Ethical issues and Security Challenges with IOT in Saudi Arabia

Yasir Javed[1, 2], Zafar Iqbal Khan[2], Yousef Aldawlatli [2] and Abdulaziz Alharthi[1]
[1]Network Security Research Group, Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak.
[2]Prince Sultan University, Riyadh, KSA
yjaved@psu.edu.sa

Abstract- This paper presents Ethical issues and Security challenges at that are related with Internet of Things. The goal of this IoT paper is to have a background about IoT and its issues. We looked for the most important issues. The most important issues were Ethical and Security. These are the most important sides that will influence our lives and how information. In terms of Ethical issues, we will look at the information how it will be stored and used, and in terms of Security how the attacker attack and use the information that is provided by IoT devices. This paper presents the ethical and security challenges in area of IoT. It also highlight the key issues identified in literature to raise the awareness about ethical issues in IoT.

Index Terms- IOT, Security, Privacy, Attacks, Personal Data

I. INTRODUCTION

In the broadest sense, the term IoT encompasses everything connected to the net, however it's progressively getting used to outline objects that "talk" to every other node. "Simply, the internet of Things is created of devices – from easy sensors to smartphones and wearables – connected together," Matthew Evans, the IoT programmer head at tech UK, says. By combining these connected devices with automatic systems, it's attainable to "gather info, analyze it and build an action" to assist somebody with a selected task, or learn from a method. In reality, this ranges from sensible mirrors to beacons in retailers and on the far side. "It's regarding networks, it's regarding devices, and it's regarding knowledge," Caroline Gorski, the top of IoT at Digital Catapult explains. IoT permits devices on closed personal net connections to speak with others and "the internet of Things brings those networks along. It provides the chance for devices to speak not solely among close silos however across totally different networking varieties and creates a far additional connected world [1].

As mentioned IoT is simply made of sensor up to very big and complex systems that send, receive and maybe store store data or information about the users and can these data or information can be used to help or assist someone in a specific task. So it's very clear that this technology can be danger from those who don't know much about how these devices works. Specially in Saudi Arabia because we thought that must of the people here don't have a very clear idea about these devices and their issues with regards to the user's privacy. So we did this research paper in order to measure or at least have an idea about the level of knowledge that people in Saudi Arabia have about IoT. And in order to do so, we have made a survey that checks the knowledge of people in this country and we will show, discuss and summaries the result the we have found in this paper.

Since the data that these device send, receive and store can be personal data and these data will be transferred through the Internet, this means that these data or information can hacked and stolen. So from that, we think that people should know the danger of these device and also the must know what type of data these devices are collecting from them. So if they are aware of these ethical issues of these devices and the also aware of of type of data these devices are collecting from them, this will help this alot about how to use these devices and what information the shouldn't rely on these devices in order for their information not to be hacked. So that why this research paper is important for people in Saudi Arabia [2].

In this research, we have tried our best to cover as many people as we can. Also we focused on having both gender participating in the survey that we made, in order to see if there is any relation between the gender the knowledge of IoT in Saudi Arabia. Lastly, we Also focused on having all ages participate in the survey in order to cover anything that may have an impact on the result of our survey.

Last thing, our goal of the entire research paper is to assist or help people in Saudi Arabia about this new trendy topic, which is IoT or Internet of Things. Also we would like to have an idea about people how live in this country and their knowledge about IoT devices and Internet of Things as a concept. Lastly, the very important goal of our research is to give people or tell them about the issues that these devices can have, and how to protect them from these issues by giving some steps and guidelines that will help them to gain the best from the IoT devices and avoid as much as possible there issues.

II. SECURITY CHALLENGES

Authentication: Authentication in IoT context refers to that different IoT devices or nodes need to be authenticated in the routing peer in in order to transfer data. There are two main challenges with regards to the efficiency deployment and management authentication. First, one is generating the cryptographic key while the generation of key must be least cost, as IoT nodes cannot handle this. The second one is that, the guaranteed of the Certificate Authority (CA) is almost absent in The IoT context and it has been replaced with some mechanisms

to validate the cryptographic key and making sure of the integrity key [3].

