IBIMA Publishing
Journal of Internet and e-Business Studies
https://ibimapublishing.com/articles/JIEBS/2020/937087/
Vol. 2020 (2020), Article ID 937087, 9 pages, ISSN: 2169-0391
DOI: 10.5171/2020.937087

Research Article

Investigating Cyber Readiness for IoT Adoption in Saudi Arabia

Meshari Alanazi and Ben Soh

Department of Computer Science and IT, La Trobe University, Melbourne, Australia

Correspondence should be addressed to: Meshari Alanazi; M.alanazi@latrobe.edu.au

Received date: 14 October 2019; Accepted date:12 December 2019 ; Published date:22 June 2020

Academic Editor: Donna M. Schaeffer

Abstract

There is a global trend towards the use of the 'Internet of Things' technology in smart applications like smart cities, energy engagement and others. However, this creates many electronic risks because of the IoT technical and technological nature. With multiple e-risks forms and types, it becomes necessary that each country develops protective measures so as to reduce the expected level of risk. Such measures can take the form of actions via legislatures or educating users and companies about the seriousness of this upcoming IoT technology. This can be done by identifying some types of cybercrimes, determining the required security requirements to maintain the security and privacy of users, and defining the actions and duties required by the government and software developers. However, to date, there has been a lack of qualitative and quantitative studies on the awareness of the IoT security risks that could constitute the first line of defence. This study employs a mixed-method approach to tackle the IoT potential threats in the Kingdom of Saudi Arabia, especially in government sector. While a descriptive survey method is utilized to collect information about the requirements of applying the Internet of things and its anticipated cybercrimes, a traditional screening method with combined analysis is applied to examine the role of national data centers, national information centers, different ministries and government departments in minimizing the cybercrime risks in Saudi Arabia.

Keywords: IoT, Cybercrime, Saudi Arabia.

Cite this Article as: Meshari Alanazi and Ben Soh (2020)," Investigating Cyber Readiness for IoT Adoption in Saudi Arabia", Journal of Internet and e-Business Studies, Vol. 2020 (2020), Article ID 937087, DOI: 10.5171/2020.937087

Introduction

The risks of Internet connectivity are growing rapidly with the widespread use of Internet of things technology or Next Generation Internet as this technique will allow space for tens of millions of intelligent systems (Smart Systems) to connect to the Internet (Gartner CIO, 2016). This technology will open up prospects and new ways for hackers to control the most Internet-connected devices, such as the steering wheel controls, operating rooms, baby monitors, devices with air conditioning and cooling control, and lighting, as well as other devices including aviation control towers, operating rooms, control missile, or any other device connected to the Web network.

Experts of information security technology and electronic crimes assert that we cannot eliminate cybercrimes, but we can reduce them, and their risks and impacts (Chris Folk, 2015). With multiple e-risks forms and types, it becomes necessary that each country develops protective measures so as to reduce the expected level of risk (Securing the Internet of Things, 2011). This is not limited to software manufacturers only, but to further include service providers, users, governments and regulations, legislation, and governmental and private bodies.

This study aims to determine the possible types of electronic crimes resulting from the application of the Internet of Things in Saudi Arabia and the expected risks, as a result of that application, as well as the actions required from software companies, service providers, governments and users. The study and the analysis will also include the governmental sphere beside the aim to address the impact of electronic crimes in the public sector.

Literature Review

The study (R. Roman, 2011) confirmed that the Internet of Things technology needs more research and mechanisms in order to maintain confidentiality and privacy. The results of the study confirmed that the big obstacle is security and confidentiality because of the risks threatening the safety of the use of the Internet of Things. The study recommended the need to reconsider the traditional security methods used in current applications, such as encryption protocols, reliability, property rights and security policies, as well as the need to reconsider government laws and regulations, in order to promote a concept of the Internet of Things that can be applied more safely.

In (Chris Fold, 2015), the researchers said that "there is a rapid progress in the Internet of Things technology, where it is expected that over the next few years, in 2020, the number of devices connected to the Internet , will be about 50 billion devices and that the trade volume will exceed trillions of dollars". This technical explosion requires the transition to technologies, new and sophisticated ones like IPv6 rather than IPv4, to enable the technical definition of this huge number of devices and control. This transition will create new problems for users. The new threats, called “action at a distance”, will create a new type of responsibility, laws and regulations, and protocols of computer security. The study suggested a change to the traditional security architecture (new IoT security model) in order to maintain the privacy, security, management of identification cards (Identity management) and data ownership and control in the IoT space. Also, the researchers have revealed, in the study, the compelling reasons for the reluctance of people to use online Internet services, such as purchasing, banking operations, the purchase of stocks, bonds and other business activities. Finally, the researchers proposed a "Service acceptance model" to explain why people refrain from dealing with electronic services.

