then switch to the user role to enter data into them, then switch back to the developer role to change the design, design more tables, etc. Access can to a large extent restructure the data that already is in the database so that it matches the new table design.

We are going to start a new database of Health IoT and save all the Files — word processed files, presentation files, spreadsheet files, or database files in own Data Files folder (not in the Work Files folder).

Open Access (Start > All Programs > Microsoft Office > Access 2007)

Click on the Office button and, from the menu, select New...

Access now presents with the Getting Started with Microsoft Access screen.

Figure 3. 1: Getting Started with Microsoft Access

As we can see in the left-hand frame is a list of different types of database templates. In the center is a set of illustrations of the templates for the specific template type currently selected in the left-hand frame. Then, over on the lower right is the box where we type the name for the new Blank Database.

Double click in the Title Bar at the top of the Microsoft Access window

Now, before typing the name for the new database, we need to locate the place where the database will be saved on the disk.

Now click on the Browse button next to the File Name box and, in the

File New Database dialog box, locate the Office 2007 Work Files folder and open it.

Now double click to open the Data Files folder.

We need to create a new folder for the databases where we are going to build.

Click on the New Folder icon in the File New Database dialog box and name the new folder Database Documents, then click on OK.

Figure 3. 2: Creating a new folder for your databases

Now type Health IoT Template.accdb for the new database name and click on OK, then click on the Create button in the lower right corner of the window

Notice that the Table object is selected on the left side of the Access window. A Table is the default object in a new Access database. But first we need to remove the Security Warning as before.

Click on the Options… button and click in the radio button next to Enable this content

Now click on the Create Tab so that we can see the Ribbon for creating Tables, Forms, Reports and other database items

In the Tables group, click on Table Design and we will now see the Table's Design View dialog box.

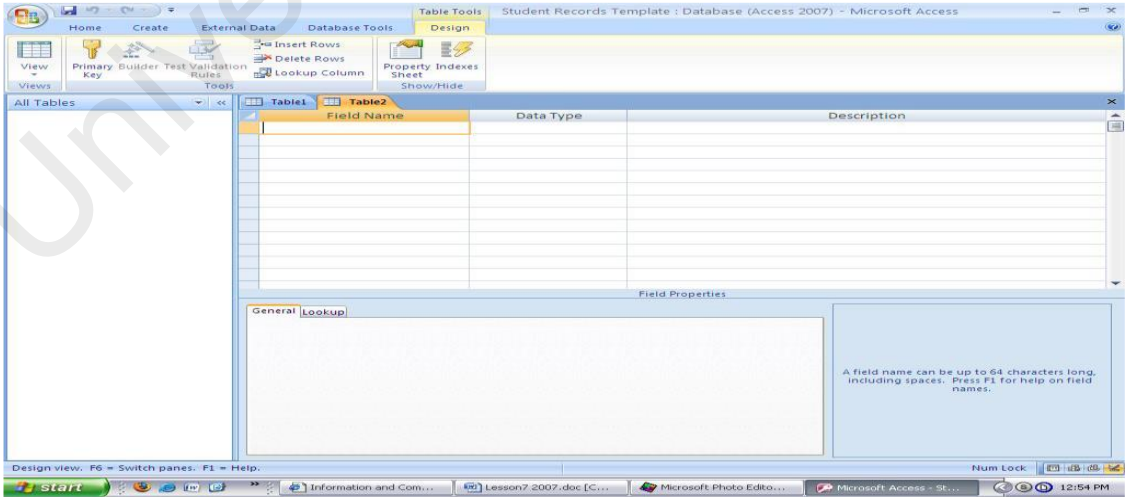


Figure 3. 3: The Table Design View dialog box

On the screen, Access is waiting to begin typing in the field names. The cursor is located in the first data entry box in the Field Name column, prompting to type in a

name for first field. Access field names can be up to 64 characters in length. Before entering the field names, however, read what follows.

Editing field names below provides complete list of all the field names for The IoT Healthcare database and can be easily change, add or delete fields.

Selecting the data type of a field, after typing in the field name in the first column, need to decide what the field's data type should be in the second column.

Setting up predefined entries for a field-To reduce the likelihood of bad data getting into the database, we can limit the user's choices when they enter the data for a particular field. For example, when they enter the Gender, we can limit the choices to M or F

3.1.1 Create the database

1. Locate the Access program. Depending on the way the system is set up, we will find it under Pro-grams -> Microsoft Access or Programs -> Micro-soft Office -> Microsoft Access.
2. In Access 2007: Open Access and click the New icon (under the File menu). Then click Blank da-tabase in the help area to the far right.
3. Access now asks where to store the new database. Select the folder we want and give the database the name health (or health.mdb).
4. Define a table
   Here we define the fields (attributes) of the table. The list of fields runs downwards with one line per field. Initially there are only empty lines. The table hasn't got a name yet. Access asks for the name when we close the window.

