Open Challenges in Internet of Things Security

Ali Selamat
Media and Games Center of Excellence (MaGiCX) UTM & School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, 81310 Skudai, Malaysia
E-mail: aselamat@utm.my

Zeinab Selamat
School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, 81310 Skudai, Malaysia
E-mail: gold_beesan@yahoo.com

Abstract. The uses of internet of things (IoT) is increasing exponentially, number of connected devices became (according to reports) larger than human population, the uses of IoT applications involved of all aspects of our lives, and the data itself that is collected and transmitted by IoT devices and networks is very sensitive and need to be secured. All those reasons create and increase the need for improving IoT security solutions. In this paper, IoT security challenges was explored collected and categorized, for the purpose of having big picture for the situation. Number of researches during the last three years were studied to find out the still open challenges in IoT security, we also determined the different types of challenges categorization that was used by the researchers, and finally, we select a bigger sample of researches to discover the trend in IoT security challenges, and the changes happened during the last five years. The result of the analysis gives a clear idea about the importance of IoT security, it provides us of motivation for more researches in this area.

1. Introduction
With the emergence of a new generation of smaller and cheaper wireless devices and objects (e.g RFID), and the prediction by Cisco of the extremely increasing in connected devices by 2020: there will be 50 billion connected devices serving 7.6 people, with the rate of 6.6 devices/person [1, 2]. IoT devices has limitations in resources, usually less processing, and less power supply, also different environment, problems in software updates, usually not recommended to restart for software updates. Sometimes interactions in IoT need to deal with huge numbers of nodes, which may lead to serious security problems in an uncontrolled environment [3, 4].

Many researches have been discussed the IoT security challenges from different point of view, we select three classifications to collect different types of security challenges; some researches focused on the IoT layered architecture, other discovered challenges based on IoT applications, the third classification studied IoT security requirements, then extract challenges that faces each requirement.
In this article, we focused on the IoT security challenges and its classifications without going in-depth with details, to achieve the purpose of this paper, which is to view of the big picture of IoT security - still open challenges, and its classifications. Also, to analyse and explore the trend in the selected area, and the rank for each challenge. In the discussions, we take a broad view of different classifications that were studied in recent researches.

2. IoT security challenges

Many studies have been published in the previous few years in the IoT area. General issues were mainly the subjects of these surveys, security and privacy have been the most presented issues in IoT area. As mentioned in [3], many researches have focused on studying security challenges in IoT, researches have followed different ways for categorizing these challenges. Where the other researchers; [3], and [5] worked on the IoT security features itself, like availability, integrity, privacy, etc.

Security and privacy have been shown as a joint as a single term in many papers. We selected six studies that was published in the previous two years discussing IoT security challenges. In [6]; the researchers discussed IoT security challenges from the perspective of IoT networks, based on five selected requirements; privacy, confidentiality, secure routing, robust management and attack detection for both DDoS and insider attacks, privacy, lightweight cryptographic which is highly required in IoT networks and suitable for its special characteristics. In addition to privacy, lightweight cryptographic which is highly required in IoT networks and suitable for its special characteristics. Where in [7], the researchers started from the four-layers architecture in exploring IoT security challenges. Figure 1 shows security challenges from the IoT architecture view.

![Figure 1. Security challenges based on four-layer IoT architecture.](image)

2.1. Security challenges based on IoT application

When studying security challenges that faces IoT and the possible threats based on requirements for each application and its characteristics. We found the following:
- Smart home, which is responsible for controlling, monitoring home devices remotely using smart phone applications [8, 9], needs to achieve privacy, availability, trust, access control, authentication [10] as application security requirements, and faces Application challenges such as system access panel, gateway connection, remote access [10].

- Smart grids, which is responsible for improving cost and enhancing energy consumption [11], needs to achieve availability, confidentiality, data integrity, privacy, trust, and non-repudiation [5, 12, 13], faces challenges such as heterogeneity, scalability issues, information system vulnerability [5, 12, 13].