The study (Wexter, 2014) proved that electronic crimes have significantly changed the role of the police in the community because these crimes are beyond borders. The research confirms that in 2013, a theft involving withdrawals from ATM machines for 10 hours resulted in a loss of $45 million. Recommendations of this study include increased awareness and law enforcement.

Problem Formulation and the Study

There is a global trend towards the use of the Internet of Things technology (Peter Friess, 2014). It is certain that the Internet of Things application will change the current way of life, in terms of investment, opening up new areas of work and saving energy and resources. At the same time, it will create many technical, technological, cultural and moral problems worldwide.

Many companies have started to prepare and equip the next generation of equipment and software to be ready for the Internet of Things. In fact, Samsung announced that 90% of its products by 2017 would contain the "Internet of Things" techniques, and in 2020, 100% of its products will contain this technology. Cisco predicted the Internet-of-Things-related businesses would be worth about 41 billion US dollars and become a trend for all global companies, including Saudi companies, to be on the same level of readiness and awareness. However, according to the views of the researchers, there are many challenges still facing the applications of the Internet of things, including creativity in integrating software applications in Internet devices, security, availability, maturity, complex integration and interoperability.

The field of Internet of Things security is one of the most complicated and sensitive research topics (Peter Friess, 2014). This is because of the problems faced by researchers, such as small Internet devices, limited storage, processing and power of the battery. There is a trend towards the use of intelligent systems to tackle IoT security problems that are progressing very fast in the areas, such as the identified risks and ways to protect them. However, to date, there has been a lack of proper qualitative and quantitative studies on the awareness of IoT security risks (Ovidiu Vermesan, 2014).

To that end, the problem of this study is formulated based on the following points (Ovidiu Vermesan, 2014) (Center, 2015):

- Build a model that is acceptable to all parties, producers and consumers, and that addresses confidentiality, privacy and reliability within a reliable work environment based on digital certificates and authentication protocols.
- Address the problems related to technical IoT security barriers.
- Propose solutions to the problems of bad ethical practices and their reflection on the cultures of the communities, and the development of legislations and procedures related to modern techniques.

The hypothesis of the study

The study is based on the following main hypothesis:

- There is an inverse relationship between Readiness for and Awareness of the Internet of Things and Cybercrimes. That is, the greater the level of Readiness for and Awareness of the Internet of Things, the fewer the cybercrimes.

The Significance of the Study

This study deals with an important and vital topic in the field of electronic crimes, on a worldwide level and in Saudi Arabia in particular, the challenges that accompany the new wave of electronic crimes, which are expected to expand and spread with the beginnings of using the "Internet of Things." In fact, the "Gartner Group" studies (Gartner CIO, 2016) predicted that the number of smart Internet-connected devices reaches about 25 billion a year in

2016, at a rate of 3.4 devices for each person of the world's population, and 50 billion devices at a rate of 6.5 for each person is forecast in 2020.

The IoT security risks should be faced by taking actions via legislatures, educating users and companies about the seriousness of this upcoming IoT technology. Although Saudi Arab has a legislation to counter cybercrimes (Gercke, 2012), the current legislation remains insufficient to cope with the IoT cybercrime sophistication.

Objectives of the Study

The study aims to achieve the following objectives:

1. Identify some types of security risks and electronic crimes, which threaten the future of technology "Intelligent Systems and the Internet of things" in Saudi Arabia.
2. Identify the required security requirements, to maintain the security, confidentiality, privacy of users and smart systems within Saudi Arabia.
3. Identify actions and duties, security standards, confidentiality required by the government, software development firms and service providers to reduce the risk of electronic crimes anticipated inside Saudi Arabia.
4. Publication of research papers including the results of the study, in conferences and scientific journals.
5. Prepare a list of the pilot used by law enforcement authorities (police and justice) in addressing the problems resulting from the application of the Internet of Things in Saudi Arabia.

Terms of the Study

Internet of Things (IoT): Is the network of physical objects or "things" embedded with electronics, software, sensors and network connectivity, which enables these objects to collect and exchange data. (Chris Folk, 2015).

