Journal of Theoretical and Applied Information Technology
31st July 2019. Vol.97. No 14
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COMMON PRACTICES IN ELICITING SECURITY REQUIREMENTS OF INTERNET OF THINGS (IOT) APPLICATIONS

[1]ASMA ASDAYANA IBRAHIM, [2]MASSILA KAMALRUDIN, [3]SAFIAH SIDEK
[1] Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka, 76100, Malaysia
[2] Innovative Software System and Service Group,
Universiti Teknikal Malaysia Melaka, 76100, Malaysia
[3] Institute of Technology Management and Entrepreneurship,
Universiti Teknikal Malaysia Melaka, 76100, Malaysia
E-mail: [1]asmaasdayana@gmail.com, [2]massila@utem.edu.my, [3]safiahsidek@utem.edu.my

ABSTRACT

The increased complexity in security requirements due to the widely spread development of Internet of Things (IoT) applications requires Requirements Engineers (REs) to have a security knowledge and experience in the process of eliciting requirements. Requirements captured by REs are commonly inconsistent with their client's intended requirements and often error prone. This paper intends to address this issue by conducting a survey to investigate the common practices among practitioners in IoT industry, focusing on how they deal with security requirements, what are their knowledge about IoT and its security and what resources they use when dealing with security. An online survey has been conducted involving 42 respondents from IoT organizations in Malaysia. The results show that respondents have knowledge of IoT and its security, but they have less involvement in eliciting security requirement in developing secure IoT applications. Therefore, there is a need to propose a new approach in eliciting security requirement in IoT application to help the professionals to develop more secure applications.

Keywords: *Requirement Engineering, security requirements, Internet of Things (IoT), elicitation*

1 INTRODUCTION

The number of Internet-connected devices had surpassed the number of human beings in 2011, and by 2020, Internet-connected devices are expected to reach between 26 billion and 50 billion globally [1] [2] [3] [4]. In the case of IoT, people will not just be interacting with other people and things, but the things themselves will also be interacting with one another. With the increasing usage of IoT devices and applications, security has become the most important part in the IoT industry. Millions of dollars are spent on developing the application, but will be a big failure if it does not have proper security measures [5]. For this reason, addressing the security issue, especially in the elicitation process has become the most challenging issue in the application and software project development. Since, security is one the non-functional requirement most of the times it is ignored in the elicitation phase [6]. But, it is possible to reduce application development cost and time to identify security requirements in the beginning stage of the application development process.

Designing an application or a software is an exercise in meeting a business objective. The application design and development stage is the perfect time to think about how security requirements and business needs converge [7]. Building security into the software development lifecycle (SDLC) is a sound business decision, there may be an expense in securing the vulnerabilities, however allowing to be presented to malicious activities has costs as well [8]. Prevention is a more reasonable cost to justify and ultimately a much lower cost for an organization to assimilate. Studies have more than one demonstrated that detecting and preventing code flaws early in the software development life cycle leads to significant cost savings. Unfortunately, the way to securing an application too often begins with rigorous testing for vulnerabilities, to ensure the application will not compromise, or enable others to compromise, data privacy and integrity.

Moreover, early consideration for security in requirement phase helps in tackling security problems before further proceeding in the process and in turn avoid rework. In order to integrate security with requirement engineering, we have to consider security requirements. The basic task of security requirement eliciting is to identify and document requirements needed for developing secure applications. Satisfying such security requirements should lead to more secure application development. Security requirements is defined as constraints on the functionality of the system focusing on what should be achieved [9]. The security requirements also should be expressed as positive statements and not negative statements. Expressing requirements in such way can help in verifying its satisfaction. Security requirements can be elicited by analyzing the assets and the threats from which these assets should be protected. Security requirements need to be adequate as possible. They need to be explicit, precise, complete and non-conflicting with other requirements. However, knowledge of security is a basic necessity prior to practicing security requirement elicitation. The analyst should have background on how to identify and analyze the system assets, threats, vulnerabilities and requirements. One of the challenges for secure application development is to assist developers in performing security requirements engineering. A more effective approach for security requirement engineering is needed to provide a more systematic way for eliciting adequate security requirements.

This paper reports on a study that explores the common practices in addressing security requirements among practitioners and developers in the industry related to Internet of Things (IoT). The survey consists of a series of questions about security requirements elicitation in several organizations involved in IoT in Malaysia. The answer to these questions helps to understand common practices, whether the research on security requirement has contributed to real-world practices. It helps the professional to evaluate the security requirements elicitation in the earlier phase in application developments especially in IoT industry.

This paper is organized in seven (7) sections. After the introduction section, we discuss the background of the research in Section 2. Then, we present the purpose of the research for this study in Section 3. This is followed by the research method in Section 4. The findings and discussions of this study are presented in Section 5 and the related works in Section 6. Finally, the conclusion are presented in Section 7.