- Smart city, includes e-Gov, street lighting, water and waste management [14], need to achieve confidentiality, authentication, data integrity, and availability of information [15] as a security requirements, and faces high heterogeneity, scalability, as well as data management issues [15] for the reason of large scale network.

- Smart healthcare, which responsible for healthcare management and processes such as utilizing smart health cards [16], suppose to support authentication, confidentiality and integrity, and privacy [5, 17], as a security requirement, faces challenges such as resource limitation, mobility, and heterogeneity [5, 17].

![Figure 2. Possible threats based on IoT application.](image-url)
• Smart manufacturing, which can support creation of smart factories delivering cost-effective, efficient sustainable and safe manufacturing systems [5], it needs to achieve confidentiality, authentication, data integrity, and availability of the system [5] as security requirements.

• Smart transportation, which responsible for controlling traffic, parking and public transportation [18], with the importance to achieve availability, authentication, non-repudiation, and privacy [5, 19, 20] as security requirements, and faces high mobility, heterogeneity, diversity of attacks [5, 19, 20].

2.2. Security challenges based on IoT requirements
For the seven IoT security requirements, which were found in the selected literatures, we addressed the following security challenges:

• Privacy: many security challenges for privacy requirement, include profiling and tracking localization, and secure data transmission[6], user data that is generated by end devices [21], a huge data volume also produce a challenge, with streaming data processing, composability, personalization, secure and anonymous Communication, interaction-enhancing and compliance-enhancing techniques, privacy challenges at application layer[7], beside access privacy[3]. Other challenge based on how to offers an attractive trade-off between sensitive information utility and privacy protection[22].

• Trust: heterogeneous networks [3] [23] [22], and cross-domain identification and trust [22] are the biggest challenge that face trust requirements, where Lightweight primitives, consume low resources[6] face confidentiality requirement, also we have secure route establishment, isolation of malicious nodes[3], self-stabilization of the security protocol, and preservation of location privacy[6], all affect secure routing requirement.

• Access control and Identification/ authentication requirements face the following challenges; credential management between different entities, scalability, security attackers[3]. Access control and privilege management [22], cyber-attacks, scalability (large number of objects), and continuous changing in the networks [3]. Finally; for Attack detection, we found many challenges include resource efficient DoS attack detection, resource efficient insider attack detection[6], impersonation/identity spoofing, data tampering, and unauthorized control access [22].

3. Discussion and conclusions
The importance of IoT security comes from several points, as follows:

• IoT is growing in a very fast way and will become more involved in almost all our daily life activities, which increase the need of availability and security.

• IoT security challenges are different from those in the Internet, and the traditional techniques is not suitable for IoT.

• IoT security is a critical issue because of the very sensitive data that is collected and transmitted by IoT devices.

• The combination of IoT components has heterogenous technologies inside, which is not easy to close all security gaps with one magic solution.

In this paper, we have explored recent researches that studied IoT security challenges, we found three major classifications based on the following: IoT layered architecture, IoT applications, and IoT security requirements. For classifications based on IoT four-four layered architecture; perception, network, middleware, and applications, the challenges were collected and arranged in figure1. For the
classifications based on IoT applications, we have selected six IoT applications, then possible threats that may affect each application were addressed and shown in figure 2. For challenges based on IoT security requirements classification, the following security requirements was determined; privacy, trust, access control, identification, authentication and attack detection. The challenges were listed section 2.2.

We performed analysis for IoT researches to find out the importance of the area, and research trends in IoT security, the selected sample is researches that was published during the last five years; from the starting of 2014 to the end of 2018 and was resulted from Scopus database search engine. We found the following;

- IoT research interests has been increased exponentially in all IoT applications, with the highest rate for both smart cities and smart healthcare applications, and lowest rate for smart manufacturing, as shown in figure 3 and 4.
- Privacy as IoT a security requirement is the highest rate challenge that was analysed and discussed in research, access control and authentication/authorization in the second level, where connaturality is the lowest one.

