Acta Scientific COMPUTER SCIENCES

Volume 4 Issue 12 December 2022

Research Article

Secure IoT Software Application Development Model for Security Requirement Elicitation

Asma Asdayana Ibrahim[1]* and Massila Kamalrudin[2]

[1]Sultan Azlan Shah Polytechnic, Behrang Stesyen, Perak, Malaysia

[2]Innovative Software System and Service Group, Universiti Teknikal Malaysia Melaka, Malaysia

***Corresponding Author:** Asma Asdayana Ibrahim, Sultan Azlan Shah Polytechnic, Behrang Stesyen, Perak, Malaysia.

Received: September 28, 2022

Published: November 29, 2022

Abstract

The term Internet of Things (IoT) generally refers to situation where network connectivity and computing capability are extended to objects, sensors and common household items that are not typically thoughts as computers, allowing these devices to generate exchange and consume data with few human intervention. We are currently living in the Internet of Things era, in which digitally connected devices are infiltrating every aspect of our lives, including tools, workplaces, transportation, and others. Connecting such a large number of devices will be one of the most difficult challenges of the future of IoT, challenging the very structure of current communication networks and underlying technologies. Currently, it is necessary to rely on the centralized, server/client paradigm to authenticate, authorize, and connect various nodes in a system. Providing requirement for the security for this giant technology is also really challenging, mainly because there is not boundary or limitation on the way that it can go. Therefore, considering eliciting security requirements from early development of IoT application is crucial. To do this, determination of the most important security requirements and IoT technologies need to be done to define correct requirements is produced. In this paper, we discussed our findings of study conducted to analyses the relationship dan correlation between security requirements and IoT technologies for developing secure IoT applications based on perspectives of the users. This study was carried out 101 of respondents from IoT industries in Malaysia. The results indicated most of them were a significant relationship between security requirements and IoT technologies with IoT application. Then, a Secure IoT Application Development (SecIoTA) model is proposed.

Keywords: Internet of Things (IoT); IoT Applications; Security Requirement; IoT Technologies; Reliability Test; Correlation Analysis; IoT Model

Introduction

The Internet of things (IoT) is the network of devices such as vehicles, and home appliances that contain electronics, software, actuators, and connectivity, allowing them to connect, interact and exchange data. The IoT involves extending Internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internet-enabled physical devices and everyday objects [1]. These gadgets have technology built into them, so they can interact and communicate online and be monitored and controlled from a distance. There are currently over 23 billion IoT-connected devices worldwide. By 2020, this number will increase even further, reaching 30 billion, and by the end of 2025, it will exceed 60 billion [2-4]. There are a number of security issues and concerns that arise with the increased use of IoT-connected devices and the development of IoT applications. A system or application with so many components that can be randomly merged in different systems at different times and places is the most severe requirements engineering challenge, particularly in terms of defining security and privacy needs. It is challenging to even imagine what system

an object will be a part of given the diversity and complexity of the IoT. As a result, we investigate IoT security requirements in the early stages to assist users in understanding the various facets and aspects of security requirements [5,6], and to assist developers in properly handling them.

Furthermore, capturing security requirements early in the system development process is critical for building public trust and facilitating the adoption of novel systems such as the Internet of Things. However, security requirements are frequently mishandled due to their numerous facets and aspects, which make them difficult to formulate. Most requirements engineers are lack adequate training to elicit, analyse, and specify security requirements, frequently conflating them with the architectural security mechanisms that are traditionally used to meet them [7]. They thus end up specifying architecture and design constraints rather than true security requirements. Moreover, IoT security may raise critical issues that the IoT device, service is adopted everywhere in our real lives and security problems can cause not only data breach or monetary damages but also threatening our lives. In this regard, security requirements for IoT should be identified to make a secure and safe IoT application. Existing studies tend to focus on finding security issues in the technical perspective [8-10]. However, understanding the security issues that may arise during the development and implementation of IoT is critical. As a result, our research focuses on determining security requirements in IoT applications by taking into account IoT technologies and security requirements.

Furthermore, even though the full scope and nature of the IoT's potential effects are still unknown, they may have a considerable impact on many elements of the economy and society. According to many analysts, the development of the IoT will improve productivity, efficiency, and integration across numerous industries and the global economy. Agriculture, energy, health care, manufacturing, and transportation are frequently mentioned [11-13]. Additionally, there may be significant effects on urban development, infrastructure, and consumer spending in general. IoT advancements could, however, be hampered by technical and policy obstacles, such as security and privacy concerns. IoT applications have recently received praise for having the potential to be transformative. Indeed, modern technology are being used for a wide range of objectives across many different industry. However, due to difficulties with both technical and policy issues, it is still unclear how IoT will develop. Lack of new Internet addresses under the most popular protocol, the availability of high-speed and wireless connectivity, and a lack of agreement on technical standards are some notable technical constraints that could hinder the development and use of the IoT [1].

This paper presents the results on relationship between security requirements and IoT technologies that address user perspectives on developing secure IoT applications. The rest of this paper is organized as follows: Section 2, we discussed the background and motivation. Next in Section 3, we explained the methodology. In Section 4, we discussed the results from the survey conducted. Then in Section 5, we explained the model and Section 6, limitation of the study. And finally, this paper end with Section 7 with the conclusion and propose agenda for future work.

Background and motivation

Definition of requirements

The requirements engineering of a business, system or software application, component, or (contact, data, or reuse) centre entails far more than just engineering its functional requirements. Quality, data, and interface requirements, as well as architectural, design, implementation, and testing constraints, must all be engineered. While some requirements engineers may remember to elicit, analyse, specify, and manage quality requirements such as interoperability, operational availability, performance, portability, reliability, and usability, many do not [7].

Requirements imply that there is someone out there requiring - a specific user who knows what she wants. In some projects, requirements are defined as a list of features (or functions, properties, constraints, and so on) requested by the user. In practise, there is rarely a single user, but rather a diverse group of people who will be impacted by the system in some way. These individuals may have disparate and conflicting goals. Their objectives may be oblique or difficult to articulate. They may be unsure of what they want or what is feasible. In these circumstances, asking them what they "require" is unlikely to be fruitful [14]. A system's requirements are descriptions of what the system should do, the services it provides, and the constraints on its operation. These requirements reflect users' needs for a system that performs a specific function, such as controlling a device, placing an order, or finding

information [15]. Requirements engineering (RE) is the term for the process of discovering, examining, documenting, and verifying these services and restrictions.