2 BACKGROUND OF RESEARCH

In requirements engineering, requirements elicitation is the practice of researching and discovering the requirements of a system from clients, customers, and other stakeholders. The practice is also sometimes referred to as “requirement gathering”. In a software organization, usually to have a project group that comprises of requirements engineers and security engineers. The primary responsibilities of requirements engineers or system analysts are to assemble, analyze, document and validate the needs of the project stakeholders [10]. They are capable at the requirement phase which is to capture security requirements from clients. Security engineers, on the other hand are responsible for designing, developing and deploying security related systems and security in systems. Their responsibilities and skills can be very specific such as designing a hardware security appliance. The task of a security engineer is generally focused at the implementation or design phase. Although both engineers have complementary responsibilities in capturing requirements, they do not communicate effectively with each other; consequently, there is a lack of integration on the work done between them. This condition can lead to inconsistency and incorrectness of the developed software and it fails to fulfill the needs of the stakeholders. Also, the current standard, such as the Common Criteria (ISO) has been identified as extensive, complex and difficult to comprehend by requirements engineers [11] [12]. Existing techniques, such as interviews and brainstorming, are tedious and neglect to precisely recognize security requirements. For this situation, captured security requirements using the present standards and techniques are prone to be inaccurate, inconsistent and incomplete which can lead to instances of insecure software.

Before being able to secure an application, it is important to first understand the functional and technological details of the application to be secured. This will require security engineers to work closely with the developers of the IoT ability to present security requirements early in the design process. Using a methodical systems security engineering approach for each IoT implementation within an enterprise is recommended. Standards supporting the IoT have not yet been completely developed, leaving the market open to competing platforms, protocols, and interfaces [13]. This lack of standards drives increased complexity which can introduce vulnerabilities and provides attackers with a way to infiltrate the industry.

Since IoT solutions are developed with specific technologies and focus on specific applications, they lack standardization, which results in fragmented and heterogeneous architectures [2]. The present fragmentation of IoT security guidelines, initiatives, standards and other schemes needs to be addressed [4]. A first and solid step in the direction is to define a list of best practices and guidelines for IoT security and privacy, which can be used as a baseline for the development and deployment of IoT systems in the market. However, there is lack of knowledge present within IoT developers, industries as well as end users and consumers. It is clear that lack of security impacts business continuity and this is indeed the case also for IoT that is driven by Research & Development (R&D) activities and a rush to push products and services in the market. In this respect, business continuity can serve as a driver for justifying costs in cyber security solutions. Moreover, interoperability, standards, protocols, and conventions are a primary issue in the early development and adoption of IoT applications.

3 PURPOSE OF RESEARCH

The purpose of this study is to gain an understanding of the real practices among REs dealing with security requirements during the eliciting process. Focusing on the practitioners in the IoT related organizations, the following questions were designed for the purpose of this study shown in Table 1.

Table 1: Research Question and Motivation

Research Question	Motivation
How is involvement of practitioners in IoT and security?	The involvement of practitioners in IoT and security.
What are the experience in eliciting security requirements?	The experience in eliciting security requirements.
What are the security knowledge and standards practiced by software professionals?	Security knowledge and standards practiced by software professionals.

4 RESEARCH METHOD

This study aims to explore the knowledge and practices of requirements engineers when dealing with security requirements, particularly in the development of IoT applications. For this purpose, this study adopts an online survey as it is an efficient way to collect a widely dispersed data and the information can be gathered automatically. The margin of error is also greatly reduced with online survey since respondents can enter their responses directly into the system. Further, it is flexible for the respondents as they can choose the most suitable time to complete the survey.

In this survey, 42 software professionals and experts with various positions in IoT organizations in Malaysia (located in Klang Valley), such MDEC Sdn. Bhd, MIMOS Berhad, SME Corp, MCMC and other companies related to IoT industries participated in the survey. The survey was sent electronically to the respondents and the feedbacks were collected through a web-based survey. This study targets software and requirement engineers which were dealing with security requirements in real-world IoT industry.

The survey is organized into three sections, which consists of 14 multiple-choice questions, focusing on different aspects related to security requirements practice in IoT application development. The three sections together with the purpose for each section of the survey are as shown in Table 1. The questionnaires have been validated by two academic experts and one industry expert. The reviewed on the content validity of the questionnaires and gave opinion and idea on the contents related to involvement in eliciting security requirements in early phase of application development [2].