Authorization and access control: The difference between the Authentication and the Authentication of access control is that, access right of resources to how to access each resource. Every node should support up to specified number of mechanisms to verify the access and checking that it should be different than the connected object to the same node. Because of all that, the deployment and management of the Authentication and the Authentication of access control is challenging in the IoT context [4].

Privacy: IoT and privacy are tied in a very strong relationship. Most of the IoT devices collects information of surroundings or personal data such as health care. IoT devices can collect private information or data about people without even them noticing that. There are regulation that guides user to manage the privacy and keep their data private [5].

III. LITERATURE REVIEW

1) Luigi et al [6] conduced a survey on IoT addressing the usage of IoT. According to Luigi Atzori,Antonio Iera, Giacomo Morabito in The Internet of Things: A survey. Their main purpose of this paper is to address the main concept of IoT, RFID and explain their uses. Also, talking about how to enable this variety technology and how to let them help us in our daily life. The research paper talks about identification, sensor and communication technologies. And then some application was reviewed in this paper. such as healthcare, educational and social domain. The list goes on. The outcomes of this research is describing how IoT changes our life.
2) According to Security in the Internet of Things [7]: A Review. This article focuses on security and privacy issues. The main focus also was on the application of this technology. The introduction was about how to secure architecture secure feature, secure requirements. The most important is that this research paper talk about the challenges of using IoT. But several aspects were not addressed. For example, did not address how to secure your privacy information from using it in marketing or just storing it. Also, this paper did not talk how our information were analyzed to some several purposes.
3) According to Internet of Things security and forensics: Challenges and opportunities. Also, this article explains the basic idea of the IoT technology. Then directly jump to the security challenges around the environment [8].

4) According to Impact of Internet Usage in Saudi Arabia [9] [10]: A Social Perspective. This paper introduces how IoT has started in Saudi Arabia in 1990s. This paper is good sample for survey paper, it has variety questions that may be help us to understand the trend in Saudi Arabia.

IV. METHODOLOGY

The technique that we have used in this research paper was the survey. We think that people here in Saudi Arabia will participate in survey forms more than any other option due to that it's easy to participate and choose the answer from multiple choice questions. Instead of writing, ask them to write their answers, which will consume a lot of time.

We used the google forms to survey people in Saudi Arabia. In addition, we have shared the survey through different applications and other things. We have used for example WhatsApp, twitter and Facebook.

We design the Google Form to make sure we get all what we need to complete this research paper. We have asked for the gender, age, country for getting the general needed information. In addition, we have asked some questions specifically for IoT and the awareness of it. In addition, we have asked some open questions for the participants to get their full opinions and thoughts about IoT devices and technology.

We used google excel due to that google forms supports transferring the data to google excel easily and fast. In addition, from the excel sheet, we have generate charts that represents the actual data in order to come up with some useful information from our survey. We also used some restrictions to analyses the data, for instance we have focused on the age and the level of knowledge about IoT since we thought these are the most important ones to write this paper.

The questions are:

A. What kind of knowledge you have about IoT

B. Have you ever used some application of IOT?

C. have you ever know what are the risks of using IOT on privacy ?

D. Do applications store and use your personal data ?

E. If Yes, in your opinion does this break your privacy?

F. Do you know that your personal data or your IoT devices' data can be sold for advertising purposes?

G. would you allow your family to use IOT applications?

H. would you feel more safe in a IOT if others use the information and data about you?

I. Do you agree with this saying "Business systems that would gain greatest value from IoT data"

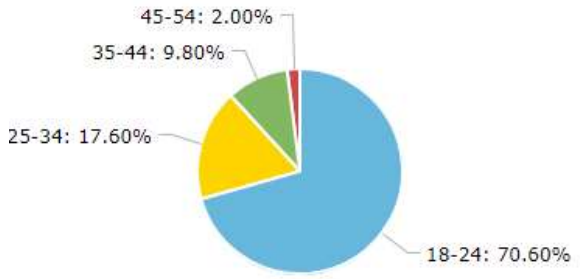

Fig1: Awareness of IOT issues

As shown in figure 1 we Asked several questions about using IoT, and others measure the awareness in people about IoT knowledge. We are focusing on Saudi Arabia.