There are two types of requirements: functional requirements and non-functional requirements. A system feature or functionality that is directly visible to external system users is referred to as a functional requirement. A non-functional requirement is a system feature that is hidden from system users. It may, however, have an effect on the quality of visible system features of functional requirements. Meanwhile, requirement elicitation is the process of deriving system requirements from existing systems, discussions with potential users and procurers, task analysis, and so on [15]. This could entail creating one or more system models and prototypes. These assist users in comprehending the system to be specified.

Security requirements

A security requirement is a security feature that system users must have or a quality that the system must have in order to increase the users' trust in the system. A security requirement can also be defined as a system specification with required security, which includes the types and levels of protection required for the systems' data, information, and applications [16]. In general, a security requirement is considered as a non-functional requirement. In addition, Ibrahim and Kamalrudin [5] conducted a systematic literature review to identify and analyse related literature on the elicitation of security requirements for IoT applications. According to previous research, there are six security requirements: authentication, confidentiality, integrity, authorization, access control, and availability. The description of security requirements is described in table 1.

IoT technologies

The Internet of Things (IoT), which is the internet based on the integration of numerous technologies integrated application, will gradually become the primary body of the next generation of information network [23]. With the IoT, all of the objects in our environment may communicate with one another over the Internet. The Internet of Things (IoT) encompasses a lot more than only machine-to-machine communication, wireless sensor networks, sensor networks, 2G, 3G, and 4G networks, GSM, GPRS, RFID, WI-FI, GPS, Bluetooth, microcontrollers, and other components [24]. The

Table 1: Description of Security Requirements.

Security requirement	Description	Examples of Attributes
Authentication	Authentication is the process of identifying users, devices, applications, and restricting access to authorized users and non-manipulated devices or services. It is the process of determining whether someone or something is, in fact, who or what it declares itself to be [4,7,5,17-19].	Username Password PIN ID card Fingerprint Retinal pattern Biometric identifier
Authorization	Authorization is the process of verifying that you have access to something and gaining access to a resource because the permissions configured on it allow you access. It is a process to grant an access of a subject, such as a human user or a client entity, to an object, such as a file or a server entity [7,5,17,20].	Permission Verify Gain access
Availability	Availability is the process that refers to the ability to make information and related physical and logical resources accessible as needed, when they are needed, and where they are needed. The user has ability to access information or resources in a particular location and in the correct format. This process ensures that an authorized party can access information when required [5,19].	Accessible Obtainable Software patching
Confidentiality	Confidentiality is a set of rules that limits access to information. The process is to ensure that the data is only readable by the proposed destination. The information is not made available or disclosed to unauthorized individuals, entities, or processes [4,5,19].	Limits access Unreadable data Restricted access
Integrity	Integrity is the process to protect data or information from being modified by unauthorized parties. The data has not been altered or destroyed in an unauthorized manner [7,5,19].	Protect data Unmodified data Unaltered data
Access control	Access Control is an ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual [5,19].	Limited access Control the access Dicretionary Mandatory Roled-based

Trust	The obligation or responsibility imposed on a person in whom confidence or authority is placed: a position of trust, charge, custody, or care: to leave valuables in someone's trust, something committed or entrusted to one's care for use or safekeeping, as an office, duty, or the like; responsibility; charge [21,22].	Disposition Institution-based Beliefs Intention

most popular IoT technologies, according to Ibrahim and Kamalrudin [5], include sensors, mobility networks, RFID systems, Wi-Fi, Bluetooth, and ZigBee. The description of the IoT technologies as shown in table 2.

Hypothesis development

Although there is no direct empirical evidence depicting the relationship between security requirement and IoT technologies,

Table 2: Description of IoT Technologies.

IoT Technologies	Description	Attributes/Devices
Sensor	A sensor is a device that detects and responds to some type of input from the physical environment. The specific input could be light, heat, motion, moisture, pressure, or any one of a great number of other environmental phenomena [5,25].	Temperature Vibration Motion Current detection
Mobile networks	Mobile computing, a generic term describing one's ability to use technology untethered, but often used to refer to access to information or applications from occasionally-connected, portable, networked computing devices [5,26,27].	North coordinate East coordinate Altitude Signals Locator Identifier Tracker Mobility Connection density Spectral efficiency Latency Peak data rate
RFID system	RFID (Radio Frequency Identification) is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or a person [5,28,29,30].	RFID tags/transponder RFID readers
Wi-Fi	Wi-Fi is technology for radio wireless local area networking of devices on IEEE 802.11 standards. Devices that can use Wi-Fi technologies include desktops and laptops, video game consoles, smartphones and tablets, smart TVs, digital audio players and modern printers. Wi-Fi compatible devices can connect to the Internet via a WLAN and a wireless access point [5,31].	Access point Scalability
Bluetooth	Bluetooth is the wireless communications technology for developers which allows devices to communicate with each other without the need for a central device like a router or access point. Bluetooth has a special low energy feature which means it can be used without requiring much power from the devices using it [5,32].	Packet-based Access point-centered Firmware binary Peer-to-peer communication
ZigBee	ZigBee is a standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks [5].	Persistent Memory Storage Singleton

several previous studies have implied such relationships indirectly. Based on related literatures [5], the following section further explores the relationship between the research variables and the development of the hypothesis.

We found that there are relationship between security requirements and the development of secure IoT applications. To guarantee a secure IoT application, security requirement such as confidentiality, integrity, authentication, authorization, availability and access control must be assured for entire IoT application development.