![Figure 3. Number of published papers during (2014-2015) based on application.](image1)

![Figure 4. Number of published papers during (2014-2015) based in security requirement for each application.](image2)

Acknowledgments
The research is supported by Universiti Teknologi Malaysia (UTM) under Research University Grant Vot-20H04, Malaysia Research University Network (MRUN) Vot 4L876 and the Fundamental Research Grant Scheme (FRGS) Vot 5F073 supported under Ministry of Education Malaysia.

References
[1] Evans, D., *The Internet of Things, How the Next Evolution of the Internet, Is Changing Everything*. April 2011, Cisco Internet Business Solutions Group (IBSG).
[2] Kremenova, I. and M. Gajdos, *Decentralized Networks: The Future Internet*. Mobile Networks and Applications, 2019: p. 1-8.
[3] Riahi Sfar, A., et al., *A roadmap for security challenges in the Internet of Things*. Digital Communications and Networks, 2018. 4(2): p. 118-137.
[4] Vasilomanolakis, E., et al. *On the Security and Privacy of Internet of Things Architectures and Systems*. in *Proceedings - 2015 International Workshop on Secure Internet of Things, SiIoT 2015*. 2016.
[5] Kouicem, D.E., A. Bouabdallah, and H. Lakhlef, *Internet of things security: A top-down survey*. Computer Networks, 2018. 141: p. 199-221.

[6] Hameed, S., F.I. Khan, and B. Hameed, *Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review*. Journal of Computer Networks and Communications, 2019. 2019.

[7] Li, C. and B. Palanisamy, *Privacy in Internet of Things: From Principles to Technologies*. IEEE Internet of Things Journal, 2019. 6(1): p. 488-505.

[8] Raja, S. and K. Mandour, *Smart Homes: perceived benefits and risks by Swedish consumers*. 2019.

[9] Rani, K.G., S.R. Kishore, and B. Dhanne, *An intelligent universal remote control for home appliances*. Indian Journal of Public Health Research & Development, 2018. 9(11): p. 2066-2069.

[10] Ali, B. and A. Awad, *Cyber and physical security vulnerability assessment for IoT-based smart homes*. Sensors, 2018. 18(3): p. 817.

[11] Bi, Z., G. Wang, and L.D. Xu, *A visualization platform for internet of things in manufacturing applications*. Internet Research, 2016. 26(2): p. 377-401.

[12] Dalipi, F. and S.Y. Yayilgan, *Security and privacy considerations for IoT application on smart grids: Survey and research challenges*. in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). 2016. IEEE.

[13] Khelifa, B. and S. Abla, *Security concerns in smart grids: Threats, vulnerabilities and countermeasures*. in 2015 3rd International Renewable and Sustainable Energy Conference (IRSEC). 2015. IEEE.

[14] Zhu, C., et al., *Green internet of things for smart world*. IEEE Access, 2015. 3: p. 2151-2162.

[15] Zhang, K., et al., *Security and privacy in smart city applications: Challenges and solutions*. IEEE Communications Magazine, 2017. 55(1): p. 122-129.

[16] Aman, W. and E. Snekkenes, *Managing Security trade-offs in the internet of things using adaptive security*. in 2015 10th International Conference for Internet Technology and Secure Transactions (ICITST). 2015. IEEE.

[17] AL-mawee, W., *Privacy and security issues in IoT healthcare applications for the disabled users a survey*. 2012.

[18] Jing, Q., et al., *Security of the Internet of Things: perspectives and challenges*. Wireless Networks, 2014. 20(8): p. 2481-2501.

[19] Gerla, M., et al. *Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds*. in 2014 IEEE world forum on internet of things (WF-IoT). 2014. IEEE.

[20] Leng, Y. and L. Zhao, *Novel design of intelligent internet-of-vehicles management system based on cloud-computing and internet-of-things*. in Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology. 2011. IEEE.

[21] Sadique, K.M., R. Rahmani, and P. Johannesson, *Towards security on internet of things: Applications and challenges in technology*. in Procedia Computer Science. 2018.

[22] Zhou, W., et al., *The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved*. IEEE Internet of Things Journal, 2018: p. 1-1.

[23] Alaba, F.A., et al., *Internet of Things security: A survey*. Journal of Network and Computer Applications, 2017. 88: p. 10-28.