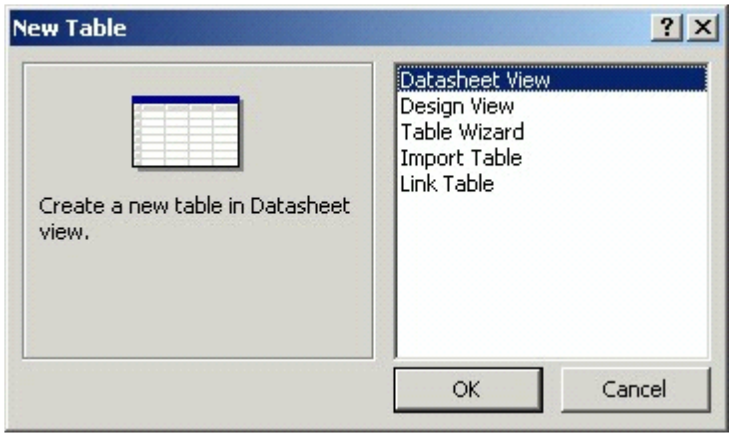
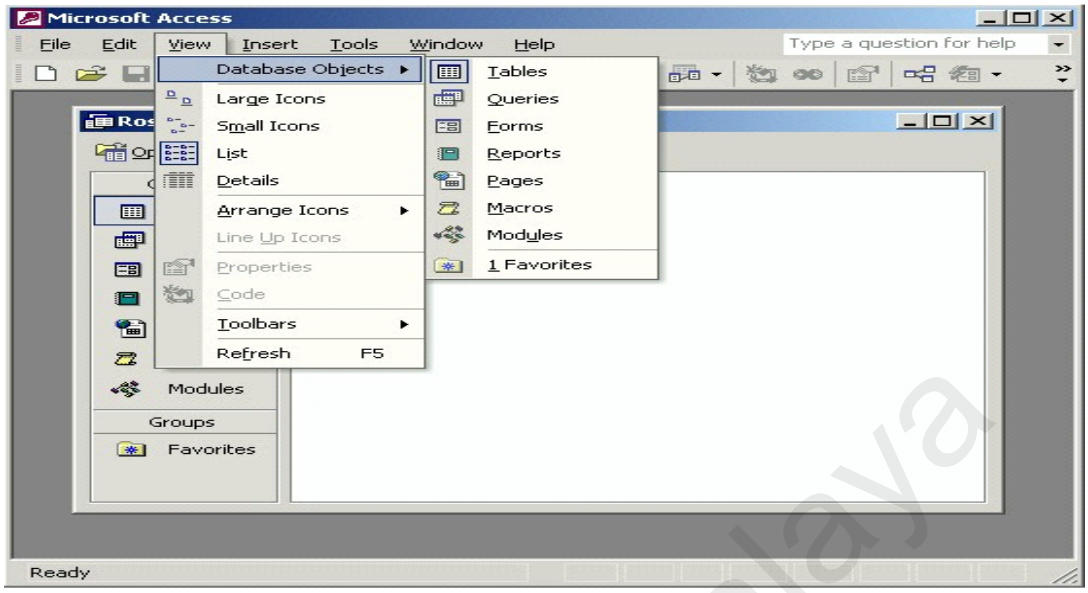


Figure 3. 4: New Table dialog box

Double click on Create table in Design view.



Now we will get a window and here we define the fields (attributes) of the table. The list of fields runs downwards with one line per field. Initially there are only empty lines. The table hasn't got a name yet. Access asks for the name when you close the window.

Tbl:Patient Data

Patient ID	FirstName	LastName	DOB	Sex	PhoneNumber	Country	Click to Add
1	MS Yang	Qin	15-Sep-87	Male	(60) 111-2582848	Malaysia	
2	Alia	Bhatt	01-Jan-86	Male	(60) 182-4709706	Bangladesh	
3	Aisha	Nadhu	16-Jun-89	Female	(60) 832-4753555	Malaysia	
4	Mrs Wahida	Khatun	25-Mar-78	Female	(60) 112-4367537	Germany	
5	Hamida	Begum	27-May-65	Female	(60) 183-4687558	Germany	
6	Mrs Haniffa	Alya	25-Feb-95	Female	(60) 172-3573859	Malaysia	
7	Khaleda	Zia	15-Aug-65	Female	(60) 123-4762364	Bangladesh	
8							
(New)							

Figure 3. 5: Patient Data table

The figure 3.5 shows the finished patient table. You see the field names to the left. In the middle column is the type of the field - Data Type. The figure shows all the possible types as a combo box. The most important data types are Text, Number, Date/Time, and AutoNumber. An AutoNumber is a counter that Access increases for each new record, so that it serves as a unique key. The value is a Long Integer (32-bit integer).