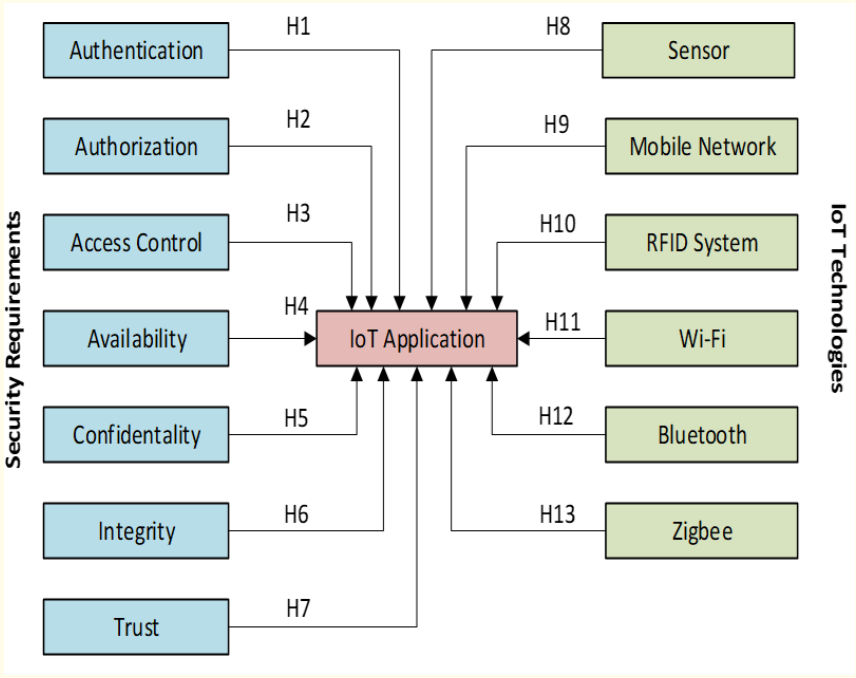

Figure 1: The Proposed Research Hypothesis.

- **The first hypothesis "H_1:** Authentication requirement (AUT) has a significant relationship with the IoT application development" to determine if the authentication requirements has an effect in developing secure IoT application. Authentication is the process of checking the originality of the user or entity participating in the communication [33]. It works along with integrity, confidentiality and authorization. Though the amount of devices connected to internet is keep on increasing, scalability posts a big threat to the authentication of devices. It is important to propose a mechanism or an architecture that will securely handle the adaptability of hardware in IoT environment. It requires appropriate authentication infrastructures for IoT scenarios.
- **The second hypothesis "H_2:** Authorization requirement (ATH) has a significant relationship with the IoT application development" is to determine if the authorization has an effect in developing secure IoT application. Authorization is the permitting any user or device to avail the information from the IoT environment [34]. Permission is delivered with the device or user's identity. With proper identity, anybody can access the information from the IoT environment. Without authorization, no one can access any data or service from this environment. Therefore, efficient authorization mechanism is the need of the hour for IoT environment and tightening of identity verification is another challenge.

- **The third hypothesis "H_3:** Access control requirement (ACC) has a significant relationship with the IoT application development" is to determine if access control requirement has an effect in developing secure IoT application. Access control should be enforced at each of these interfaces in this complex IoT ecosystem. The majority of IoT frameworks impose coarse-grained access control policies [35]. A fine-grained authorization mechanism that limits access to IoT device interfaces and data to authorised users only should be built to meet these limitations. The capabilities of smart devices, connections between users of the devices, and environmental elements like time and location should all be taken into account by such a system for enforcing laws.

- **The fourth hypothesis "H_4:** Availability requirement (AVA) has a significant relationship with the IoT application development" is to determine if availability requirement has an effect in developing secure IoT application. IoT availability involves recoverability and reliability [36]. By highly distributed nature of IoT environment, an explosive amount of data are available everywhere. Everyone, every device can generate data when they are connected with internet and try to store the data anywhere. Therefore, anyone can be tracked or traced without their assent or their insight. Proper algorithm has to be developed to ensure the availability of data and services in the IoT environment.

- **The fifth hypothesis "H_5:** Confidentiality requirement (CON) has a significant relationship with the IoT application development" is to determine if confidentiality requirement has an effect in developing secure IoT application. It guarantees the authorized entities to access and modify data. In IoT environment, authorization is given not only to the users, but also to the objects [37]. Confidentiality needs to address two important concepts such as defining an access control mechanism and an object authentication process. Description of a proper query language for permitting applications to recover the desired information out of a data stream will be another issue related to data confidentiality in an IoT scenario.

- **The sixth hypothesis "H_6:** Integrity requirement (INT) has a significant relationship the IoT application development" is to determine if integrity requirement has an effect in developing secure IoT application. It is nothing but veracity, honesty and reliability. As the devices and users connected to the IoT environment become countless, integrity becomes a core issue with reference to security. Integrity is the guarantee that the data received has not been altered while in transit [38]. The devices' identities are complicated, making it incredibly challenging to pinpoint the data's original source. The usage of reliable tools and information is a muddle. In IoT technologies, data protection through passwords is insufficient, and trusted computing solutions must be built to preserve the integrity of data and devices.

- **The seventh hypothesis "H_7:** Trust requirement (TRU) has a significant relationship with the IoT application development" is to determine if trust requirement has an effect in developing secure IoT application. Trust is defined as the belief and expectation of an entity's dependability, integrity, security, and ability [22]. Trust is an important concept that should be implemented in IoT because of its utility in securing object-to-object communication, such as assisting objects in selecting another trustworthy object during communication [39]. Meanwhile, reputation is used to determine the level of trust, and it can be measured based on prior knowledge of the interaction with other objects as well as other objects' experiences. Reputation can also be used to assess an object's level of trustworthiness. In the IoT, a dynamic trust mechanism is useful for the object as a control for selecting application services. We explored many connectivity technologies including WiFi, Bluetooth, and LPWANs. The reason we have so many options for connectivity is because IoT applications can differ drastically, meaning varying requirements.

- **The eighth hypothesis "H_8:** Sensor technology (SEN) has a significant relationship with the IoT application development" is to determine if sensor technology (SEN) has an effect in developing secure IoT application. The real-world variable that sensors are designed to measure is transformed into a digital data stream for transmission to a gateway [40]. Industries and organizations have traditionally used a variety of sensors, but the advent of the IoT has brought sensor development to an entirely new level. IoT platforms use a range of sensors to operate and offer different types of information and data. They collect data, push it, and share it with a network of connected devices. All of this collected data enables

devices to function autonomously, and the entire ecosystem is becoming "smarter" by the day [41]. Devices share information with one another and improve their effectiveness and functionality by combining a set of sensors and a communication network.

