Users Experiences with and Awareness towards IoT Privacy and Security and Analysis of related Cybercrime Laws in Saudi Arabia : Does your very own Smart Device Spy on you ?

By Abdalmajeed Alharthy (PhD)
Abdalmajeed.Alharthy@Canberra.edu.au
Faculty of Science and Technology
University of Canberra

UNIVERSITY OF CANBERRA

Abstract

Technology has changed the way people live completely and how they interact with each other. This relationship extends to machines in different ways. Humans can instruct machines to perform various functions depending on their needs. However, an even more interesting phenomenon informs the internet space, the internet of things. It involves the connection of devices between each other, easing productivity and eliminating the tedious process of operating machines directly. However, there are privacy and security issues involved. This research study will investigate what security, privacy and safety risk Internet of Things devices may bring, how aware people are about these risks, how the user can minimise the risk of being hacked or attacked and what manufacturers can do to make safer Internet of Thing devices.Moreover, this research study stands to examine IoT-related cybercrime legislation in Saudi Arabia. Following, a background that introduces the issue and defines the IoT phenomenon is provided. The research problem, questions and aim along with a list of objectives are also given. Following that, a brief literature review (to be developed further), and a methodology/approach and conduction of the research are introduced.

Introduction

In the recent past, even though the technology was still important, networking technologies were restricted to connecting to end-user devices such as mainframes, desktop and laptop computers, and later on smartphones. However, today, more than eight billion devices in the world connected to network technologies, excluding traditional devices (Yoo, 2016). They include virtual assistant devices like Alexa, vehicles, home appliances, wearable technologies, traffic controls, and smart televisions. Televisions, previously a means for delivering news can now connect to the internet and can receive and share information in ways that would have seemed impossible in the recent past (Yusufov & Kornilov, 2013). The connection of such devices to networks is predicted to rise to twenty-five billion devices by the end of 2020 (Yoo, 2016).

The different devices involved in IoT differ in the way they operate, depending on how they are set. However, they share various features. First, they store and process data in a distributed way, depending on the purpose and use of different devices (Yoo, 2016). This kind of storage is very different from the traditional centralized data centers. Moreover, these devices are sometimes referred to as cyber-physical systems. This name stems from the fact that they can collect data from the environment using installed sensors (Masoud, Jaradat, Manasrah, & Jannoud, 2019). They can also receive instructions from human beings when need be. The use of IoT devices makes work easier in different ways. It makes the delivery of services much faster and more convenient, and it allows people to monitor different devices without interfering with their functioning as well (Masoud, et al., 2019). The IoT is a phenomenon that holds so many opportunities that humanity is in the process of exploring.

However, as much as the IoT is a promising field that is budding with chances and opportunities, its development comes with various challenges that need to be mitigated (Van Kranenburg & Bassi, 2012). Connection to the Internet presents systems and devices to issues such as violation of privacy, breach of information, and destruction of information by infection with viruses (Hameed, Khan, & Hameed, 2019).

Cybercrimes have been on the rise since the invention of the internet, and the efforts of malicious hackers keep improving. Therefore, it is essential to keep advancing and being aggressive in retaliatory and preventative methods when it comes to the security of these devices and systems (de Bruijn & Janssen, 2017). According to a Samsung report, it is critical to secure every connected device by 2020 (Burgess, 2018). This warning indicates that exists a possibility of cyber-security issues increasing as technology is also advancing. One of these significant issues revolves around espionage. The FBI provided a report showing that smart TVs could be monitoring and policing everything a user does while watching TV (Brown, 2019). It is a violation of privacy to do so, and there is a need to comprehend the issue further. Graham (2020) provides a systematic guide on how to stop the spying through the TV, showing that the spying is indeed a serious issue.

Moreover, such advanced technologies are no longer a problem that only applies to wealthy people and those in developed countries. These devices and systems are everywhere today, and the majority of the world has one or more devices connected to a network (Dahir, 2018). It is much easier for cyber-criminals to go undetected in developing countries, where retaliation processes are much less advanced (Kshetri, 2010). Therefore, resilient measures to educate people on matters of cyber-security and to empower them to protect themselves are necessary in all demographics in the world.

Research Question

1. What are the users' experiences with and awareness of information security, privacy, and safety issues with the IoT in Saudi Arabia?
2. How widespread is IoT-related cybercrime in Saudi Arabia?
3. How effective is IoT-related cybercrime laws in Saudi Arabia to combat IoT-related cybercrime?
4. What are the current countermeasures to combat IoT-related cybercrime?