All the fields are of type Text, except the patientID which is of type AutoNumber.

Note that although we say phone number and passport number, these fields are texts because the "numbers" contain parentheses, dashes and maybe letters.

When we have chosen a data type, we can choose a number of other field properties. They are in the lower part of the window. On the figure we can see that the name field is a text field with space for 50 characters. We can also see that the user doesn't have to enter anything in the name field (Required=No). We should change this to Yes since it doesn't make sense to have a patient without a name.

Try to use Access's help to find more information about the data types and their properties. For instance, put the cursor in the Data Type of a field and click F1. Or point at one of the properties and click F1.

Lookup Wizard is not a field type. If we select Lookup Wizard, it makes the field into a combo box where the user can select a value instead of typing it into the field.

Key fields

Often we have to define a key field so that other tables can refer to this one. In our case, patientID must be the key field:

1. Right-click somewhere in the patientID line. Then select Primary Key. Access now shows that the
2. Close the window. Access asks for the name of the table. Call it tblpatient. (The prefix tbl will help to remember that it is a table. As the system grows, there will be patient windows, patient buttons and many other things. Without discipline on our part, it becomes a mess.)

If we have not defined a primary key, Access will warn and suggest that it makes one for us. Don't let it - do it yourself. Or at least check what Access makes in its excessive helpfulness.

Enter data

After these efforts, it is time to record some patients.

Select the patient table in the database window. Click Open or just use Enter.

1. Now the system shows the table in user mode (Datasheet view) so that we can enter patint data.
2. We can add a new patient in the empty line of the table - the one marked with a star. Notice that as soon we start entering something, the record indicator changes to a pencil and a new star line appears. The pencil shows that we are editing the record, and the record we see is not yet in the database.

We originally entered a patient that got patientID 4, later deleted this patient. Access will never reuse number 4 for a patient.

Close and reopen the database

To feel confident with Access, it is a good idea to close and open the database now.

1. Close the large Access window. (Not the small database window inside the Access window.)

Notice that Access doesn't ask whether we want to save changes. Access saves them all along, for instance when we define a table or when we enter a record in the table.

2. Find database file (healthcare.mdb) in the file folders. Use Enter or double click to open it.

Create relationships

When we have several tables, we can make relationships. Then we get an E/R model instead of a simple collection of tables. The relationships allow Access to help us retrieve data across tables, check referential integrity, etc.

Figure 2.3 shows the patient data relationships in Access. It resembles the crow's feet model quite well. You define the relationships in this way:

1. Start in the database window and right-click somewhere.
2. Choose Relationships.

Now you see an empty Relationship Window. You have to tell Access which tables to show here. Some-times a Show Table window pops up by itself. Other-wise you have to invoke it with a right-click in the re-lationship window.

1. In the Show Table window, select the tables you want to include. In the hotel system it is all the tables.
2. Click Add and close the window. Now the tables should be in the relationship window.
3. Create the relationship between blood sugar and bone mineral density, breast report and basic physical quality by dragging patientID from one table to patientID in the other.
4. An edit-relationship window pops up. If not, right-click on the relationship connector and choose the edit window.

In the edit-relationship window, you can specify foreign keys that consist of several fields. You can also specify that the relationship has referential integrity, so that all records on the m-side point to a record on the 1-side.

1. In our case, all ID must point to a patient, so mark the connector enforce referential integrity. (If Access refuses this, it is most likely because you have not defined the foreign key as a long integer.)
2. Close the relationship window. The relationship connector now appears in the window between the foreign key and its target.

The referential integrity makes Access show the connector as 1-∞ (1:m). Based on referential integrity and whether the connected fields are primary keys, Access may also decide that it is a 1:1 relationship. It is not important what Access decides in these matters. You can later tell it otherwise when you want to use the connector.

