IoT Security: Review and Future Directions for Protection Models

Awad M. Awadelkarim Mohamed
Faculty of Computers and Information Technology
University of Tabuk, Tabuk, Saudi Arabia
awad@ut.edu.sa

Yahia Abdallah M. Hamad
College of Computer Science and Information Technology
Sudan University of Science and Technology, Sudan
yahia@sustech.edu

***Abstract*—Nowadays, Internet of Things (IoT) has gained considerable significance and concern, consequently, and in particular with widespread usage and adoption of the IoT applications and projects in various industries, the consideration of the IoT Security has increased dramatically too. Therefore, this paper presents a concise and a precise review for the current state of the IoT security models and frameworks. The paper also proposes a new unified criteria and characteristics, namely Formal, Inclusive, Future, Agile, and Compliant with the standards (FIFAC), in order to assure modularity, reliability, and trust for future IoT security models, as well as, to provide an assortment of adaptable controls for protecting the data consistently across all IoT layers.**

Keywords—IoT Security, Security Models, IoT Security Models, Formal Security Models, IoT Security Standards.

I. Introduction

The Internet of Things (IoT) is the third wave of the IT transformation that will introduce the primitive and resource constrains devices having the ability to be identifiable and a capability to communicate and interact with the Internet world [1]. The first time IoT concept becomes popular was in 1999 by Kevin Ashton, a British technologist at Massachusetts Institute of Technology (MIT). For Kevin Ashton, the meaning of the IoT and the consequences of its implementation in our environments, eventually, to have devices and systems knew everything about things, so everything can be tracked and registered, and considerably use such datum to serve humanity and the universe. [2].

Over time and due to its evolving nature, several organizations and research centers have been involved and contributed on attempting to provide a common definition for IoT. Internet Engineering Task Force (IETF) defined IoT as *" the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with the manufacturer, operator and/or other connected devices"* [3]. The International Telecommunication Union (ITU) defined the term on its ITU-T Y.2060 (06/2012) Recommendation as *"a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"* [4]. The Institute of Electrical and Electronics Engineers (IEEE), however, described the phrase "Internet of Things" on its IEEE "Internet of Things" 2014 special report as *"A network of items—each embedded with sensors—which are connected to the Internet"* [5].

Considering the usage perspective, IoT has been widely applied in various applications and more IoT devices are coming online every day pushing the world toward a new era of technology. Moreover, the estimated growth of IoT connected devices is been expected to reach about 50 billion objects by 2020 [6]. This is ranging from Wearable devices to business model. The Wearable devices record large amounts of data by measuring signals around the body, and they come in many different forms such as wristbands, armbands, watches, and headbands [7]. Whilst, the IoT implementation and business model come in use in different sectors, such as:

- Building sector: which includes smart cities, smart home consumer and home sector, consumer products, home products.
- Public Sector: this is a wide range of domains that include, but are not limited education, transportation, public security and safety, public safety, public security, law enforcement, smart health care and connected medical devices, continuous patient monitoring, medical therapy [8], transport system [9], Manufacturing, factory, smart products [10], agriculture [11], environment monitoring [12].
- Energy Sector: Oil and gas, smart grid, energy management [13, 14].

In fact, a considerable number of manufactures and service provider companies took such great opportunities, *(i.e. IoT is presented),* to build new business models, improve internal efficiencies, and serve customers better. Therefore, they have started developing and enhancing their business line models by adding and deploying IoT into their existing network in a rapidly scale. However, they are, accidentally or intentionally, forgetting or neglecting the new diverse threat landscape that IoT brought over. The IoT ecosystem poses new security challenges that extend beyond traditional data security because of the unique IoT multi-tier network and the used architecture nature. The IoT security is uniquely challenging due to its interplay between physical and digital components. In addition, the IoT business model environment (and its governing regularity and contractual obligations and liability requirements) represents one of the crucial area.

978-1-7281-2680-7/20/$31.00 ©2020 IEEE

Recently, IoT has shown that it's representing a real new security threats through different security breaches and attacks took place in the real world, proving that IoT endpoint security is a challenging issue, which may lead to loss of life [15]. Another IoT attack scenario was "Dyn cyberattack, 2016", which use the IoT endpoints as weapons on a massive DDOS attack [16]. The two pervious mentioned real attacks scenarios took place only on one part of the IoT complex architecture; it is the IoT endpoint building block. Farther, the IoT communications and IoT gateways are security-challenging issues. Also, and due to the unique characteristics of resource constraints, self-organization, and short-range communication in IoT, it always resort to the cloud for outsourced storage and computation [17]. Hence, IoT cloud infrastructure security is another issue, add to that, the security and privacy of the users' stored data, Facebook scandal [18] is one real scenario of privacy breach added to the IoT application security.