- **Cybercrime:** cybercrimes (or cyberattacks) generally refer to criminal activities conducted via the Internet (Singleton, 2014).
- **Next Internet Generation:** a number of projects intended to improve Internet performance or content quality in regions of various sizes and locations. (Chris Folk, 2015).
- **Smart Device:** is an electronic device, generally connected to other devices or networks via different wireless protocols such as Bluetooth, NFC, WiFi, 3G, etc., that can operate, to some extent, interactively and autonomously (Riek, 2014).
- **Smart System:** incorporate functions of sensing, actuation and control in order to describe and analyze a situation and make decisions based on the available data in a predictive or adaptive manner, thereby performing smart actions (Wexler, 2014).

The Limits of the Study

A. The objective limits:

- Identifying possible types of cybercrimes resulting from the application of the Internet of Things in Saudi Arabia and the expected risks, as a result of that application, as well as the actions required from software companies, service providers, governments and users.
- Analysis of the impact of electronic crimes in the public sector and the statement of the government's measures to be taken to curb the phenomenon, at the legal level as well as at the judicial and procedural level.
- Defining the role of the national information centers and the Center for Rapid Response (CERT) in the reduction of the phenomenon, in

addition to the roles of ministries, government departments, volunteers, and the regulations and legislations in the reduction of electronic crimes.

B. The spatial limits:

- The topic of the study is readiness for and awareness of the Internet of Things. Although the phenomenon is cross-border, it will only be applicable in the Kingdom of Saudi Arabia.

C. The time Limits:

- Studying the readiness and awareness required for the application of Internet of Things technology is anticipated in the coming period of the next five years, according to reports and studies of information technology experts.
- Studying modern electronic crimes in less than five years old, and projecting them over the next period, according to reports, studies and security experts.

Methodology

This section describes the research and the methodology that will be applied to carry out the study. It discusses the research design, data collection, data analysis, study period and mechanisms to assure the quality of the study. It also describes the nature and source of the data sample size. The methods adopted for data collection are also illustrated, together with the reliability and validity of the research instruments' methods of data analysis and ethical considerations.

A. Study Design

This study uses mixed-method research involving a descriptive survey design in collecting information by administering questionnaires to a sample of the target population. The study will be aimed at collecting information from the respondents regarding readiness for and awareness of the Internet of things (IoT) in the Kingdom of Saudi Arabia. The investigator will use both primary and secondary data. While the primary data will be obtained using questionnaires, the secondary data will be collected from books, journals and the Internet. A survey will be used to determine the users' requirements for the application of the Internet of things phenomenon and related electronic crimes.

Traditional screening methods and standard testing techniques will be applied using analytical software. Examination and analysis processes will address a collection of previously published research similar to this study. The work of previous studies is compared with each other, and conclusions are drawn from them for the purpose of the current study.

B. Study population

The target population will form the basis of the selected sample from Saudi Arabia. It will include officials of service providers, software developers, users, leaders of relevant government agencies responsible for the equipment, officials of the legal authority (judiciary & police), directors of some private sector organizations, leaders of the Saudi national information centers and employees of Rapid Response Center (CERT).

C. Study Tools

The main data collection instruments used are as follows:

1. Survey questionnaires: Survey questionnaires have the advantage of achieving rapid contact with many people. It will be very useful for this research project to obtain responses to the diverse indicators that require consultations with

specific populations. The primary objective of the survey is to measure the awareness of the Internet of Things phenomenon and the risks associated with them. The results of this study are then analyzed using a specialized statistical analysis software

2. Interviews: The interview procedure is shedding the light on the research process through an informal conversation. As part of this research project, an interview guide will be drawn to make the interviews semi-structured. Interview questions will be written down and the interviewers will be trained so that they truly understand the subject matter as well as the responses they receive. To achieve the objectives of the study, the researcher will conduct interviews with some leaders of government and private agencies, individuals and service providers in Saudi Arabia.
3. A compendium of textual data: The compendium of textual data will primarily gather, organize and analyze diverse documents that contain information relevant to the topic of study, especially with regard to readiness for and awareness of the internet of things (IoT) in Kingdom of Saudi Arabia. The compendium of textual data will include: unpublished research; data dealing with cybercrimes; the security of smart and Internet of Things regulations; reports of hardware manufacturers, software and operating systems; the systems standard international reference reports; products of major international companies in the field; the security of smart systems and Internet of Things, in addition to research papers and studies, specialized projects, articles published in journals, refereed conferences, and technical reports on the subject of e-crimes arising from the application of Internet of things and the new wave of electronic crimes.

