Indonesian Journal of Electrical Engineering and Computer Science
Vol. 15, No. 1, July 2019, pp. 414~420
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v15.i1.pp414-420

The internet of things in healthcare: anoverview, challenges and model plan for security risks management process

Nur Azaliah Abu Bakar, Wan Makhtariah Wan Ramli, and Noor Hafizah Hassan
Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Malaysia

Article Info

Article history:

Received Dec 12, 2018
Revised Feb 10, 2019
Accepted Mar 2, 2019

Keywords:

Healthcare
Internet of things
Risk model plan
Security challenges

ABSTRACT

The Internet of Things (IoT) has not been around for very long. However, since the notion of IoT introduced, most of IoT studies focused on a strategic level such as planning, architectures, standardization, and latest technologies, however, studies of risk management plan of IoT are still lacking. IoT has been widely used to link existing medical resources and provide reliable, effective and smart healthcare services to elderly and patients with chronic illnesses. However, a systematic process is missing when managing and anticipating the risk of IoT usage in healthcare. For this purpose, this paper extensively explores various IoT technologies used in health care services and its security challenges. As a result, IoT Security Risk Model for Healthcare is introduced to cater a complete process of risk management based on ISO/IEC 27005:2018 standard. It is believed that by having this model, it will emphasize on iterative IoT risk management process as it may increase the depth and detail of the assessment at each iteration.

Corresponding Author:

Nur Azaliah Abu Bakar,
Advanced Informatics Department,
Razak Faculty of Technology and Informatics,
Universiti Teknologi Malaysia,
Kuala Lumpur, Malaysia.
Email: azaliah@utm.my

1. INTRODUCTION

It was in 1999, the term Internet of Things (IoT) firstly introduced in the EPC Global standards [1]. The aim is to expand the Internet from the network computer to a matter (or object) network. The IoT is a concept that reflects a relevant group of anything, anytime, anywhere, any service, and any network. The main underlying components of IoT are Hardware, Middleware and Presentation [2]. The hardware consists of sensors and actuators, while the middleware is referring to data storage and computing tools for data analytics. Finally, the presentation is the visualization and interpretation of the data via an online interface or web-based platform [2, 3]

The IoT is megatrend in next-generation technology, which affects the entire spectrum of businesses due to the ability to interconnected smart objects and any unique devices. Thus, it brings extended benefits to the existing internet infrastructure such as advanced extensions of devices, systems, and services of machine-to-machine (M2M) scenarios [4]. In reality, the IoT provides appropriate solutions for a wide range of applications for example in smart cities, healthcare, security, traffic management, emergency services, logistics, retails, waste management and industrial control.

The usage of IoT in the healthcare industry has increased dramatically. Thus far, most of the IoT's application in healthcare initiatives revolve around enhancement of care such as remote monitoring and telemonitoring of patient's health condition [1]. In addition, there are also IoT initiatives on tracking,

monitoring and maintaining assets such as the inventory of medical equipment, healthcare assets, and the level of non-medical assets (e.g. facilities and building assets) [5]. The IoT-based healthcare services are expected to reduce costs, improve quality of life, and enrich the user experience [6]. IoT can correctly identify the optimal time to add supply to various devices for their smooth and continuous operation. Figure 1 explains the recent health care trends.

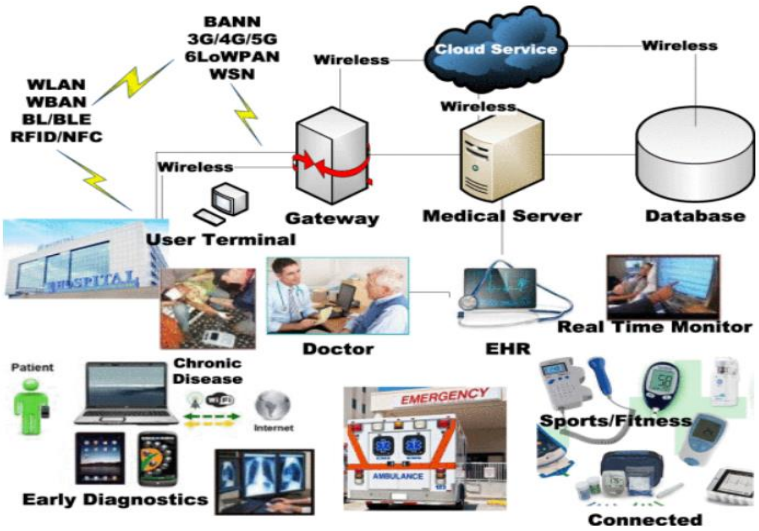

Figure 1. Healthcare trends

The cost-effective interaction facility through seamless and secure connections across patients, clinics, and individual healthcare organizations is the most important aim in any healthcare services. The latest healthcare network driven by wireless technology is expected to support chronic illnesses, early diagnosis, real-time monitoring, and medical emergencies [7-8]. Therefore, IT architects, medical servers and healthcare databases play an important role in creating health records to deliver on-demand health services to authorized stakeholders.