3. Create the remaining relationships too.

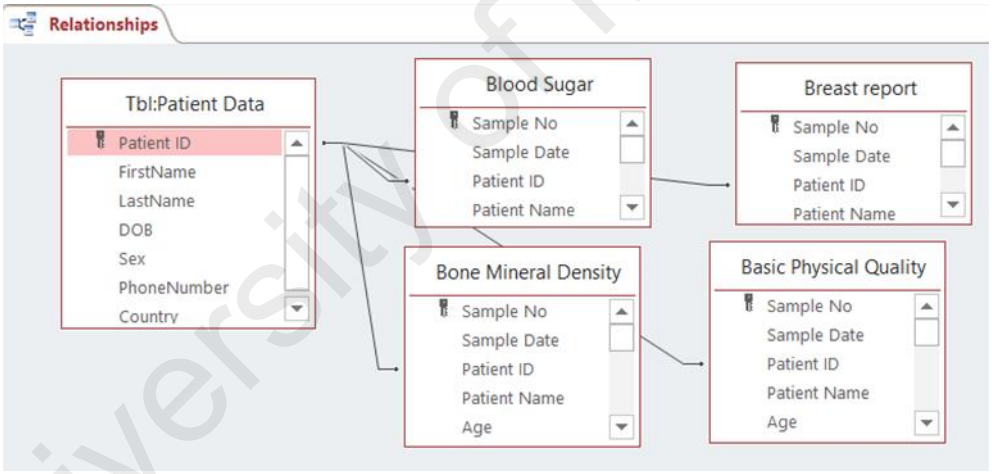


Figure 3. 6: Relationship Table

Query: join two tables

Create a query

1. Start in the database window. Select Queries and Create query in Design view. (In Access 2007 select New and then Design view.

2. Access asks you to select the tables you want to combine. Select patient and tblpatient. Click Add and then Close.

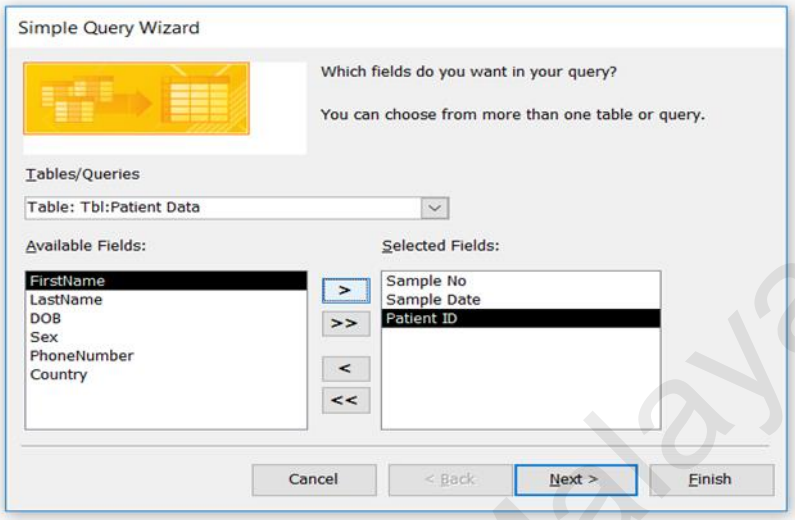


Figure 3. 7 Simple Query Wizard

Now we can see the query design window The top part of the window is an E/R-model, in our case consisting of tblID and tblpatientdata. Access has included the relationship from the full E/R-model. It shows that the tables will be combined according to patientID. This is just what we want in our case, but in other cases we have to remove the relationships we don't need and add new ones that we need for the query. These changed relationships are only used in the query; they don't influence the full E/R-model.

We may delete tables from the query window or add further tables by right-clicking in the E/R-model.

In the lower part of the window, we will see the query grid where we will make a column for each field in the computed table.

1. Drag patientID from tblID to the grid. Then drag name, address and phone from tblpatient. Finally, drag state from tblpatient. (We may also double-click the fields.)

   We may rearrange the columns by selecting a column and dragging it to another place.
2. Switch to datasheet view. The query table should look like the bottom of the figure. It contains all stays recorded in the database with patient information attached.
3. Save the query and give it the name qry1. (The standard prefix for queries is qry.)

Access has made a so-called join of tblID and tblpatient. According to the E/R-model, each record in tblID has a connecting string to a record in tblpatient. In the query table, there will be one record for each of these strings.

Since each query record corresponds to a string be-tween two source records, we can include arbitrary fields from both source tables. This is what we have done.

Star = all fields? Note that the data model at the top of the query window has a star in each box. It means "all fields". You may drag it to the grid and all source fields will be included in the query table. Assume that you drag the star from both tables. Then you will have two patientID fields in the result. You then have to refer to them as tblpatient.tblID and tblpatient.patientID. This leads to endless confusion later, particularly because some of Access's built-in Wizards cannot figure out about these names and screw things up.