As a result for these ongoing research problems in IoT, there is a real lack of well-established Formal Specifications and verification techniques for future proposed security models. In technical jargon, formal specifications are mathematical-based techniques whose purpose is to help in software and system implementation. More concretely, they are used to describe the system under subject, analyze its behavior and to consolidate its design by verifying key properties of interest. The task is often achieved through utilizing some rigorous and effective reasoning tools. We say some specifications are formal when they have a syntax, their semantics fall within one domain and they can be employed to infer useful information.

The syntax should be restricted. The semantics must be well-defined and must be built on the top of well- structured mathematical concepts, too. A language with such precise semantics must be used in our formalism so as to avoid any ambiguity that may – unintendedly – occur. Such disambiguation may serve as a tool for proofing specification properties.

The rest of the paper is organized as follows: section II gives summarized review for the status of the corresponding IoT security models and frameworks. Section III presents the proposed future directions for IoT Security Models, specifically, it covers the motivation and aim behind such proposal, followed by the proposed unified criteria and characteristics for the future IoT security models, and end with brief road map to attain such goal, which nominates the least possible for both the scope and the required research phases. Finally, section IV gives the conclusion.

II. LITERATURE REVIEW

Several organizations and research centers contributed to such context (i.e. the security of the IoT) by proposing different security solutions to different IoT security challenging issues. Some of these contributions focused on the IoT endpoints part such as embedded networked sensor devices, which proposed by Stanford university research center [19]. The paper focused only on the endpoints tier of IoT multi-tier architecture, and did not cover all other IoT levels/tiers. In [17], another contribution came related to the security and privacy for mobile cloud based IoT, it was only for mobile cloud base IoT and focused mainly on security and privacy issues within cloud base IoT, and it did not consider the future security requirements. While, the Open Web Application Security Project (OWASP) presented its top 10 IoT vulnerabilities check list for IoT devices and application as basic testing guide [20]. Such checklist guide neither comprehensive nor supple. All the way through, organizations started contributing by laying the foundation for IoT security framework, for example, AT&T Cyber Security Insights proposed a CEO guide to secure the IoT [21]. However, such security guide is inadequate for future rather than incompliant with standards. In [22], The State University of New York proposed a framework to classify the IOT security vulnerabilities. The offered framework classify only the IoT security vulnerabilities based on analyzing the security violations and breaches that have occurred in the world of IoT during that period. While [23] proposed a framework focusing on security and privacy in addition to the efficient energy management in the energy internet (EI).

Alternatively, the IoT Security Foundation ("IoTSF"), a non-profit organization, released version 1.0 & then 1.1 of the IoT security compliance framework. However, both versions are applicable only for IoT consumer not for all IoT business model [24]. In addition, the Industrial Internet Consortium (IIC) has also published the industrial Internet of Things (IIoT) security framework. The IIoT framework mainly designed to provide trustworthy system for the industrial IoT systems [25], specifically to provide security, resiliency, safety, privacy and reliability for IIoT systems. This framework provided guidance for improving organizational approaches, processes and the use of technologies for creating a trustworthy system. The framework is informational in nature and not a normative technical specification. It does not contain specifications for conformance or compliance too.

III. IOT SECURITY: FUTURE DIRECTIONS FOR PROTECTION MODELS

A. Motivation and Aim

Currently, Internet of Things has gained considerable significance and concern, likewise, and by the end of 2020, the estimation of the amount of the connected devices to the Internet to reach in excess of 50 billion [6]. Consequently, and in particular with widespread usage and adoption of the IoT applications and projects in various industries, the consideration of the IoT Security has increased dramatically too. On the other hand, the multi-tiers of IoT architecture along with the diverse of the associated applications open new security challenges, likewise, expanding the existing security directions excessively. Therefore, the IoT Security research field extensively and relatively considers new, fertile, enthusiastic, and challenging. Moreover, and consistent with our critical review and investigation, the number of the provided solutions are confined and limited. Thus, currently, there is high need and demand for a security model with such proven quality (formal) in achieving its Specific required functionality (IoT security) leveraging a well-known formal specification and verification techniques as well as cover nearly all IoT security aspects (comprehensive) in addition to its capability to be implemented effectively (practical), and clasp the current gaps in IoT security as well as persist over 10-20 years' lifespan (future). At the same time, such expected security models are required to comply with the associated standards as well as to provide straightforward and complete guidance for the intended security implementation, deployment, and practice.