Table 2: The Survey

Section	Topic	Purpose
A	General and Background	To gather general information about the organization's primary industry, respondents' primary role in the organization and their training in computer security.
B	IoT and Security	To investigate their involvement in IoT and security, the use of security standards, guidelines or checklist in respondents' work in the organization and their security practices regulated in their organization.
C	Security Requirements Elicitation	To elicit the knowledge and technique in eliciting security requirements, the security solutions routinely used in security requirement elicitation and the options considered in dealing with security issues or security requirements.

5 FINDING AND DISCUSSIONS

The results derived from the survey show interesting and surprising trends in IoT industry. This section provides the main findings on the common practices in security requirements in IoT organizations in Malaysia.

5.1 General and Background

Respondents of this survey are experts and software professionals of diverse roles from various IoT organization in Malaysia. Figure 1 shows the majority of the participating organization consisting of the smart home/building (29%) and the remains are involved in various sectors, such as smart grid (19%), smart mobility and tourism (17%), logistic and product lifetime management (7%), independent living (7%), medical and healthcare (5%), industrial processing (5%), agriculture and breeding (5%) and public safety and environment and monitoring (2%). IoT has huge potentialities for developing new smart applications in nearly every field [14] [15]. They spread various persepective: personal, social, societal, medical, environmental, logistics to cite a few. Based on the result, it demostrates that the organization in Malaysia involved in almost all aspects in IoT industry. The Ministry of Science, Technology and Innovation (MOSTI) takes the view that the IoT is a key to the transformation of Malaysia's digital economy [1]. IoT gives rise to the interconnected world and is made possible by technologies and research disciplines that enable the Internet to reach out to the real world of communicating objects. IoT will be technologically and economically feasible to transform the way people interact with objects and enrich the digital user's experience.

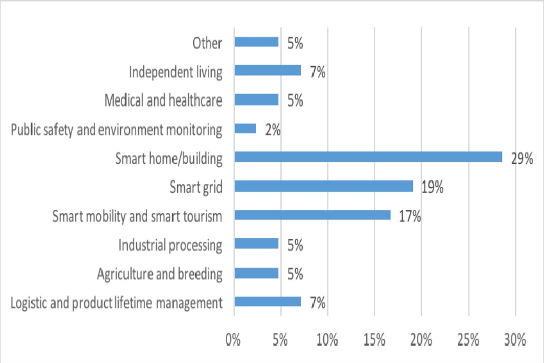

Figure 1: Organization's primary industry

Figure 2 shows the respondents' primary roles in their organizations. The majority of the respondents described their roles as IT Officer (21%), 14% Programmer, 10% Information Security Analyst, 10% IoT Engineer. Additionally, 7% identified themselves as Project Manager, Software Designer, System Designer, Software Engineer or Requirement Engineering, while 2 % as Software Developer. The others (7%) are identified as Product Manager, Laboratory Director and Material Engineer. This indicates that all the respondents have experience working with software and information technology.

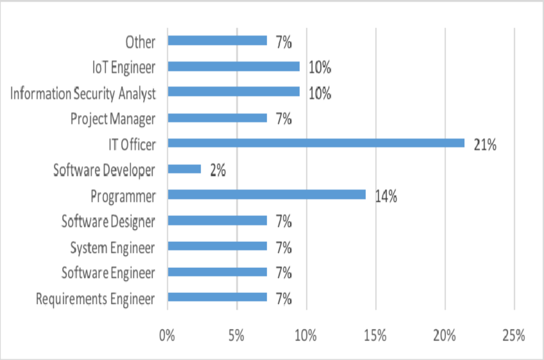

Figure 2: Respondent primary roles in organization

The respondents were also requested to declare whether they have any security education and training. Figure 3 shows that 38% had the security education as part of the training they received at their job, 33% as part of the formal education, 24% self-study due to job demand and 5% did not have any security education and training. This indicates that the respondents have a security education and training in dealing with their work. Further, the population of the respondents shows that they have a sufficient security awareness to provide relevant feedback in the survey. Education and training are among the important aspects in developing secure software or application. Higher education programs must ensure that the next generation of engineers understands how to design and build technological systems as well as deals with security issues [16]. The biggest challenge in materialising the greater benefits of IoT is the human factor, where the capabilities of industry players in swiftly creating new and differentiated products will be a primary determinant of their success [17]. In addition, the challenge is in developing a safe and secure software and applications using a systematic process. With that, security education and training needs to be established in industries, including knowledge of state-of-the-art, best practices, reference structures and accesibility of building blocks, methodologies and tools for secure IoT applications [2].