However, these innovations can also put a big risk on healthcare security efforts. In this hyper-connected, technology-driven world, data breaches and cyber-attacks remain a significant threat to organizations, and a lack of awareness of the risks is often to blame. As stated by several studies [9-11], there are so benefits that come with these new connected devices but they also present new unexpected risks and vulnerabilities. For example, the average cost of a healthcare organization data breach has exceeding USD 3.6 million, which is almost USD 380 per individual data record [12]. Therefore, looking at this loss, this paper aims to investigate what are the challenges and risk of IoT in the healthcare industry, followed by proposing a security risk model plan for healthcare IoT ecosystem.

2. ISSUES AND CHALLENGES IN HEALTHCARE IOT AND ENTERPRISE RISK MANAGEMENT

In recent years, there has been an increasing amount of studies on IoT as well as on ICT Security Risk. This section will explain those areas in details by focusing on the issues and challenges in health IoT implementation and security risk management in an enterprise.

2.1. Challenges in Healthcare IoT Implementation

The most ccommon problem in bringing IoT to the enterprise is about their security issues. As a healthcare organization rushing to adopt and implement this next-generation technology, the priority for security has turned toward convenience and ease of use to eliminate the company's downtime. Unfortunately, this means that security is usually much lower on the priority list than it should be. With more innovations, difficult challenges arise. Following are the several challenges identified when implementing IoT in the healthcare enterprise.

Privacy in Healthcare Application: Healthcare application contains lots of sensitive information, including personal details, medical condition, prescriptions, and medical history. If the hacker has ever held

this information, they will be able to make a fake ID to purchase medicines or medical equipment for resale. In certain cases, the attacker may have direct control over IoT equipment, which results in potentially fatal results. For example, Johnson & Johnson warned patients about unsuspected insulin pumps that allow hackers to inject insulin injections without permission [13].

Asset Security Management: In most cases, security leaders use the same strategy that preceded the proliferation of IoT devices but implemented them in new ways. It is always being a matter of knowing where the device is located, and what they are doing on the network and its implementation within a facility [14-15]. Most IoT devices do not include controls to protect their connected network from threats should an emergency scenario occur [16]. Hence, this becomes a challenge to the health care provider in managing and ensuring the security of their asset including the IoT asset.

Data and analytics complexity: The usual practice seen in this industry is that they send their sensor data directly to the cloud or datacenter [17-18]. This is not always the best option as it can make latency, drive costs, and unlock security risks. Those risks also include harm to the patient's safety and health. The huge amount of data collected via IoT devices also require more processing time as it requires a massive Extract-Transform-Load (ETL) process.

BYOD Trend: Bring Your Own Device (BYOD) is a nowadays trend. Despite the benefit imposed such as flexibility and own personalization of application usage, however, it became one of the threat in IoT environment [19-20]. For example, the control mechanism of all the devices entering hospitals become more complicated because it can consist of an extensive range of channels and devices. It becoming harder to recognize and monitor the device operation. Beyond that, BYOD may introduce additional risks by putting these standalone devices into the hospital's network without the authorization.

Lack of awareness about IoT Security: Lastly is the lack of awareness on IoT security among the healthcare stakeholders. Providing an understanding of IoT security from a user's perspective is not an easy task. Since the use of IoTs is growing and changing, there needs to be a widespread awareness of them within the healthcare ecosystem [20-21]. Only through persistent push and promotion by healthcare authorities, medical and IT providers can assure the secured practice is embedded in IoT implementation.

2.2. Security Risk Management in an Enterprise

As of today, there is still no comprehensive security risk management for IoT [22-23]. They still need action call for IoT risk management like IoT devices to require new approaches to security, need further look to the network for better security (e.g. gateways, transport networks, DC / Clouds) and a network virtualization, which brings opportunities for better security, not just an operational savings [9]. To develop an IoT Security Risk Management Model there are three aspects to consider which are 1) IoT Security Technology, 2) IoT Safety and System Security Assurance and 3) IoT Network Infrastructure Safety.

IoT Security Technology

a. Creating conditions, developing architecture, basic IoT's basic security structure design, developing information gathering, transmission, processing and technology applications specific to the IoT capabilities introduced
b. Performs privacy protection, device/node validation, access control, cryptographic key management, infrastructure update security, intrusion detection and fault tolerance steps

IoT Safety and System Security Assurance

a. Develop a risk management plan built around NIST and ISO frameworks and government regulatory compliance requirements specific to IoT. This plan should include the establishment of a third-party compliance verification security system established.
b. Implementing SDLC and interoperability programs to cover the overall life cycle planning, design, operation and maintenance of the IoT
c. Establish service level agreements for IoT outsourcing projects or application development to ensure IoT application security, risk management and system reliability assurance

IoT Network Infrastructure Safety

a. Design secure integration architecture design for secure integration of IoT devices and applications into existing network architecture. This will ensure the full integration of existing resources with new technology application space, recognizing the smooth and compatible conversion of old and new technologies, and ensuring the safety and security of the IoT infrastructure.