Dynaset and data entry to query table

The query not only shows data, it can also be used for data entry. Try these experiments:

1. Open qrypatientList and tblpatient at the same time.
2. In the query table, change the name of one of the patient. As soon as we move the cursor to the next line, we will see the change in the query table as well as the patient table.
3. In tblpatient, try to change the patient name again. The query table will be updated immediately.

The query table we look at is a dynaset because it is updated automatically. We can enter data into it be-cause it is a simple query where Access can find out how to store the data into the source tables. For more complex queries, this is not possible.

The query has a property called Recordset Type. It is Dynaset as a standard, but we can change it to Snap-shot. Then Access computes the record list when we open the query, and doesn't update it dynamically. In this case we cannot enter data through the query.

How to find the Recordset Property? From the query design window, use View -> Properties. But don't change anything right now.

Adding/deleting records in a dynaset

1. In the query table, enter a patient name in the last line (with star-indication). When we move the cursor up, we have created a new patientt record (but not a new stay record). We cannot see it in tblpatient, but if we close and open tblpatient, we will see it. (Using the sort button A/Z on the tool-bar will also show the new patient.)

2. In the query table, enter a state in the last line and move the cursor up. Access refuses to do it. It tries to create a stay record, but lacks the foreign key to the patient and cannot preserve the referential integ-rity. If we had included the foreign key in the query, we could set it now and succeed. Remember to use Esc to get out of the in-consistent data update.

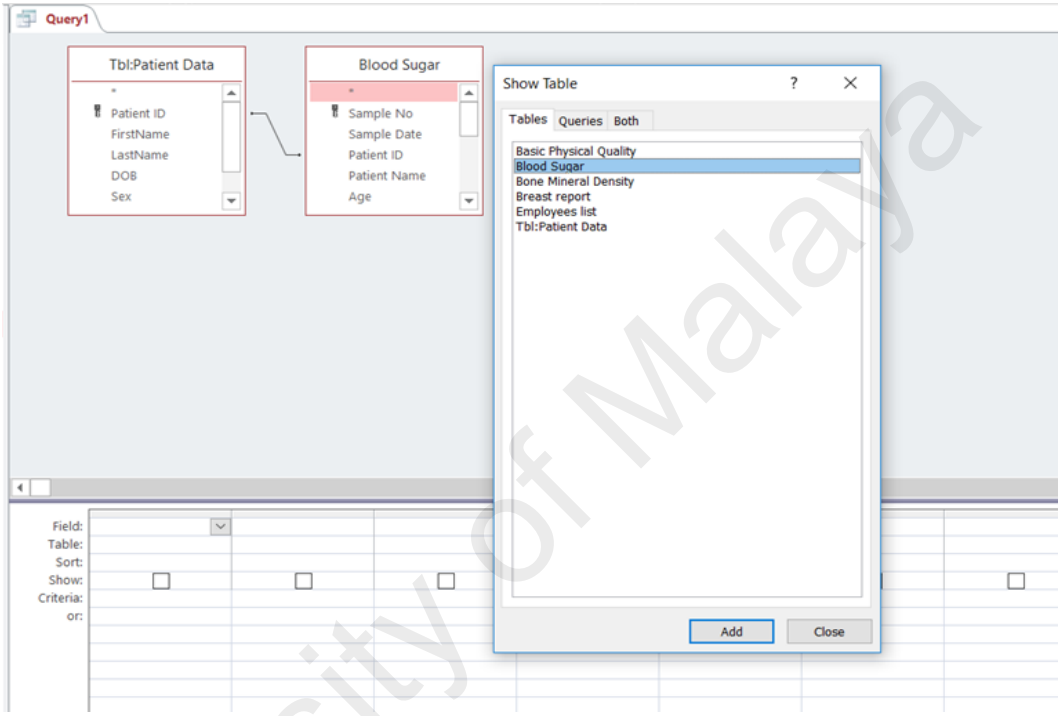


Figure 3. 8: Query 1

CHAPTER 4: RESULT

The Internet of Things (IoT) has been widely used to interconnect the available medical resources and offer smart, reliable, and effective healthcare service to the young and elderly people. Health monitoring for active and assisted living is one of the paradigms that can use the IoT advantages to improve the lifestyle of every people.

In this project, we had collected health information data from various hospitals and built Microsoft access database for healthcare environments for better presentation of the healthcare related data. By saving the database on the cloud we can to get remote access from anywhere and anytime to help the patients and health professionals in order to improve the services in the hospitals and clinical environments.

Figure 4.1 shows interface for the login page of the Health care facility. Upon putting the user name and password one can enter to the main page of the individual health professional login to the system.

Figure 4. 1: Main Login page interface

Figure 4.2: After clicking on the Doctor button put the doctor user name and password to get access for the doctor's panel.