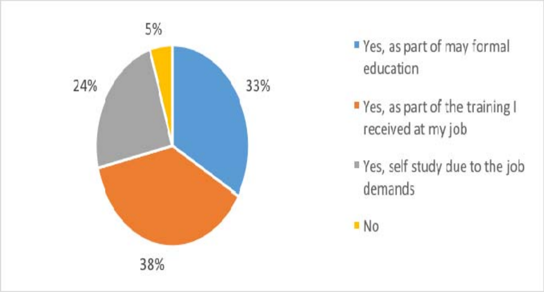

Figure 3: Security education and training

5.2 IoT and Security

This section investigates the security involved in IoT industry. The respondents were requested to give their level of their understanding towards IoT, as shown in Figure 4. 81% respondents agreed that they fully understand the term and the relevance of IoT to their job. This indicates that the respondents and their organization are fully involved in IoT industry. On the other hand, only 19% of the respondents thought that it was just a hype and they had vague idea of IoT. Most of the cybersecurity industry is already familiar with the security issues around the IoT, largely driven by the impact they have already seen from smartphones, tablets and industrial control systems [18]. Today, the IoT has turned into a well known term for describing scenarios in which Internet connectivity and computing capability extend to a variety of objects, devices, sensors, and regular things.

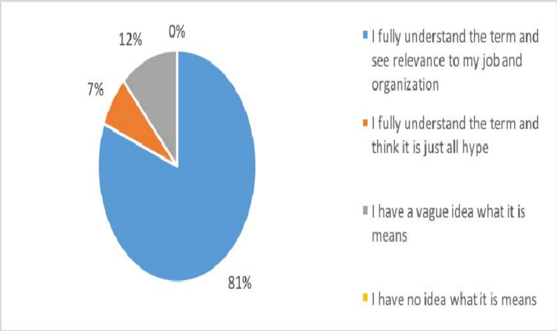

Figure 4: Level of understanding of the term the "Internet of Things" (IoT)

Furthermore, the majority of the respondents, which is 67% agreed that their organization are currently active in any areas that fit into the latest wave of connectivity to IoT, as shown in Figure 5. 31% respondents responded that their organization involved in IoT within 5 years and the rest (2%) claimed that their organization never get involved in IoT. This clearly shows that the industry nowadays is currently engaging in work related or directly involved in the technologies of IoT. Futhermore, IoT Malaysia shall be the industry body that will be responsible for the development of the IoT industry in Malaysia. IoT Malaysia shall be the Community of Practice (CoP) of IoT-based industries with the vision to help enhance each industry's performance by way of sharing knowledge and insights.

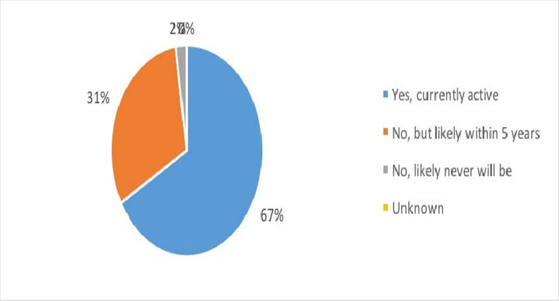

Figure 5: Organization involved in connectivity to IoT

According to the respondents, 55% agreed the IoT will have the same level of security problem that they have today with other applications or systems. While the others (45%) said the IoT will provide an opportunity to increase security in comparison to today, as shown in Figure 6. It can be concluded that IoT can actually help to improve security protection and processes overtime [19]. For example, IoT will be an impetus for bringing together physical security, IT security, and industrial systems security. While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. Tending to these difficulties and ensuring security in IoT applications and devices must be a fundamental priority. Users need to believe that IoT devices and related data services are secure from vulnerabilities, especially as this technology become more pervasive and integrated into our daily lives. Poorly secured IoT applications and devices can serve as potential entry points for cyber attack and expose user data to theft by leaving data streams inadequately protected.

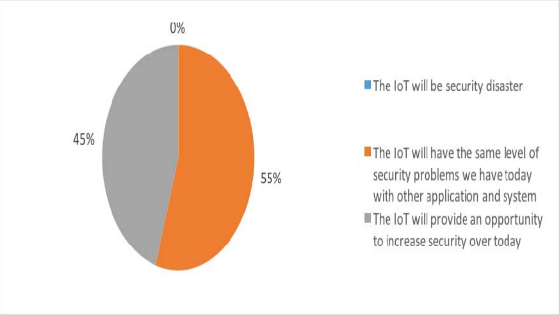

Figure 6: Statement about the IoT and security

From Figure 7, we ask the respondents whether they use security standards, guidelines or checklist at their work. Surprisingly, we discovered that security standards, guidelines or checklist are less considered when they dealing with their work. Results show that 43% said they did not use the security guidelines or standard even though their organizations have it. 26% used ISO, 21% used Common Criteria and 10% used NIST as their guidelines in work. This clearly shows security standard and guidelines have yet to be used as the main references when dealing with their work. As they are involved in IoT industry, they may need a security standard or policy, especially in IoT industry. Standards, protocols, interoperability, and conventions are a primary issue in the early development and adoption of IoT applications [4]. Lack of standards and documented best practices have a greater impact than just limiting the potential of IoT application developement. In a passive way, absence of the proper standards can enable unsecure by IoT applications. In other words, without standards to guide deveoplement, developers sometimes design products that operate in disruptive ways on the Internet without much regard to their impact. These applications are worse than simply not being interoperable. If poorly designed and implemented, they may have negative consequences for the networking resources they connect to and the broader Internet.