D. Data analysis methods

Quantitative analyses will be appropriate for this project with a bit of use of qualitative methods as well. Codes will be assigned to qualitative variables such as readiness for and awareness of the Internet of Things. The qualitative data analysis will be carried out using this coding strategy. The content study will be used to analyze the substantial body of data collected in this study with the following procedure:

1. Reading of collected data.
2. Definition of classification categories for the collected data.
3. The categorization of the collected data.
4. Quantification and statistical treatment of data.
5. The scientific description of the studied cases.
6. The interpretation of results.

For quantitative data analysis, both the descriptive and inferential statistics will be done to better understand the readiness for and awareness of the Internet of Things (IoT) security in the Kingdom of Saudi Arabia.

E. Mechanisms to Assure the Quality of the Study

- Data Privacy: Confidentiality will be enhanced in the research, and individuals filling in questionnaires will not be required to write their names. Relevant authorities will be contacted so as to gain permissions to carry out the research.
- Control of Bias: the researcher will make sure that the research study is objective, independent and balanced. The researcher believes that objectivity is critical to the success of scientific analysis. Thus,

the researcher will actively work to keep a neutral and objective research environment.

- Use accurate and most reliable data: To assure that the research study is useful, informative and understandable, data and information of the best quality will be used. The data and information used in the research study will be validated from multiple sources, and it will be assured that it is reliable and accurate.

Proposed Theoretical Framework

To achieve the objectives of the study, a model that has 5 layers is proposed:

- **Layer 1** (Introduction and Definitions) (information security - cybercrime - Internet of Things).
- **Layer 2** (Problem of the Study) (penetrations and types - types and classifications of hackers - security risks in cyberspace - the security risks that threaten the Internet of Things - jamming electronic internet connectivity - prevention and treatment methods - the role of software manufacturers - the role of service providers - the role of government and legislation - user role - description of the problem and the local and global impact).
- **Layer 3** (the New Wave of Electronic Crimes) (introduction and historical overview - types of anticipated dangers - kinds of the expected crimes - the source of such crimes as "state, age and interests" - an inventory of the most anticipated crimes - its impact on the Internet of things "locally and globally" - classification of electronic crimes according to various international standards, "the degree of risk, proliferation, easiness ").
- **Layer 4** (Analysis and Discussion) (analysis of the most anticipated crimes - classification of anticipated crimes by severity - the impact of electronic crimes on the agenda of each of the "public sector, private sector, civil society organizations, individuals and personalities" - the required measures to curb cybercrimes "required actions of software designers, the measures required from service providers, the measures required from governments, actions required from users "- the government's use of available mechanisms to speed the detection of the electronic" national information centers crimes, national data stores, government rapid response centers CERT " - the various ministries and government departments and their role in the speed detection of electronic crimes - volunteers of experts and citizens - the role of regulations and legislations in the reduction of the electronic crimes).
- **Layer 5** (Results of the Study - the recommendations of the study).

Conclusion and Future Work

The proposed work attempts to address the different types of potential Cybercrimes that face the advent of the Internet of Things (IoT), and to determine the required procedures and actions by software development companies, service providers, government agencies and users, before the IoT phenomenon invades the world. The work will tackle the IoT potential threats in the Kingdom of Saudi Arabia, especially in the government sector, where it is important to elaborate the government roles from different perspectives to minimize the cybercrime threats to the IoT. The roles of the legislations, national data centers, national information centers, different ministries and government departments are also important to help minimize the cybercrime risks. The future work aims to analyze the results and present the recommendations and findings in the study, and also, the results will be published in scientific journals and conferences.