Thus, the future IoT security models must accomplish and satisfy the following main objectives:

- Embrace ALL typical security services across all IoT layers.
- Provide reliable and trustful Security Solution for IoT by adding some preferable characteristics and criteria for such models (i.e. best achievable with desirable features such as Formal, Inclusive, Future, Agile, and Compliant with the standards security model).

B. *Criteria and Characteristics*

The proposed future direction is to construct and develop novel "IoT Security Models" that provide an assortment of adaptable controls for protecting the data consistently across all IoT layers. Thus, some preferable characteristics and criteria namely *Formal, Inclusive, Future, Agile, and Compliant with the standards (FIFAC)* are proposed in order to assure modularity, reliability, and trust for such security models, the "FIFAC" clarification is as follows:

- Formal: a model with a quality that guarantee the achievement of its required functionality (IoT security) using a formal specification and verification techniques. Thus, Formal Specification and Verification are required and vital for the future security models, using formal language such as "Petri Net and Z language" to assure correctness and reliability of the new models.
- Inclusive: the future models should be comprehensive. Inclusive security models that include all *(or nearly all)* IoT Security aspects and levels. The future models must plan to embrace all standard security services across all IoT tiers.
- Future: the forthcoming security models ought to accomplish and clasp the current security gaps as well as persist over 10-20 years lifespan. Additionally, obedient and adaptable with the future Internet architecture.
- Agile: the modern security models should provide simple and complete GUIDANCE associated with a Case Study for such proposed "IoT security Models" in term of implementation, deployment, and practice.
- Compliant with the standards: the incoming security models should confirm and verify (i.e. formal verification) the attributes/qualities of such planned/proposed "Models" are Compliant with the associated IoT Security Standards.

Therefore, the expected upshot and effect of such proposed "FIFAC" Security Models for the Internet of Things applications and solutions, is to provide and assure such intended and anticipated security objectives and features.

C. *Scope and Methodology*

In order to attain best and utmost solutions, the scope of the proposed "FIFAC" models should cover, at least, the following areas and domains, (i.e. *but not limited)*:

- The Internet of Things and its entire multi-tier level architecture (including the associated hardware and devices).
- The IoT Security (covering cryptography and cybersecurity).
- The Information Security Standards and Policies
- The Formal Specification and Modeling

In addition, the preferable and straightforward methodology to follow in order to accomplish the "FIFAC" goals, might include the following proposed phases:

- Risk Analysis Phase: identifies and determines the anticipated IoT Security vulnerabilities and the associated attacks, across all IoT layers.
- Security Requirements Definition and Determination Phase: identifies and determines the security requirements (including services, mechanisms, & controls) of the offered model.
- The Model Development Phase.
- Formal Specification and Verification Phase.
- A Case/Porotype Study Phase

IV. CONCLUSION

The IoT ecosystem poses new security challenges that extend beyond traditional data security because of the unique IoT multi-tier network and the architecture nature. Thus, having unified criteria and characteristics for the future IoT Security models is vital, essential, and significant in order to assure modularity, reliability, and trust for such security models, as well as, to provide an assortment of adaptable controls for protecting the data consistently across all IoT layers. Accordingly, and to contribute to such context, this paper presented brief review for the status of the corresponding IoT security models and frameworks. Furthermore, it proposed unified criteria and characteristics for the future IoT Security models, namely Formal, Inclusive, Future, Agile, and Compliant with the standards (FIFAC).

REFERENCES

[1] S. Jankowski, J. Covello, H. Bellini, and J. Ritchie, "The Internet of Things: Making sense of the next mega-trend." [Online]. Available: http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf The Goldman Sachs Group, Inc. Equity Research September 3, 2014.

[2] Q. Hassan, A. Khan, and S. madani, "Internet of Things: Challenges, Advances, and Applications", CRC Press Taylor & Francis Group 2018.