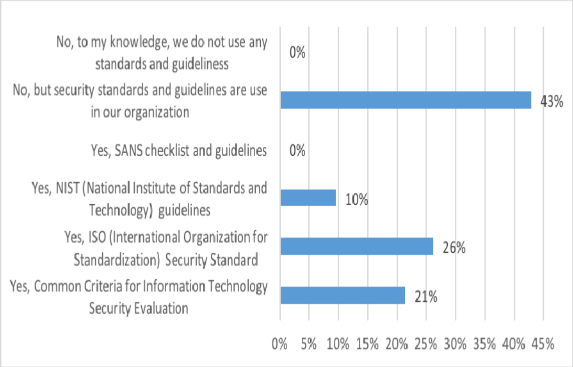

Figure 7: Security standards, guidelines or checklist at work

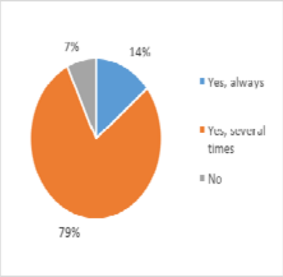

Figure 8: Experience and knowledge in eliciting security requirements

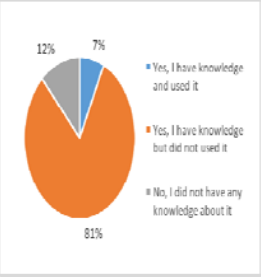

Figure 9: Knowledge about technique for security requirements elicitation

5.3 Security Requirements Elicitation

This section describes the answer regarding the elicitation of security requirements. The respondents were asked to indicate their experience and knowledge in working or eliciting the security requirements. Figure 8 shows the majority of the respondents (79%) stated that they have several experience in eliciting security requirements. 14% have been always dealing with elicitation process and only 7% did not have experience in eliciting security requirements. Figure 9 shows the respondents' knowledge about the techniques used for security requirement elicitation. Specifically, 81% respondents expressed that they have knowledge but did not used it and 12% did not have any knowledge of the technique in elicitation. Only 7% have knowledge and used it. This shows that although respondents have experience working in security requirements, they have less knowledge in the techniques of requirements elicitation. Many IoT engineers and develioper are not yet familiar with secure development best practices. The rush to create new IoT-based capabilities will probably result in constrained focus on the security of the new functionality being created [13].

According to Figure 10, 7% respondents expressed that security requirements are gathered and documented in the early stages of the project developments. However, 36% agreed that security issues were deal only during the implementation phase or after the application being developed. 24% stated that they did not deal with security requirement, 21% stated security requirement are discussed from the early stages but are not documented, and 7% did not know about the eliciting process. This finding confirms the existing belief that security requirements are not typically analyzed thoroughly and they were not analyzed from the early phases of the development life cycle [20]. The survey clearly shows that eliciting security requirement is commonly ignored during the early phase and was not appropriately documented. In view of the crucial treatment of security requirements, the elicitation process should be applicable as early as possible in the RE process [21] [6], that is, it is utmost important to emphasize security requirements as they arise from stakeholder interviews and documents.

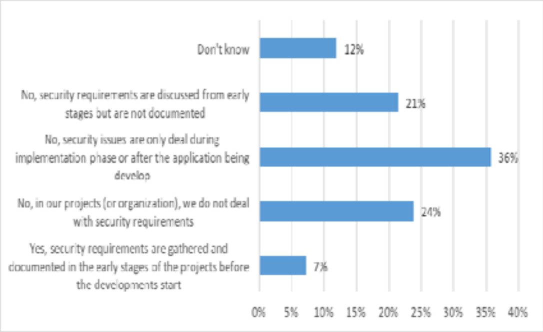

Figure 10: Person(s) responsible for requirements gathering elicit and document security requirements

In the survey, respondents were asked to choose the list of security resources that they used routinely to look for security solutions. Figure 11 shows, 31% of the respondents used security standards such as ISO, IEEE, CISSP, 21% stated that they used software vendor's data sheet, 18% used security–related text books, 14% used security design patterns and 11% used other standards. This indicates that the use of different security knowledge sources and they did not have any standards in IoT that can be referred in the industry. It can be concluded that these resources are still underexplored and usable applications are still unrearly non-existence. This existing scenario will make eliciting security requirement in IoT domain becomes more challenging.