Here we have to illustrate the most balance results

Gender	*Age*	*Background about IOT?*	*Their level*
Male=42	18 – 24	Yes = 39	Intermediate = 31

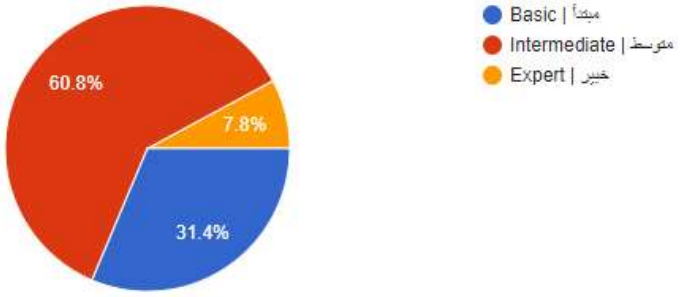

Figure 1 What kind of knowledge you have about IoT

VI. Analysis of Results

The technique that we have used in this research paper was the survey. we think that people here in Saudi Arabia will participate in survey forms more than any other option due to that it's easy to participate and choose the answer from multiple choice questions. We have used for example WhatsApp, twitter and Facebook. We used google sheets as supported by Google forms. We also used some restrictions to analyses the data, for instance we have focused on the age and the level of knowledge about IoT since we thought these are the most important ones to write this paper.

V. Results

The result shows that awareness among young people in IoT is much then older people. People aged 18 to 34 holds almost 88% of time knowledge to IOT while others don't. In order to test the knowledge we see that many youngsters have at least intermediate knowledge that shows their interest as well as contribution of colleges and univeirsties.

VII. CONCLUSION

In this paper, we have focused on the ethical issues and security challenges of Internet of Things. we have made and published a survey to see or measure the awareness of IoT security challenges and ethical issues in Saudi Arabia. we have introduced the important challenges and issues regarding this topic. Also we have collected and analyzed the data or information that we collected from the

References

[1] Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 200.

[2] El-Rahman, Sahar A., et al. "A Secure Cloud Based Digital Signature Application for IoT." International Journal of E-Services and Mobile Applications (IJESMA) 10.3 (2018): 42-60.

[3] Javed, Yasir, et al. "EEoP: A Lightweight Security Scheme over PKI in D2D Cellular Networks." Journal of Telecommunication, Electronic and Computer Engineering (JTEC) 9.3-11 (2017): 99-105.

[4] Javed, Y., Khan, A. S., Qahar, A., & Abdullah, J. (2017). Preventing DoS Attacks in IoT Using AES. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(3-11), 55-60.

[5] Khan, A. S., Javed, Y., Abdullah, J., Nazim, J. M., & Khan, N. (2017). Security issues in 5G device to device communication. IJCSNS, 17(5), 366.

[6] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." *Computer networks* 54.15 (2010): 2787-2805.

[7] Sait, Sadiq M., et al. "Impact of internet usage in Saudi Arabia: A social perspective." *International Journal of Information Technology and Web Engineering* 2.2 (2007): 81.

[8] Said, Omar, and Mehedi Masud. "Towards internet of things: Survey and future vision." *International Journal of Computer Networks* 5.1 (2013): 1-17.W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[9] Ukil, A., Bandyopadhyay, S., & Pal, A. (2014, April). IoT-privacy: To be private or not to be private. In 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 123-124). IEEE.

[10] Lin, H., & Bergmann, N. (2016). IoT privacy and security challenges for smart home environments. Information, 7(3), 44.