- **The ninth hypothesis "H_9:** Mobile Networks technology (MOB) has a significant relationship the IoT application development" is to determine if mobile networks technology (MOB) has an effect in developing secure IoT application. In many IoT applications, mobile networks, commonly referred to as cellular networks, play a crucial and expanding role. A cellular network is a radio communication network that spans numerous cells, or geographic regions, in a given location. Each cell is described as the physical area that at least one fixed-position transceiver, but frequently three base transceiver stations, serves. These cell sites provide coverage for voice or data packets sent within the cell. Different types of wireless devices, including smartphones, tablets, and laptops with portable modems, interact with one another and with base transceiver stations while moving across one or more fixed cells. In order to accomplish authentication and authorization of services, the cellular networks are therefore dependent on service providers and their network architecture. Data must be delivered with distinct frequencies among neighboring cells in order to prevent interference and ensure network security.

- **The tenth hypothesis "H_{10}:** RFID technology (RFI) has a significant relationship with the IoT application development" is to determine RFID technology (RFI) has an effect in developing secure IoT application. Radio Frequency Identification (RFID) is frequently viewed as a requirement for the Internet of Things (IoT). All common household items might be detected and inventoried by computers if they were given radio tags. Tags (transmitters/responders) and readers (transmitters/receivers) are the basic components of an RFID system [30]. One of the major IoT potential, which will profoundly and substantially alter the world, is RFID [42]. The RFID readers located all over the world can recognise, track, and monitor the items attached with tags globally, automatically, and in real time, as needed, when they are connected to an Internet terminal and follow the proper communication protocols [43]. In the near future, IoT will emerge as a global network, connecting every object around us. RFID technology provides a platform for resolving this issue through the use of RFID tags. RFID tags have a unique identification number and can be attached to or embedded in an object. The use of RFID tags in IoT allows for the management of unique identification for trillions of objects that are expected to be connected in the IoT.

- **The eleventh hypothesis "H_{11}:** Wi-Fi technology (WIF) has a significant relationship with the IoT application development" is to determine Wi-Fi technology (WIF) has an effect in developing secure IoT application. Some IoT applications, including home and building automation or internal energy management, can benefit from WiFi. WiFi can transfer large amounts of data for many additional Internet of Things applications, but at the expense of high energy consumption and limited range. For Internet of Things (IoT) applications that don't have to worry about power consumption (things that are plugged into an outlet), send a lot of data (like video), and don't require high range, WiFi can be beneficial. A home security system is a wonderful illustration.

- **The twelfth hypothesis "$H1_2$:** Bluetooth technology (BLU) has a significant relationship with the IoT application development" is to determine Bluetooth technology (BLU) has an effect in developing secure IoT application. Bluetooth is crucial for the rapidly expanding Internet of Things (IoT), which includes industrial and smart home applications. Bluetooth was designed for portable devices and related uses. When two devices can communicate with little configuration, it's fantastic. Additionally, Bluetooth devices may communicate in "noisy" surroundings with less interference because it uses weak signals. For IoT applications, Bluetooth is ideal for this reason. The Bluetooth Low Energy (LE) specification found in Bluetooth v4.0 is one of the few available energy- and communication-constrained technologies. Bluetooth LE, in addition to combining a standardized communication technology designed for low- power systems and a new sensor-based data collection framework, offers easy integration with most handheld IoT devices (such as smartphones and tablets), something that conventional wireless sensor networks are still working towards [44].

- **The thirteenth hypothesis "H_{13}:** ZigBee technology (ZIG) has a significant relationship with the IoT application development" is to determine ZigBee technology (ZIG) has an effect in developing secure IoT application. ZigBee is an open standard for low-data-rate, low-power applications [45]. ZigBee uses a mesh networking protocol and substantially lower data rates in IoT application development to avoid hub devices and produce a self-healing architecture. The properties of ZigBee set it distinct from other potential IoT protocols and enable it to carve out a niche for itself in the industry. Because of its mesh topography, it can operate over longer distances than Bluetooth LE, and Wi-Fi is less IoT-friendly than it could be. While this theory allows for the mixing of implementations from various manufacturers, in reality firms have expanded and personalized ZigBee products, which causes interoperability problems.

Methodology

Data collection

This study was conducted to determine and analyze the variables of the seven (7) security requirements and six (6) IoT technologies. The Likert scale was use from 1 (strongly disagree) to 5 (strongly agree) in the survey. This study was done to 101 respondents of software professionals and experts with various positions in IoT organizations in Malaysia mostly located at Klang Valley. The survey was conducted through online and face to face. The survey was organized into three sections. First section consist of participant's background and two other section that consists of multiple-choice questions, focusing on security requirements and IoT technologies. Before the survey, two academic experts and one industry expert have validated and reviewed the questionnaires and they gave opinion and idea on the contents related to security requirements and IoT technologies.

Data analysis

The data was analyzed using SPSS version 25 consisting of descriptive analysis, reliability test, and correlation and regression analysis. Descriptive analysis is use to analyze the general information, which is profile of the respondents. Reliability test is use to analyze the reliability of the question to generate accurate results. Through the reliability analysis, we know the designed questionnaire is acceptable or unacceptable. Then, correlation and regression analysis is use to test the strong relationship between the variables.

Results

Respondent profile

Table 3 shows the profile of the respondents. Majority of the respondents are 57 males with 56.44%, while frequencies of 44 female respondents are 43.56%. In addition, 63 of the respondents are in age 30 - 49 years with 62.38%, 13.86% of the respondents are in age 18 - 29 years and only 3.96% of the respondents in age 50 - 64 years. Based on the results, responding holding bachelor degree are 61 respondents with 60.40%, while 21 respondents with 20.79% holding diploma. The rest of the respondents is 16.83% master qualification and 1.98% were PhD holder. Table 4 also shows the position of the respondents. Majority of the respondents are IoT/Software Developer with 41.58%. Meanwhile, 37.62% of the respondents are in Software Engineer. The rests of the respondents are 9.90% in System Analyst and 6.93% are Programmer. The percentage of System Engineer and others are same, which is 1.98%, each position.

Table 3: Demographic Profile.

Item		Frequency	Percentage (%)
Gender	Male	57	56.44
	Female	44	43.56
Age	18 - 29 years	14	13.86
	30 - 49 years	63	62.38
	50 - 64 years	4	3.96
Education level	Diploma	21	20.79
	Bachelor	61	60.40
	Master	17	16.83
	PhD	2	1.98
Position	IoT/Software Developer	42	41.58
	Software Engineer	38	37.62
	System Analyst	10	9.90
	System Engineer	2	1.98
	Programmer	7	6.93
	Others	2	1.98

Reliability test

Reliability test is the used to analyses the reliability of the question to generate accurate results. Through the reliability analysis, the researcher can know the designed questionnaire is acceptable or unacceptable. In the table 4 present the alpha coefficient of in which all attributes were accepted required level of 0.7 and above suggested by George and Mallery [5]. The data is only acceptable if the Cronbach's Alpha coefficient is higher than 0.7. If the Cronbach's Alpha coefficient is higher than 0.8, then they are considered as a good reliability. Furthermore, the excellent reliability of the questionnaire will have the Cronbach's Alpha coefficient which is higher than 0.9.