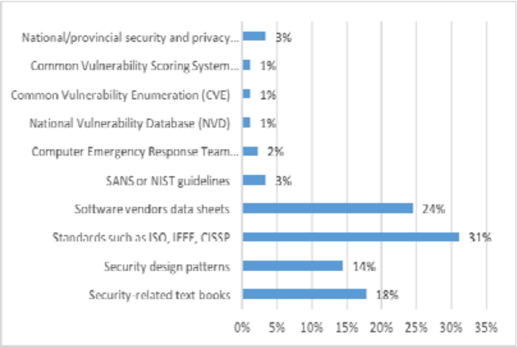

Figure 11: Resources used in security knowledge

When dealing with the security requirements or issues, 88% of the respondents usually look for multiple alternative solutions and then they select one. Only 12% usually considered for single solution. This results is presented in Figure 12. Standards supporting the IoT have not yet been completely developed, leaving the market open to competing platforms, protocols, and interfaces. This lack of standards drives increased complexity which can introduce vulnerabilities and provides attackers with a way to infiltrate the enterprise [13]. Organizations must be able to plan for the compromise of IoT devices, keys and certificates. This includes performing forensic analysis on compromised systems and devices.

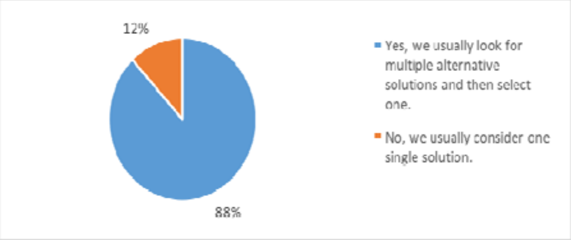

Figure 12: Alternative solution when dealing with a security issue or a security requirement

Based on the previous question, it was found that multiple security solutions were considered by the respondents, as shown in Figure 13. The result shows that 46% of the respondents stated that the multiple solutions were considered based on their usability, the level of the privacy and the security they provide such as costs, time and market. 19% of the respondents considered the most economical solution and balance out the security and financial costs. While 16% choose the most secured solutions, even though it not the most economical solution. The IoT does not require a completely new set of application security solutions or guidelines and best practices. The same set of guidelines at the application hold true for any traditional implementation.

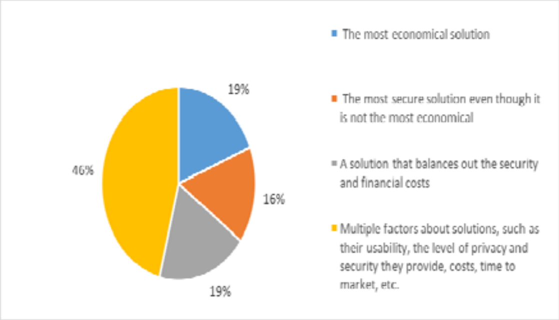

Figure 13: Options for multiple security solutions

6 RELATED WORKS

The IoT's anywhere, anything, anytime nature could easily change these advantages into disadvantages, if security aspects would not be provided enough. While the term IoT has been uncontrollably overhyped, security experts are already dealing with the first several waves of Internet-connected Things and have started to get ready for the challenges of the next wave of more diverse, more complex devices [18]. Currently adopted internal controls are inadequate to manage huge numbers of the present IoT devices; alternative controls or technological advances need to be adopted to maintain effective internal controls. Many are starting from security strategies and controls based on securing user devices, such as smartphones and tablets. Based on the survey done by [18], most of respondents expected IoT device manufacturers to take a larger level of responsibility for security than security professionals have expected of PC and server hardware and application vendors in the past. More than half plan on having to do their own evaluation and testing of devices before allowing them on the corporate network. These results suggest that manufacturers who invest in secure development life cycles for their IoT products and provide both visibility into vulnerability levels and support for patching and updating will see competitive advantages when selling to enterprises.

A survey related to the privacy and security challenges of the IoT is done by D. Mendez et. al [22]. The survey addresses the challenges from the perspective of technologies and architecture used. This work concentrates also in IoT intrinsic vulnerabilities as well as the security challenges of various layers based on the security principles of data confidentiality, integrity and availability. This survey analyzes articles published for the IoT at the time and relates it to the security conjuncture of the field and its projection to the future. However, the survey did not involve the eliciting of security requirements before develop an IoT applications.