Research Aim and Objectives

There are opportunities for Saudi Arabia IoT cybercrime legislation to explore the protection of user's information, privacy, and safety. The study aims to explore both the Saudi users' experiences towards information security, privacy and safety issues with the Internet of Things and to examine IoT-related cybercrime legislation in Saudi Arabia context. In line with the research aim, the following primary research objectives are identified:

Objectives related to the research questions:

I. To explore users' awareness of information security, privacy and safety issues with IoT in Saudi Arabia.
II. To observe users' experiences with information security, privacy, and safety issues with IoT in Saudi Arabia.
III. To gauge the level of awareness of information security issues among uses is smart devices, such as smart TVs.
IV. To gauge the level of understanding of measures of protecting their information among users of smart devices in Saudi Arabia.

To explore the degree of IoT-related cybercrime in Saudi Arabia to determine the current threats.

To determine effective IoT-related cybercrime laws in Saudi Arabia .

To identify the current countermeasures to combat IoT-related cybercrime to provide the best advice and recommendations for combating expected future of IoT-related cybercrime .

Methodology/approach

This research study proposes to adopt a mixed-methods approach (Schoonenboom & Johnson, 2017). A mixture of quantitative and qualitative approaches may provide more promising outcomes and a better understanding of the research problem (J. Creswell & Poth, 2017; J. W. Creswell, 2009).

The research study will involve a survey of people who have experience using IoT devices and are aware of the issues that surround the devices, and identify how to protect their devices and systems from privacy, security, and safety concerns. This research study proposes to have two main sections: one is the major users' experiences with IoT. This section will include analysis of respondents' experiences and their awareness towards information security, privacy and safety issues in Saudi Arabia. In other words, this section with considering the IoT in Saudi Arabia, gauging the people's awareness of IoT, the security issues involved, and ways of mitigating the risks. The method of data collection in this section will be questionnaires. The questionnaires will test the awareness of users of IoT devices and their experiences using them. Online forms, social network sites, and other Web 2.0 tools will be used for recruiting the study participants.

The second part of this research study is an analysis of the current legislations and countermeasures used to combat IoT-related cybercrime in the country.

This research study proposes to combine two research designs; a descriptive design and an exploratory design. In one hand, the descriptive design would be used to obtain valuable data concerning the status of the topic. Likewise, it can produce a large amount of rich data, which lead to significant theoretical and practical recommendations. On the other hand, the exploratory design would help in conducting this research, given that not much is understood about the research problem (University of Southern California, 2020). Through reviewing literature and different relevant sources to this research area, the study will introduce the Saudi Arabian background emphasising on the Internet of Things. It will investigate the current situation of IoT-related cybercrime in the country.

Limitations of the Research

The research will be limited to Saudi Arabia.

References

Brown, A. (2019, December 9). Your Smart TV could be watching EVERYTHING you do on the sofa, FBI cautions Retrieved 18 July, 2020, from https://www.express.co.uk/life-style/science- technology/1214042/Smart-TV-Spying-On-You-FBI-Warning
Burgess, M. (2018). What is the Internet of Things? WIRED explains. *WIRED, February 16th, www. wired. co. uk/article/internet-of-things-what-is- explained-iot, accessed July 10th*.
Creswell, J., & Poth, C. (2017). *Qualitative inquiry and research design: Choosing among five approaches*: Sage publications.
Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Method Approaches*: Sage Publications, Inc.
Dahir, A. L. (2018). Half the world is now connected to the internet-driven by arecord number of Africans Retrieved 20 July, 2020, from https://qz.com/africa/1400997/more-than-half-of-worlds-population- using-the-internet-in-2018/
de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7.
Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal of Computer Networks and Communications, 2019*.
Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly, 31*(7), 1057-1079.
Masoud, M., Jaradat, Y., Manasrah, A., & Jannoud, I. (2019). Sensors of Smart Devices in Internet of Everything (IoE) Era: Big Opportunities and Massive Doubts. *Journal of Sensors, 2019*. doi: 10.1155/2019/6514520
Schoonenboom, J., & Johnson, R. B. (2017). How to Construct a Mixed Methods Research Design. *KZfSS Kölner Zeitschrift für Soziologie und Sozialpsychologie, 69*(2), 107-131. doi: 10.1007/s11577-017-0454-1
University of Southern California. (2020, 1 April, 2020). Research Guides Retrieved 04 April, 2020, from http://libguides.usc.edu/writingguide/researchdesigns.
Van Kranenburg, R., & Bassi, A. (2012). IoT challenges. *Communications in Mobile Computing, 1*(1), 9.
Yoo, C. (2016). The Emerging Internet of Things: Opportunities and Challenges for Privacy and Security Retrieved 19 July, 2020, from https://www.csiponline.org/articles/emerging-internet things?gclid=CjwKCAiAy9jyBRA6EiwAecIQhNSjK7R04DnLiXOicgLhWVk4v7cEyeE3cCgEpYIP5nFRQaEmJhtSiyhoC81YQAvD_BwE
Yusufov, M., & Kornilov, I. (2013). *Roles of smart TV in IoT-environments: a survey*. Paper presented at the 2013 13th Conference of Open Innovations Association (FRUCT).