The scale Cronbach's Alpha values for all study variables are between ranges 0.829 - 0.986 which show a good and an excellent level as the minimum acceptable level is 0.70. The scale Cronbach's Alpha for variable (AUT = 0. 887). The scale Cronbach's Alpha for variable (ATH = 0.899). The scale Cronbach's Alpha for variable (AVA = 0.929). The scale Cronbach's Alpha for variable (CON = 0.912). The scale Cronbach's Alpha for variable (INT = 0. 933). The scale Cronbach's Alpha for variable (ACC = 0.911). The scale Cronbach's Alpha for variable (TRU = 0.837). The scale Cronbach's Alpha for variable (SEN = 0.986). The scale Cronbach's Alpha for variable (MOB = 0.829). The scale Cronbach's Alpha for variable (RFI = 0.856). The scale Cronbach's Alpha for variable (WIF = 0.882). The scale Cronbach's Alpha for variable (BLU = 0.876). The scale Cronbach's Alpha for variable (ZIG = 0.941). The result of reliability test showed that the item measured are reliable. Table 5 shows the Cronbach's Alpha values for all variables.

Descriptive statistics of research variables

Descriptive analysis was adopted to test the hypothesis. For this purpose, the variables were analyzed based on mean and standard deviation values. The variables involved in this descriptive analysis are: Authentication, Authorization, Availability, Confidentiality, Integrity, Access control and Trust, Sensor, Mobile networks, RFID system, Wi-Fi, Bluetooth and ZigBee. The mean value for the variables involved was interpreted according to Salleh., *et al*. (2012) as shown in table 6.

Table 4: Reliability Test.

Variables	Cronbach's Alpha	Reliability
Authentication (AUT)	0.887	Good
Authorization (ATH)	0.899	Good
Availability (AVA)	0.929	Excellent
Confidentiality (CON)	0.912	Excellent
Integrity (INT)	0.933	Excellent
Access control (ACC)	0.911	Excellent
Trust (TRU)	0.837	Good
Sensor (SEN)	0.986	Excellent
Mobile networks (MOB)	0.829	Good
RFID system (RFI)	0.856	Good
Wi-Fi (WIF)	0.882	Good
Bluetooth (BLU)	0.941	Excellent
ZigBee (ZIG)	0.876	Good

Table 5: Mean Scores (Salleh., *et al*. 2012).

Mean scores	Interpretation
0.10-1.80	Strongly Disagree/very dissatisfied
1.81-2.60	Disagree/Dissatisfied
2.61-3.40	Moderate Agreement/Moderate Satisfies
3.41-4.20	Agree/Satisfied
4.21-5.00	Strongly Agree/very Satisfied

Table 7 presents the mean values for the thirteen variables of the study. The results shown that the range of mean values was between 3.2504 and 3.9637. Specifically, the highest mean value for security requirements was authentication requirement (3.9637). This is followed by authorization requirement (3.9076), access control requirement (3.7921), availability requirement (3.7558), trust requirement (3.4208), integrity requirement (3.3663) and confidentiality requirement (3.2504). Meanwhile, mean value for IoT technologies was mobile network technology (3.9010), RFID system technology (3.8713), Bluetooth technology (3.5578), sensor technology (3.3980), ZigBee technology (3.3505) and Wi-Fi technology (3.2059). All these values show positive values indicating that respondents agreed and satisfied with all variables.

Table 6: Descriptive Statistics of Research Variables.

Variables		Mean	Std. Deviation
Security Requirements	Authentication	3.9637	0.5810
	Authorization	3.9076	0.3648
	Availability	3.7558	0.3805
	Confidentiality	3.2504	0.4152
	Integrity	3.3663	0.4784
	Access control	3.7921	0.4317
	Trust	3.4208	0.4964
IoT Technologies	Sensor	3.3980	0.4433
	Mobile networks	3.9010	0.3242
	RFID system	3.8713	0.5033
	Wi-Fi	3.2059	0.3638
	Bluetooth	3.5578	0.5698
	ZigBee	3.3505	0.4919
IoT Domain		3.8465	0.36869

Correlation analysis

After conducting the reliability analysis, this study inspected the correlation coefficients to discover the relationship between thirteen (13) variables and investigate the hypothesis of the research model. The Pearson's Correlation was used to measure the strength of the relationship between security requirements and IoT technologies with IoT Application. The analysis tool is also SPSS v25. The Pearson correlation coefficient was included to justify and conclude the regression analysis presented in Table 8. In the addition to 2-tailed significance indicator selected for the analysis, the rules for determining the direction of the relationship and the strength is presented in table 7.

Table 7: Guilford's Rule of Thumb (Guilford, 1956).

R value	Strength of Relationship
<0.20	Almost negligible relationship
0.20 - 0.40	Low Correlation; definite but small relationship
0.40 - 0.70	Moderate correlation; substantial relationship
0.70 - 0.90	High correlation; marked relationship
>0.90	Very high correlation; very dependable relationship

The table below shows that the correlations between the authentication (AUT), authorization (ATH), availability (AVA), confidentiality (CON), integrity (INT), access control (ACC), and trust (TRU), sensor (SEN), MOBILITY NETWORK (MOB), RFID system (RFI), Wi-Fi (WIF), Bluetooth (BLU) and and ZigBee (ZIG) with IoT applications are positive and significant.

Table 8: Correlation Matrix.