Figure 4. 2: Doctor login interface

Figure 4.3 shows the doctor panel where doctor can put patient information, look for a test result, Diagnosis and input prescription in the interface.

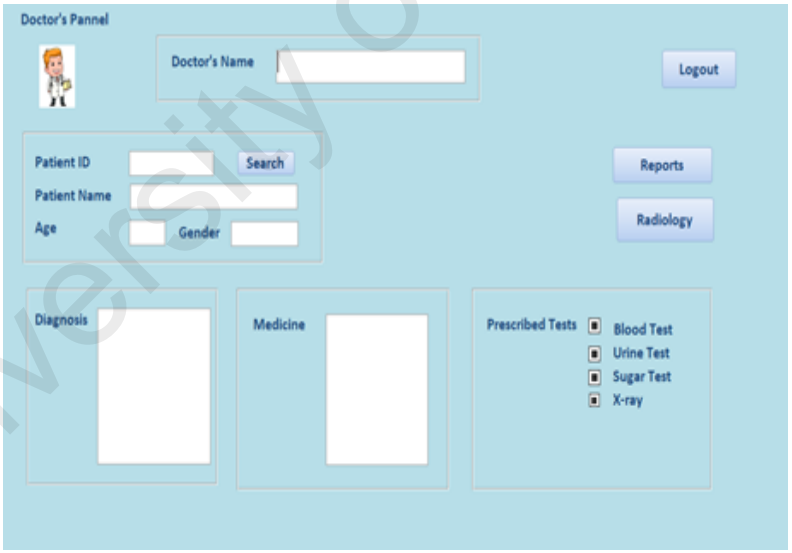


Figure 4. 3: Doctor's panel

Figure. 4.4: Analytical report contains patient information such as ID, Name, sex and Age. This page also contains different physical parameters like Basic physical quality, Blood sugar, Vitamin, Lung function and so on.

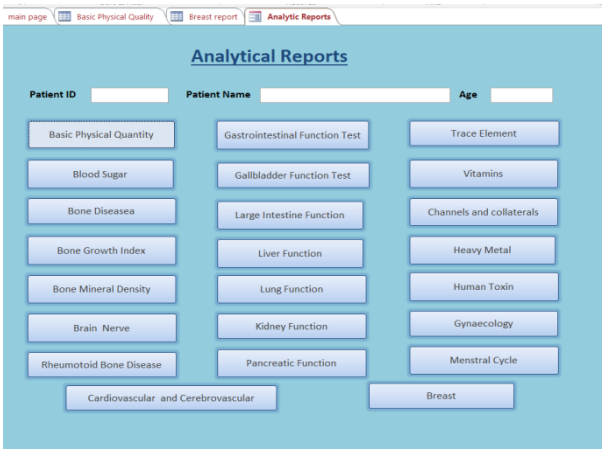


Figure 4. 4: Analytical Reports

Figure 4.5 shows results of different parameters and its indicate the status of the patients upon putting the actual measurements in the system.

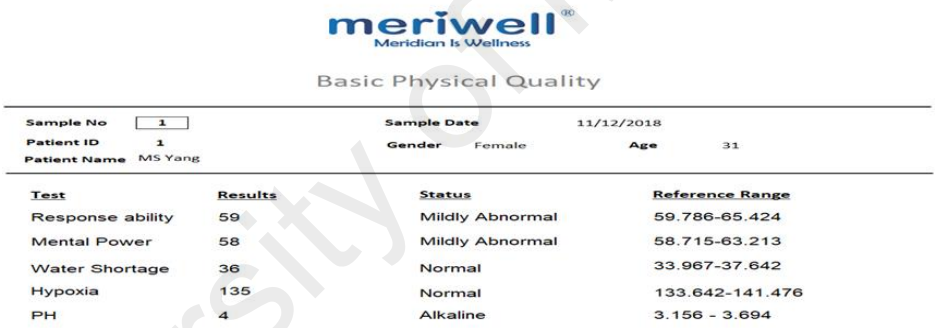


Figure 4. 5: Basic Physical Quality report

The IoT in healthcare will play a great role by adopting Microsoft access database management system and it will make healthcare systems much more easier than ever before for patient experiences and health professionals from collecting health related data to treatment plan. Advancement in low cost biosensors and IoT technology is helping a great innovation in healthcare and clinics. The device will become more and more compact to fit inside human skin in coming future at the same time the issue of cyber security and technology controlling our health will always remain our greatest concern.