[3] IETF.org, "The Internet of Things." [Online]. Available: https://www.ietf.org/topics/iot/. April 4, 2018

[4] ITU-T, "Internet of Things Global Standards Initiative" Recommendation ITU-T Y.2060 (06/2012)) [Online]. Available: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx, 2018

[5] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)." IEEE Internet Initiative iot.ieee.org IEEE Issue-1 - Published 13 MAY 2015. [Online]. Available: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf.

[6] V. Nagamalla, and A. Varanasi, “A review of security frameworks for Internet of Things” Procceding of 2017 International Conference on Information Communication and Embedded Systems (ICICES)p 1-7. IEEE Xplore Digital Library, DOI: 10.1109/ICICES.2017.8070758, 2014. IEEE Xplore: 19 October 2017

[7] B. Tripathy, and J. Anuradha, “Internet of Things (IoT) Technologies, Applications, Challenges and Solutions.” CRC Press Taylor & Francis Group 2018

[8] S. Islam1, D. Kwak, M. Kabir, M. Hossain, and K. Kwak, “The Internet of Things for Health Care: A Comprehensive Survey”, IEEE Access Vol. 3 pp.678-708, June 1, 2015.

[9] B. Russell, and D. Duren, “Practical Internet of Things Security.” Published by Packt Publishing Ltd, June 2016.

[10] Z. Bi, L. Xu, and C. Wang, “Internet of Things for Enterprise Systems of Modern Manufacturing.” IEEE Transactions on Industrial Informatics, Vol. 10, NO. 2, pp. 1537- 1546, MAY 2014.

[11] R. Shahzadi, M Tausif, J. Ferzund, and M. Suryani “Internet of Things based Expert System for Smart Agriculture”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 9, pp. 341-350, 2016.

[12] K.N. Bhoomika, C. Deepa, R.K. Rashmi, and R. Srinivasa “Internet of Things for Environmental Monitoring.” International Journal of Advanced Networking & Applications (IJANA), ISSN: 0975-0282, pp.497-501, 2016.

[13] I. Khajenasiri, A. Estebsari, M. Verhelst, and G. Gielen, Georges, “A Review on Internet of Things Solutions for Intelligent Energy Control in Buildings for Smart City Applications”, Energy Procedia 00 (2016) 000–000 Published by Elsevier Ltd, vol. 111, pp. 770-779, 2017.

[14] US Department of Energy, “The Internet of Things (IOT) and Energy Management in the Modern Building”, Presented in Better Buildings Summit, Tuesday May 10, 2016.

[15] C. Miller, and C. Valasek, “The Jeep hackers are back to prove car hacking can get much worse”, Security researchers [Online]. Available: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/ August 1, 2016,.

[16] Kaspersky, “How to Break the Internet”, [Online]. Available: https://www.kaspersky.com/blog/attack-on-dyn-explained/13325/, October 26, 2016,

[17] J. Zhou, Z. Cao, X. Dong, and A. Vasilakos, “Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future”, IEEE Communications Magazine, DOI: 10.1109/MCOM.2017.1600363CM January 2017.

[18] BBC.com, “Facebook scandal 'hit 87 million users” [Online]. Available: http://www.bbc.com/news/technology-43649018 April 2018

[19] K. Kiningham, M. Horowitz, P. Levis, and D. Boneh, “CESEL: Securing a Mote for 20 Years”, ACM Digital Library ISBN: 978-0-9949886-0-7, pp.307-312, February 2016.

[20]OWASP, “Internet of Things Top 10”, [Online]. Available: https://owasp.org/www-pdf-archive/Internet_of_Things_Top_Ten_2014-OWASP.pdf , 2014

[21] AT&T, “The CEO’s guide to secure the Internet of Things”, [Online]. Available:https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf , Exploring IoT Security, AT&T Cybersecurity Insights Volume 2, AT&T Intellectual Property, 2016.

[22]P. Mulgund, M. Gupta1, S. Singh, S. Walia1, and R. Sharman, “Framework to analyze the vulnerabilities in IOT”, Proceedings of 12th Annual Symposium on Information Assurance (ASIA '17), ALBANY, NY, JUNE 7-8, 2017.

[23] A. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Dong, “Cyber Security Framework for Internet of Things-Based Energy Internet”, Elsevier Future Generation Computer Systems, Vol. 93, pp. 849-859, 2019.

[24]IoTSF, “IoT security compliance framework Release 1.1”, IoT Security Foundation, Copyright © 2017, All rights reserved, 2017.

[25]Industrial Internet Consortium (IIC),” the industrial internet of thing security framework (IIOT)”, Copyright © MITRE October 2016.