	AUT	ATH	AVA	CON	ACC	INT	TRU	SEN	MOB	RFI	WIF	BLU	ZIG	IOT
AUT	1	.533**	.586**	.252*	.363**	.381**	.466**	.302**	.500**	.599**	.285**	.900**	.963**	.782**
ATH		1	.594**	0.153	.295**	.501**	.435**	0.139	.810**	.461**	0.175	.547**	.474**	.577**
AVA			1	0.183	.277**	.703**	.535**	.197*	.667**	.478**	0.160	.588**	.521**	.445**
CON				1	.679**	.222*	0.113	.288**	0.064	.245*	.416**	.304**	.225*	.773**
ACC					1	.256**	0.171	.562**	.249*	.331**	.516**	.356**	.328**	.686**
INT						1	.528**	.228*	.495**	.428**	.224*	.436**	.347**	.478**
TRU							1	0.111	.370**	.634**	0.127	.542**	.374**	.648**
SEN								1	0.166	.241*	.231*	.237*	.312**	.734**
MOB									1	.350**	0.073	.464**	.496**	.485**
RFI										1	.201*	.602**	.467**	.710**
WIF											1	.438*	.494**	.505**
BLU												1	.849**	.523**
ZIG													1	.542**
IOT														1

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

(AUT: Authentication, ATH: Authorization, AVA: Availability, CON: Confidentiality, INT: Integrity, ACC: Access control, TRU: Trust, SEN: Sensor, MOB: Mobile networks, RFI: RFID system, WIF: Wi-Fi, BLU: Bluetooth, ZIG: ZigBee, IOT: IoT Domain).

Hypothesis testing

For further enhance the findings, a regression analysis was conducted to test H_1, H_2, H_3, H_4, H_5, H_6, H_7, H_8, H_9, H_{10}, H_{11}, H_{12}, and H_{13}. Table 9 summarize the result of regression shows below.

Based on the results, it shown that eleven (11) variables significant influenced on IoT application development. There are two (2) independent variables that not significant influenced the IoT application development. The result show that all the independent variables explained 71.8 % (refer Adjusted R square) of total variation in IoT application development. As overall the model is good fit (p-value =.000). The summary of the result presented in table 10.

Table 9a: Regression Analysis Result.

Model Summary[b]					
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**	**Durbin-Watson**
1	.869[a]	.755	.718	.19574	1.881
a. Predictors: (Constant), ZIG, CON, SEN, TRU, MOB, ACC, RFI, WIF, INT, AVA, ATH, BLU, AUT					
b. Dependent Variable: DOMAIN					

Table 9b: Regression Analysis Result.

ANOVA[a]						
Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	10.177	13	.783	20.432	.000[b]
	Residual	3.295	86	.038		
	Total	13.472	99			
a. Dependent Variable: DOMAIN						
b. Predictors: (Constant), ZIG, CON, SEN, TRU, MOB, ACC, RFI, WIF, INT, AVA, ATH, BLU, AUT						

Table 9c: Regression Analysis Result.

Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig**
		B	**Std. Error**	**Beta**		
1	(Constant)	1.833	.202		9.056	.000
	AUT	.214	.050	.334	4.321	.000
	ATH	.219	.075	.214	2.895	.005
	AVA	.164	.051	.258	3.202	.002
	CON	-.078	.071	-.088	-1.089	.079
	ACC	.096	.070	.112	1.370	.090
	INT	.272	.073	.269	3.749	.000
	TRU	-.213	.225	-.276	-.948	.346
	SEN	.443	.069	.547	2.440	.000
	MOB	.527	.190	.678	2.773	.007
	RFI	.354	.064	.478	5.528	.000
	WIF	.257	.090	.240	2.839	.006
	BLU	-.232	.088	-.346	-2.634	.010
	ZIG	.111	.132	.094	.845	.400

Table 10: Result of Hypothesis Testing.

Hypothesis	Result		Decision
	Regression	Correlation	
H_1: Authentication requirement has a significant relationship with the IoT application development.	Significant (p-value = .000)	High correlation (r = .782)	Accept
H_2: Authorization requirement has a significant relationship with the IoT application development.	Significant (p-value = .005)	Moderate correlation (r = .577)	Accept
H_3: Access control requirement has a significant relationship with the IoT application development.	Significant (p-value = .090)	Moderate correlation (r = .686)	Accept
H_4: Availability requirement has a significant relationship with the IoT application development.	Significant (p-value = .002)	Moderate correlation (r = .445)	Accept
H_5: Confidentiality requirement has a significant relationship with the IoT application development.	Significant (p-value = .079)	High correlation (r = .773)	Accept
H_6: Integrity requirement has a significant relationship the IoT application development.	Significant (p-value = .000)	Moderate correlation (r = .478)	Accept
H_7: Trust requirement has a significant relationship with the IoT application development.	Not significant (p-value = .346)	Moderate correlation (r = .648)	Reject
H_8: Sensor technology has a significant relationship with the IoT application development.	Significant (p-value = .000)	High correlation (r = .734)	Accept
H_9: Mobile Networks technology has a significant relationship the IoT application development.	Significant (p-value = .007)	Moderate correlation (r = .485)	Accept
H_{10}: RFID technology has a significant relationship with the IoT application development.	Significant (p-value = .000)	High correlation (r = .710)	Accept
H_{11}: Wi-Fi technology has a significant relationship with the IoT application development.	Significant (p-value = .006)	Moderate correlation (r = .505)	Accept
$H1_2$: Bluetooth technology has a significant relationship with the IoT application development.	Significant (p-value = .010)	Moderate correlation (r = .523)	Accept
H_{13}: ZigBee technology has a significant relationship with the IoT application development.	Not significant (p-value = .400)	Moderate correlation (r = .542)	Reject

in IoT application development. As overall the model is good fit (p-value =.000). The summary of the result presented in table 10.