Maede Zolanvari [23] presented briefly the main ideas of IoT and pointed out the importance of having a secure structure for this new promising technology. The study went over the present challenges related with providing privacy which is the top essential component, because without enough security, this technology will not be useful and will just harm the human being. After that, they went through the recent solutions that have been provided, and finally, they provided the security issues at different layers of IoT. Also, there is still a long way ahead to provide a complete secure structure based on the fact that IoT needs to be widespread with tremendous number of users and devices with various patterns. However, this study did not focus on user or client perspective on the current practices on eliciting requirements that they are having in the development of new technology of IoT.

T. Borgohain in his studied [24] have surveyed all the security flaws existing in the IoT that may prove to be very detrimental in the development and implementation of IoT in the various fields. So adoption of sound security measures countering the above detailed security flaw as well as implementation of various intrusion detection systems, cryptographic and stenographic security measures in the information exchange process and using of efficient methods for communication will result in a more secure and robust IoT infrastructure. In the study, they had recommended that more effort on development of secured measures for the existing IoT infrastructure before going for further development of new implementation methods of IoT in daily life would prove to be a more fruitful and systematic method. But still, they did not provide the practices of any standards that being use in developing of IoT applications.

Elahi and Yu [20] conducted a survey to explore the approach of security requirements elicitation, involvement of attacks and risk in the analysis, and the use of modelling, risk assessment, and quantification practiced among practitioners in the industry. They observed that security requirements are not often explicitly elicited and documented in the early stages of the development. Instead, they are mostly considered during the implementation phase. However, this study did not support security requirements for IoT. Meanwhile, Ramesh and Reddy [5] conducted a survey on security requirement elicitation methods. They studied 15 security requirement elicitation methods, such as Abuse cases, Misuse cases, SQUARE, OCTAVE, and CLASP. Each method was analyzed against different attributes such as applicability, ease of learn and ease of use. They presented an overview of security requirements, different methods for identifying security requirements, how they are classified their merits and demerits. However, this survey does not offer user practices on elicitation of security requirement of IoT application.

Elicitation is one of the crucial issues for the systems or applications development and a major part of the RE process [25]. A survey on security requirements elicitation and presentation in RE phase has been conducted by [6]. Their work reflects current research on software user security requirements elicitation techniques in RE phase. They tried to identify the research trend, based on related published work. However, they only focus on eliciting security requirements in RE phase. In addition, Franco [26] proposed a systematic review in RE field. This work presented approaches that support RE in software development processes.

This paper reports the main characteristics of each proposal such as the purpose, sources of requirements required, target produced, type of knowledge representation used, types of resources, methods and tools required to accomplish their goal. They also identified the prominent issues of interest for the researchers, and the most influential works and trends over time. However, this study does not cover the aspects of security requirements of IoT applications.

7 CONCLUSION

This paper describes a study of common practices of involvement in security requirements elicitation among practitioners in the area of IoT. In this study, different professional's roles and positions in various IoT organizations were surveyed. We investigated the common practices of the professionals dealing with security requirements, their knowledge about security and IoT and the recourses and the alternative security solution when they dealing with a security issue or security requirements. In recent days, it has been observed that the failures of some of the applications or systems are due to the lack of security during the development phase [27]. The results of this study shows that the professionals have knowledge and security training, but they did not know how to use and handle it in the earlier phase of application developments. The survey also indicated there is a lack of a complete set of standard or solutions for eliciting security requirements that can be applied during the process of applications development in order to achieve quality and secure applications. This study also found that the respondents used multiple solutions in handling the security issues rather that considering one solution only. Therefore, a proper elicitation process for security requirements needs to be provided for software professional who are not expert in security. It can help them to incorporate the available security knowledge (from standards, guidelines, procedure or checklist) into the security requirement elicitation activities.

The limitation of this work is the population biases. The survey was only conducted in Malaysia involving several organization involved in IoT industry, which do not represent the global view of the security requirements elicitation process of another software/system context. This study contributes to help the practitioners in IoT industry to understand common practices, whether the research on security requirement has contributed to real-world practices. It also helps the professional to evaluate the security requirements elicitation in the earlier phase in application developments especially in IoT industry. As a conclusion, future research may be done to develop a new approach in eliciting security requirements in IoT applications [28]. We also plan to develop an automated tool support for security requirements and technologies for IoT applications development.

ACKNOWLEDGEMENTS

The authors would like to acknowledge Universiti Teknikal Malaysia Melaka (UTeM) and Ministry of Higher Education (MoHE) for its support and the funding of this FRGS research grant: FRGS/1/2016/ICT01/FTMK-CACT/F00325.

REFERENCES

[1] A. H. Ahmad Helmi *et al.*, 'National Internet of Things (IoT) Strategic Roadmap', 2014.

[2] ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, no. November. 2017.