References

- River, W., (2015). Security in the internet of things: Lessons from the past for the connected future.
- Russell, B., Garlati, C. and Lingenfelter, D., 2015. Security guidance for early adopters of the Internet of Things (IoT). *White paper, Cloud Security Alliance*.
- FTC, U., (2015). Internet of Things, Privacy and Security in a Connected World. Technical report, Federal Trade Commission. Jan. 2015. url: https://www. ftc. gov/system/files/documents/reports/ federal-tradecommission-staff-report-november-2013-workshop-entitled-internet-thingsprivacy/150127iotrpt. pdf.
- Folk, C., Hurley, D.C., Kaplow, W.K. and Payne, J.F., (2015). The security implications of the Internet of Things. *Fairfax: AFCEA International Cyber Committee*.
- Amiri-Kordestani, M. and Bourdoucen, H., (2017). A survey on embedded open source system software for the internet of things. In *Free and Open Source Software Conference* (Vol. 2017).
- Hassan, M.K.A., (2016). Governance, Risk and Compliance" GRC" for Internet of Things" IoT. *International Journal of New Technology and Research*, *2*(3).
- Castro, F., Miranda-Jiménez, S. and González-Mendoza, M., Advances in Computational Intelligence.
- Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S.L., Kumar, S.S. and Wehrle, K., (2011). Security Challenges in the IP-based Internet of Things. *Wireless Personal Communications*, *61*(3), pp.527-542.
- Friess, P., Ibanez, F. and Vermesan, O., (2014). Putting the Internet of Things Forward to the Next Level. *Internet of Things Applications–From Research and Innovation to Market Deployment.*
- Vermesan, O. and Friess, P. eds., (2014). *Internet of things-from research and innovation to market deployment* (Vol. 29). Aalborg: River publishers.
- Vermesan, O. and Friess, P. eds., (2013). *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers.
- Neisse, R., Steri, G., Baldini, G., Tragos, E., Fovino, I.N. and Botterman, M., (2014). Dynamic context-aware scalable and trust-based iot security, privacy framework. *Chapter in Internet of Things Applications-From Research and Innovation to Market Deployment, IERC Cluster Book*.
- Ziegler, S., Fdida, S., Watteyne, T. and Viho, C., (2016), October. F-Interop-online conformance, interoperability and performance tests for the IoT.
- Vermesan, O. and Friess, P. eds., (2014). *Internet of things-from research and innovation to market deployment* (Vol. 29). Aalborg: River publishers.
- Medagliani, P., Leguay, J., Duda, A., Rousseau, F., Domingo, M., Dohler, M., Vilajosana, I. and Dupont, O., (2014). Bringing ip to low-power smart objects: The smart parking case in the CALIPSO project. *Internet of Things—From Research and Innovation to Market Deployment*, pp.287-313.
- Vermesan, O. and Friess, P. eds., (2014). *Internet of things-from research and innovation to market deployment* (Vol. 29). Aalborg: River publishers.
- Sachowski, J., (2019). *Implementing digital forensic readiness: From reactive to proactive process*. CRC Press.
- Singleton, T., (2014). Understanding the cybercrime wave. *ISACA JOURNAL*, *1*(1), pp.1-5.
- Teplinsky, M.J., (2012). Fiddling on the roof: Recent developments in cybersecurity. *Am. U. Bus. L. Rev.*, *2*, p.225.

- Harding, L., (2017). *Collusion: Secret meetings, dirty money, and how Russia helped Donald Trump win*. Vintage.
- Moniz, R. and Eshleman, J., (2015). ACADEMIC LIBRARIES.
- Wexler, C., (2014). Critical Issues In Policing Series-The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime. Police Executive Research Forum, Washington, DC.
- Enterprise, H.P., (2015). How Safe Are Home Security Systems. *An HPE on IoT Security*.
- Folk, C., Hurley, D.C., Kaplow, W.K. and Payne, J.F., (2015). The security implications of the Internet of Things. *Fairfax: AFCEA International Cyber Committee*.
- Pal, G., (2016). Voice of the people: the case for biometrics in government. *Biometric Technology Today*, *2016*(5), pp.5-7.
- Viano, E.C., (2017). Cybercrime: Definition, Typology, and Criminalization. In *Cybercrime, Organized Crime, and Societal Responses* (pp. 3-22). Springer, Cham.
- Vermesan, O. and Friess, P. eds., (2014). *Internet of things-from research and innovation to market deployment* (Vol. 29). Aalborg: River publishers.
- Friess, P., Ibanez, F. and Vermesan, O., (2014). Putting the Internet of Things Forward to the Next Level. *Internet of Things Applications–From Research and Innovation to Market Deployment*, pp.3-6.
- Riek, M., Böhme, R. and Moore, T., (2014), June. Understanding the influence of cybercrime risk on the e-service adoption of European Internet users. In *13th Workshop on the Economics of Information Security*.
- Roman, R., Najera, P. and Lopez, J., (2011). Securing the internet of things. *Computer*, (9), pp.51-58.
- Singleton, T., (2014). Understanding the cybercrime wave. *ISACA JOURNAL*, *1*(1), pp.1-5.
- Wexler, C., (2014). Critical Issues in Policing Series-The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime. Police Executive Research Forum, Washington, DC.