CHAPTER 5: DISCUSSION

Healthcare Internet of Thing is a connected infrastructure of software applications and medical devices that can communicate with various healthcare IT systems. With a foundational mission to optimize for better health in a faster and easier environment, IoT in healthcare connects patients and healthcare providers via software and technology. The Internet of Things is an example of technology that helps physicians build better relationships with patients and cultivate their engagement in the process.

The Internet of Things can be discovered, monitored, controlled or interacted with by electronic devices which communicate over various networking interfaces, and eventually can be connected to the wider Internet to get the remote access from around the world.

Critical to the digital transformation of modern healthcare has been the rise of the internet of things (IoT), in regard to healthcare delivery and monitoring. An additional source of rich data, healthcare IoT devices also allow for more connected, remotely managed healthcare equipment that can directly feed data not only into individual treatment plans and patient records, but into larger AI-driven healthcare analytics systems.

In healthcare, IoT will solve the myriad problems by helping optimize the way things are done. With connected technology, providers will see fewer missed appointments, improved adherence to care plans and improved outcomes such as reduced inpatient admissions. Once fully adopted, IoT will align the shared goals of better health, lower costs and improved experience of all stakeholders in healthcare and clinical environments by enhancing patient experiences.

CHAPTER 6: CONCLUSION

IoT is a very interesting concept which creates many new possibilities in form of services and inventions. IoT is an enormously extensive concept that only has very general requirement postures or very specific solutions depending on how specifically you look at it.

There is a lot of research in many different areas involving IoT. Many different researchers have proposed many different kinds of adaptations to protocols and authentication methods for IoT which makes it very difficult to identify the best solution. Therefore, there is grave need of structured guidelines in the form of standardization in order to interconnect all kinds of devices, protocols, applications, etc. Developing standards or solutions needs to come with open source protocols and methods in order to attract wide acceptance and use. By trying to give an understanding of how such a standard should be developed and what requirements are needed, we hope that we have helped layer a foundation for further studies in the area.

The presented system is unique as a dedicated solution for managing patient-related data on the cloud and that utilizes both open hardware and open software resources for developing the hardware and software parts of the platform. Finally, further work will be devoted to the integration of runtime sensing information into health care records. Healthcare providers worldwide are among the most prolific generators of data, from patient records to drug trials. With this data increasingly being digitized as part of electronic patient record initiatives, it is getting easier for practitioners and their industry partners to leverage data to make more informed care decisions. This data is already used in a number of ways to understand historic events and help predict and understand current and future trends. Paired with the latest artificial intelligence (AI) algorithms, this data can drive intelligent decision-making and reasoning, speeding up

the analysis of data and providing healthcare organizations with more informed insight on which to make decisions about the patient conditions.

CHAPTER 7: FUTURE WORK

Wearable devices such as fitness trackers, blood glucose monitors and other connected medical devices have taken healthcare by storm. These devices have been embraced by the consumers and are being adopted by them for countless purposes, with or without prescription. Such wearable devices allow patients to manage and track sicknesses on their own. Today various parts of the body are connected to and monitored by 3.7 million medical devices in use, to facilitate informed healthcare decision making.

Many physicians and healthcare professionals have supported IoT as an effective patient engagement technology because of this widespread adoption. There have been a positive impact on supporting medication adherence, reducing patient readmissions and delivering home health support and monitoring, because of IoT devices.

Internet of Thing has a long way to go not only in healthcare industry but on all the paths it has tread so far and will be traversing in near future. Throughout the healthcare industry, its use is not as widespread as it has the potential to achieve, but it will come soon. As the sizes and prices of the devices go down, rapid scaling of these technologies will take place. Internet of Thing in healthcare is set to radically change the way healthcare sees the management of inventory, the optimization of workflow and the integration of devices. The digital transformation of the healthcare industry, among others, will most certainly be brought about by what is now being called the Internet of Healthcare Things (IoHT) and implementation of Artificial Intelligence.

REFERENCES

Adnane, M., Z. Jiang, S. Choi, and H. Jang. (2009). Detecting specific health-related events using an integrated sensor system for vital sign monitoring. Sensors, 9(9):6897-6912.

APHM (Association of Private Hospitals Malaysia) (2007). website Available from: http://www.hospitalsmalaysia. org/index.cfm (Accessed 13.12.08)

Ashton, K. (2009). That "Internet of Things" Thing. RFiD Journal, 4986. Retrieved from http://www.rfidjournal.com/articles/view?4986

Castellani. A. P., M. Gheda, N. Bui, M. Rossi, and M. Zorzi.(2011) Web Services for the Internet of Things through CoAP and EXI. In Proc. of IEEE ICC RWFI Workshop, Kyoto, Japan.