[3] H. Sundmaeker, P. Guillemin, P. Friess, and Sylvie Woelfflé, *Vision and Challenges for Realising the Internet of Things*, vol. 1, no. March. 2010.

[4] K. Rose, S. Eldridge, and L. Chapin, 'The Internet of Things: An Overview Undertanding the Issues of a More Connected World', 2015.

[5] M. R. R. Ramesh and C. S. Reddy, 'A Survey on Security Requirement Elicitation Methods: Classification, Merits and Demerits', *Int. J. Appl. Eng. Res.*, vol. 11, no. 1, pp. 64–70, 2016.

[6] M. M. R. Md. Alamgir Kabir, 'A Survey on Security Requirements Elicitation and Presentation in Requirements Engineering Phase', *Am. J. Eng. Res.*, vol. 2, no. 12, p. 7, 2013.

[7] O. Vermesan and P. Friess, *Internet of Things Applications - From Research and Innovation to Market Deployment*. 2014.

[8] A. Chakraborty, M. K. Baowaly, A. Arefin, and A. N. Bahar, 'The Role of Requirement Engineering in Software Development Life Cycle', *J. Emerg. Trends Comput. Inf. Sci.*, vol. 3, no. 5, pp. 723–729, 2012.

[9] H. El-Hadary and S. El-Kassas, 'Capturing Security Requirements for Software Systems', *J. Adv. Res.*, vol. 5, no. 4, pp.

463–472, 2014.

[10] I. Sommerville, *Software Engineering Ninth Edition*, Ninth. Boston, Massachusetts: Person Education, Inc., Addison-Wesley, 2011.

[11] E. Paja, F. Dalpiaz, M. Poggianella, P. Roberti, and P. Giorgini, 'STS-Tool : Socio-technical Security Requirements through Social Commitments', pp. 331–332, 2012.

[12] D. Mellado, E. Fernández-Medina, and M. Piattini, 'A Common Criteria based Security Requirements Engineering Process for the Development of Secure Information Systems', *Comput. Stand. Interfaces*, vol. 29, no. 2, pp. 244–253, 2007.

[13] B. Russell, C. Garlati, and D. Lingenfelter, 'Security Guidance for Early Adopters of the Internet of Things (IoT)', *Mob. Work. Gr. Peer Rev. Doc.*, no. April, 2015.

[14] E. Borgia, 'The Internet of Things Vision: Key Features, Applications and Open Issues', *Comput. Commun.*, vol. 54, pp. 1–31, 2014.

[15] J. Yang and B. Fang, 'Security Model and Key Technologies for the Internet of Things', *J. China Univ. Posts Telecommun.*, vol. 18, no. December, pp. 109–112, 2011.

[16] M. Selinger, A. Sepulveda, and J. Buchan, 'Education and the Internet of Everything', 2013.

[17] MIMOS Berhad, 'National Internet of Things (IoT) Strategic Roadmap: A Summary', 2015.

[18] P. John, 'Securing the "Internet of Things" Survey', 2014.

[19] J. Oltsik, 'The Internet of Things: A CISO and Network Security Perspective', 2014.

[20] G. Elahi, E. Yu, T. Li, and L. Liu, 'Security Requirements Engineering in the Wild : A Survey of Common Practices', *Comput. Softw. Appl. Conf.*, 2011.

[21] G. Islam and M. A. Qureshi, 'A Framework for Security Requirements Elicitation', no. May, 2012.

[22] D. M. Mendez, I. Papapanagiotou, and B. Yang, 'Internet of Things: Survey on Security and Privacy', pp. 1–16, 2017.

[23] M. Zolanvari, 'IoT Security: A Survey', 2010.

[24] T. Borgohain, U. Kumar, and S. Sanyal, 'Survey of Security and Privacy Issues of Internet of Things', *Cryptogr. Secur.*, p. 7, 2015.

[25] M. Rahman and S. Ripon, 'Elicitation and Modeling Non-Functional Requirements – A POS Case Study', *Int. J. Futur. Comput. Commun.*, vol. 2, no. 5, pp. 485–489, 2013.

[26] A. J. Franco, 'Requirements Elicitation Approaches: A Systematic Review', *IEEE 9th Int. Conf. Res. CHallenges Inf. Sci.*, pp. 520–521, 2015.

[27] C. Tankard, 'The Security Issues of The Internet of Things', *Comput. Fraud Secur.*, vol. 2015, no. 9, pp. 11–14, 2015.

[28] A. A. Ibrahim, M. Kamalrudin, and M. F. Abdollah, 'A New Approach to Elicit Security Requirements for Internet of Things (IOT) Application', in *Proceeding of Postgraduate Research Seminar in Conjuction with ISORIS 2017*, 2017, pp. 235–242.