As we can see, the Hypothesis 1 (H_1) shows a significant positive relationship (p-value =.000) and has high correlation (r = .782) between authentication requirement (AUT) and IoT application development. Therefore, H_1 is accepted. Based on the rules for measuring the strength of the relationship, Hypothesis 2 (H_2) has moderate correlation (r = .577) and positive statistically significant relationship (p-value = .005) and association between authorization requirement (ATH) and IoT application development. Therefore, H_2 is accepted. Hypothesis 3 (H_3) has moderate correlation (r = .686) and positive statistical significant relationship (p-value = .090) between access control (ACC) and IoT application development. So, H_3 is accepted The assumption of Hypothesis 4 (H_4) is supported and confirming a positive significant relationship (p-value = .002) and has moderate correlation (r = .445) between availability (AVA) and IoT application development. Therefore, H_4 is accepted. Following the rules for measuring the strength and relationship, Hypothesis 5 (H_5) is supported confirming a positive significant relationship

(p-value = .079) and correlation is shown as high correlation (r = .773) between confidentiality (CON) and IoT application development. So, based on the result we accepted H_5. Test of Hypothesis 6 (H_6) shows a positive, statistically significant association (p-value = .000) and moderate correlation (r = .478) between integrity (INT) and IoT application development. Therefore, H_6 is accepted. The results of Hypothesis 7 (H_7) is indicate that trust (TRU) have insignificant relationship (p-value = .346) between trust requirement and IoT application development even though they have a moderate correlation (r = .648). Therefore, H_7 is rejected. Hypothesis 8 (H_8), result is positive significant relationship (p-value = .000) and have high correlation (r = .734) between sensor (SEN) and IoT application. Therefore, H_8 is accepted. Based on the rules for measuring the strength of the relationship, Hypothesis 9 (H_9) has moderate correlation (r = .485) and positive statistically significant relationship (p-value = .007) and association between mobile network (MOB) and IoT application development. Therefore, H_9 is accepted. Test of Hypothesis 10 (H_{10}) shows a positive, statistically significant association (p-value = .000) and high correlation between (r = .710) RFID system (RFI) and IoT application development. Therefore, H_{10} is accepted. The assumption of Hypothesis 11 (H_{11}) is supported and confirming a positive significant relationship (p-value = .006) and has moderate correlation (r = .505) between Wi-Fi (WIF) and IoT application development. Therefore, H_{11} is accepted. Also, following the rules for measuring the strength and relationship, Hypothesis 12 (H_{12}) is supported confirming a positive significant (p-value = .010) relationship and correlation is shown as moderate correlation (r = .523) between Bluetooth (BLU) and IoT application development. So, we accepted H_5. Lastly, the results of Hypothesis 13 (H_{13}) is indicate that ZigBee (ZIG) have insignificant relationship (p-value = .400) between ZigBee and IoT application development even though they have a moderate correlation (r = .542). Therefore, H_{13} is rejected.

Secure iot application development (SecIoTA) model

The figure 2 shows the develop SecIoTA Model that comprises the need of 1) security requirements and 2) IoT technologies to develop a secure IoT application. Based on the findings, there are two variables which not significant relationship with IoT application 1) trust and 2) ZigBee. Therefore, we have rejected the insignificant security requirements and IoT technologies from the conceptual frameworks. The model of secure IoT application that consist of security requirement and IoT technologies (SecIoTA Model) was illustrated in figure 2.

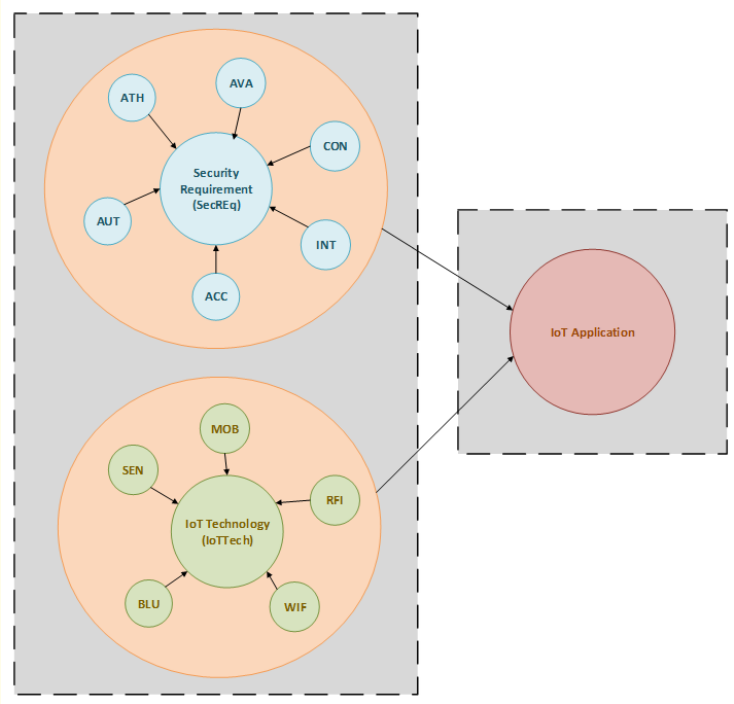

Figure 2: SecIoTA Model.

Based on the figure, to develop a secure IoT application, requirements that are almost needed are security requirements and its technologies. The security requirements that most needed are authentication, authorization, availability, confidentiality, access control, and integrity while IoT technologies that are primarily used are sensor, mobility network, RFID system, Bluetooth and Wi-Fi. The combination of these two requirements may help the developer to develop and design a secure IoT application in the future.

Limitation

There are few limitations that we need to overcome in the future. First, the number of respondents is too small to derive any discussion and conclusions. Furthermore, most of our respondents are from Klang Valley. Both constraints are believed could affect the results as different demographic and place cloud contribute to different findings of the survey.

Conclusion and Future Works

The purpose of this study is to determine and analyze the relationship between the security requirements and IoT technologies for developing secure IoT applications. Based on the results of our study, it is found that the security requirements and IoT technologies were significant to develop secure IoT applications. There also shows that they have a correlation between security requirements and IoT technologies. We also plan to develop a tool that can assist the requirement engineering in elicit security requirement for IoT applications to realize our model.

Acknowledgement

The authors would like to acknowledge Universiti Teknikal Malaysia Melaka (UTeM) and Polytechnic Sultan Azlan Shah for its support and all those who participate in the study and helped to facilitate the research process.