Chee H. L. Ownership, (2008) control, and contention: Challenge for the future of healthcare in Malaysia. Social Science & Medicine.66: 2145-2156.

Charalampos Doukas, Ilias Maglogiannis. (2012). Bringing IoT and Cloud Computing towards Pervasive Healthcare, Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.

Economic Planning Unit. (2004). Prime Minister's Department. Malaysia: 30 years of poverty reduction, growth, and racial harmony. A Global Learning Process and Conference, Shanghai, May 25-27. A World Bank report.

Gomez E.T. & Jomo K.S. (1999) Malaysia's political economy: politics, patronage and profits. Cambridge. Cambridge University Press.

Grimson, J., G. Stephens, B. Jung, W. Grimson, D. Berry, and S. Pardon. (2001). Sharing health-care records over the internet. IEEE Internet Computing, 5(3):49-58.

He, W., Yan, G., Xu, L.D.(2014). Developing vehicular data cloud services in the IoT environment. IEEE Trans. Industr. Inf. 10(2), 1587–1595.

Joe Fernandez. (2009). Politicians ticked off over KK hospital woes. http://www.malaysiakini.com/news/103275

Luca Catarinucci, Danilo de Donno, Luca Mainetti, Luca Palano, Luigi Patrono, Maria Laura Stefanizzi, and Luciano Tarricone, (2015). An IoT-Aware Architecture for Smart Healthcare Systems, IEEE internet of things journal, VOL. 2(6)

Mastura Ismail. (2008)The New Team for Nationals SCHOMOS 2008/2009. MMA News, (June), Vol. 38 (5):pg 13-14.

Mastura Ismail. (2008) Budget 2009 Increment of Specialist Allowance. MMA News, (October), Vol. 38 (9):pg14.

Ma, M., Wang, P., Chu, C.H.(2013) Data management for Internet of Things: challenges, approaches and opportunities. IEEE Cyber, Physical and Social Computing, pp. 1144–1151.

Miorandi, D.; Sicari, S.; Pellegrini, F. D.; Chlamtac. (2012) I. Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 10(7), 1497-1516.

Merican M. I. (2007). Medicine and Healthcare in 2020. Berita Academi, Vol 16;3, Pg.2.

MOH, (Ministry of Health) (2003b, 2004). Indicators for monitoring and evaluation of strategy for health for all.

MMA (Malaysian Medical Association). (1999). Health for All: Reforming Health Care in Malaysia. Academe Art & Printing Services, Selangor.

Nicola Bui and Michele Zorzi, Health Care Applications: A Solution Based on The Internet of Things, European Commission through the FP7 EU projects\Internet of Things Architecture (IoT-A)" (G.A. no. 257521,

Ong H. T. (2008). Private Healthcare Facilities and Services Act. (Letters to Editor). MMA News, Vol. 38 (9):pg23.

PCNB. (1998). Private Health Care Facilities and Services Act 1998 (Act 586). PCNB, Malaysia.

PCNB, (2006). Private Health Care Facilities and Services Regulations (P.U. (A) 137/2006). Malaysia.

Quek D. K. L. (2006). Regulations now Enforceable—Cui Bono? (Who Benefits?). MMA News, Vol. 36 (6):pg7.

Quek D. K. L. (2007). Physicians under Siege: Sensing the Pulse of Doctors… MMA News, Vol. 37 (2):pg7.

Quek D. K. L. (2008). Equitable Access to Health Care for All: Is this still a Pipe Dream for Malaysians? A Medical Professional's Perspective. Paper presented at Suhakam's "Human Rights & Access to Equitable Healthcare" Dialogue, Kota Kinabalu, Sabah, 08 January

Rajesh. S. M. (2013) "Integration of active RFID and WSN for real time low cost data monitoring of patients in hospitals," in Proc. Int. Conf. Control Autom. Robot. Embedded Syst.

Tennina, S. et al., (2014). "WSN4QoL: AWSN-oriented healthcare system architecture," Int. J. Distrib. Sensor Netw., vol. 2014, pp. 1–16.

Tung-Cheng; Chang, Hong-Jer; Huang, Chung-Chien. (2011). An Analysis of Telemedicine in Taiwan: A Business Model Perspective Original. International Journal of Gerontology, Vol.5(4), Pp189-192.

Uckelmann, Dieter; Harrison, Mark; Michahelles, Florian. (2011). Architecting the Internet of Things. Springer-Verlag Berlin Heidelberg.

WHO. (2006). The World Health Report: Working together for health. Geneva.

WHO. (2011) New Horizon for Health Through Mobile Technologies, Global Observatory for e-Health Services, vol. 3. Geneva, Switzerl