Bibliography

1. E A Fischer. "The Internet of Things: Frequently Asked Questions". *Congressional Research Service* (2015).
2. K Rose., *et al*. "The Internet of Things : An Overview". (2015).
3. Vermesan., *et al*. "Internet of Things Strategic Research Roadmap". in Internet of Things: Global Technological and Societal Trends (2011): 9-52.
4. S Jaiswal and D Gupta. "Security Requirements for Internet of Things (IoT)". Proc. Int. Conf. Commun. Networks, Adv. Intell. Syst. Comput. (2017): 419-427.
5. AA Ibrahim and M Kamalrudin. "Security Requirements and Technologies for The Internet of Things (IoT) Applications: A Systematic Literature Review". *Journal of Theoretical and Applied Information Technology* 96.17 (2018): 5694-5716.
6. M Kamalrudin., *et al*. "A Security Requirements Library for the Development of Internet of Things (IoT) Applications". in Requirements Engineering for Internet of Things 809 (2018): 87-96.
7. D G Firesmith. "Engineering Security Requirements". *Journal of Object Technology* 2.1 (2003): 53-68.
8. S R Oh and Y G Kim. "Security Requirements Analysis for the IoT". 2017 Int. Conf. Platf. Technol. Serv. PlatCon 2017 - Proc., (2017).
9. P Salini and S Kanmani. "A Survey on Security Requirements Engineering". *International Journal of Research and Reviews in Computer Science* 8 (2011): 1-10.
10. D H Kim., *et al*. "A Study of Developing Security Requirements for Internet of Things (IoT)". *Advanced Science and Technology Letters* 87 (2015): 94-99.
11. Z A Hussien., *et al*. "Secure and Efficient E-health Scheme Based on the Internet of Things". (2016).
12. S M R Islam., *et al*. "The Internet of Things for Health Care : A Comprehensive Survey". *IEEE Access* 3 (2015): 678-708.
13. E Borgia. "The Internet of Things Vision: Key Features, Applications and Open Issues". *Computer Communications* 54 (2014): 1-31.
14. E Steve. "What is Requirements Engineering?". (2004): 2-18.
15. I Sommerville. Software Engineering Ninth Edition, Ninth. Boston, Massachusetts: Person Education, Inc., Addison-Wesley, (2011).
16. P Salini and S Kanmani. "Survey and Analysis on Security Requirements Engineering". *Computers and Electrical Engineering* 38 (2012): 1785-1797.

17. M Trnka., *et al*. "Survey of Authentication and Authorization for the Internet of Things". *Security and Communication Networks* (2018): 17.

18. M Saadeh., *et al*. "Authentication techniques for the internet of things: A survey". Proc. - 2016 Cybersecurity Cyberforensics Conf. CCC 2016. (2017): 28-34.

19. S Patel., *et al*. "IoT based Smart Hospital for Secure Healthcare System". *International Journal on Recent and Innovation Trends in Computing and Communication* 5.5 (2017): 404-408.

20. K Dempsey., *et al*. "Supplemental Guidance on Ongoing Authorization". (2014).

21. V Suryani., *et al*. "Trust-based Privacy for Internet of Things". *International Journal of Electrical and Computer Engineering* 6.5 (2016): 2396-2402.

22. Z Yan., *et al*. "A Survey on Trust Management for Internet of Things". *Journal of Network and Computer Applications* 42 (2014): 120-134.

23. K Dhariwal and A Mehta. "Architecture and Plan of Smart hospital based on Internet of Things (IoT)". *International Research Journal of Engineering and Technology* 4.4 (2017): 1976-1980.

24. D Kiritsis. "Closed-loop PLM for Intelligent Products in the Area of The Internet of Things". *Computer-Aided Design* (2010): 1-23.

25. W Lee., *et al*. "A Gateway Based Fog Computing Architecture for Wireless Sensors and Actuator Networks". in 2016 18th International Conference on Advanced Communication Technology (ICACT), (2016): 210-213.

26. M Souppaya and K Scarfone. "Guidelines for Managing the Security of Mobile Devices in the Enterprise". NIST Spec. Publ. 800-124, Revis. 1 (2015): 1-30.

27. S Quirolgico., *et al*. "NIST Special Publication 800-163: Vetting the Security of Mobile Applications". NIST Spec. Publ. 800-163 (2015): 800-163.

28. E de O e Silva., *et al*. "Authentication and the Internet of Things: A Survey Based on a Systematic Mapping". ICSEA 2017 twelfth Int. Conf. Softw. Eng. Adv. (2017): 34-40.

29. T Karygiannis., *et al*. "Guidelines for Securing Radio Frequency Identification (RFID) Systems Recommendations of the National Institute of Standards and Technology". NIST Spec. Publ. 800-98, (2007).

30. T Karygiannis., *et al*. "NIST Special Publication 800-98: Guidelines for Securing Radio Frequency Identification (RFID) Systems". NIST Spec. Publ. 800-98, (2007).

31. Homeland Security. "A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family)". (2017).

32. K Scarfone., *et al*. "Guide to Bluetooth Security". NIST Spec. Publ. 800-121 Revis. 2 (2017): 63.

33. J Gubbi., *et al*. "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions". *Future Generation Computer Systems* 1 (2013): 1-19.

34. I Bouij-pasquier., *et al*. "SmartOrBAC Security and Privacy in The Internet of Things". 2015.

35. S Ravidas., *et al*. "Access Control in Internet of Things: A survey". *Journal of Network and Computer Applications* 144 (2019): 79-101.

36. N Gershenfeld., *et al*. "The Internet of Things: Converging Technologies for Smart Environment and Integrated Ecosystems" 291.4 (2004).

37. V Scuotto., *et al*. "Internet of Things: Applications and Challenges in Smart Cities: A Case Study of IBM Smart City Projects". *Business Process Management Journal* 22.2 (2016): 357-367.

38. MM Hossain., *et al*. "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things". Proc. - 2015 IEEE World Congr. Serv. Serv. (2015): 21-28.

39. R Roman., *et al*. "Securing The Internet of Things". IEEE Computer Society, Spain (2011): 51-58.

40. K Kishore and S Sharma. "Evolution of Wireless Sensor Networks as the framework of Internet of Things- A Review". 5.12 (2016): 49-52.

41. M Bilal and S G Kang. "An authentication protocol for future sensor networks". *Sensors (Switzerland)* 17.5 (2017): 1-29.

42. X Jia., *et al*. "RFID technology and its applications in Internet of Things (IoT)". 2012 2nd Int. Conf. Consum. Electron. Commun. Networks, CECNet 2012 - Proc. (2012): 1282-1285.

43. R Aggarwal and M Lal Das. "RFID Security in the Context of 'Internet of Things". in Proceedings of the First International Conference on Security of Internet of Things (SecurIT' 12) (2012): 51-56.

44. S Raza., *et al*. "Bluetooth smart: An Enabling Technology for the Internet of Things". 2015 IEEE 11th Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob (2015): 155-162.

45. Q Zhu., *et al*. "IOT gateway: Bridging wireless sensor networks into Internet of Things". Proc. - IEEE/IFIP Int. Conf. Embed. Ubiquitous Comput. EUC (2010): 347-352.