3. RESEARCH METHOD

IoT in the healthcare ecosystem has become a demanding technology and require an intensive attention to its security aspect. To analyze this situation, this study has selected Hospital Kuala Lumpur (HKL), Malaysia as a case study. It is the largest government hospital located in Kuala Lumpur, which comprises of 53 different departments; including the pharmaceutical department, training and research, clinical departments and clinical support services. Estimated, there are 2300 in-patients in one time in HKL. To date, HKL has partially implemented IoT infrastructures to cater customers need. However, it is still at the infancy stage. This is due to the lack of technical capability in supporting the IoT operation, as well as HKL, still, do not possess any strong risk management system. Their current practice on risk management totally relays on staffs' daily monitoring activities while the IT Department monitors IT-related threats. This brings strong justification why it is best to adopt HKL as a case study as their Healthcare IoT initiative is still at infancy level, thus it provides more flexibility in developing their IoT Security Risk Management Model.

4. RESULTS AND ANALYSIS

Looking at the HKL unique case study, which is a massive healthcare with a sophisticated ecosystem, it is predicted that HKL has many types of IoT devices and technology, various type of data and process as well as multiple stakeholders need and request. Thus, to cater to these varieties of requirements this study proposes that HKL should adopt the newly revised ISO/IEC 27005:2018, Information technology – Security techniques – Information security risk management [24].

This standard will provide guidance for organizations on how to wade through it all by providing a framework for effectively managing the risks, which in this case is IoT technology. This standard will assist on establishing the risk management context (e.g. the scope, compliance obligations, approaches/methods to be used and relevant policies and criteria such as the organization's risk tolerance or appetite). This standard also can quantitatively or qualitatively assess (i.e. identify, analyze and evaluate) relevant information risks by taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a 'level of risk.

Once the threat is identified, the guideline provided in this standard shall suggest either to modify [use information security controls], retain [accept], avoid and/or share [with third parties]) the risks appropriately by using those 'levels of risk' to prioritize them. Finally, this standard also emphasizes keeping stakeholders informed throughout the process; as well as monitor and review risks, risk treatments, obligations and criteria on an ongoing basis and responding appropriately to significant changes.

Given the ISO/IEC 27005:2018 in place, this means different data source interoperability needs to be addressed and all connected devices need to communicate with each other. When the patient's data goes in, the health system should have the infrastructure, resources and processes to take the expected picture of the party that the guard can use. Finally, when cyber-attacks are increasingly threatening, their health systems and partners must ensure their network protection by investing in viable features and capabilities. Since IoT devices capture and transmit data in real-time, the infrastructure for receiving and processing and storing this data from millions of devices should be planned and built to scale. Figure 2 shows the proposed model about the security risk management to address the IoT security challenges or risks in the healthcare enterprise based on ISO/IEC 27005:2018.

This IoT Security Risk Model for Healthcare cater a complete process of risk management as stated in ISO/IEC 27005:2018. ISO/IEC 27005:2018. It is designed to be an iterative process as it may increase the depth and detail of the assessment at each iteration. Firstly, is to establish the context, which is IoT in healthcare (HKL). Then a risk assessment is conducted. If this provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level, then the task is complete and the risk treatment follows. However, if the information is insufficient, another iteration of the risk assessment with revised context such as risk evaluation criteria and risk acceptance criteria is conducted perhaps in partly scope. In overall, the effectiveness of the risk treatment largely depends on the results of the risk assessment.

Firstly, is the context establishment whereby in this case is the IoT risk in healthcare. Followed by the risk assessment which consists of risk identification, risk analysis and risk evaluation. Then it reaches at a decision point in determination either it is risk or not. If it is not a risk it will return back to original context establishment with no risk associated with it. However, if it is a risk then the next step is to conduct the risk treatment. Then it will reach another decision point to determine either the risk is successfully treated or not. If it is not, then the process will be iteratively done until it reached the acceptance level. Subsequently, if the risk is successfully treated then the risk is considered acceptable and will be put into a proper communication and monitoring review.

The detailed part of the risk assessment is presented in the extended diagram of Figure 2, which highlighted five IoT layers of risk technology assessments starting from the inner layer 1) authentication, 2) encryption, 3) secured boot, 4) intrusion prevention system and firewall, and 5) education and policies. Following are details description of each layer.

Authentication: To ensure the safety of the patient, the hospital must ensure confirmation. A two-factor authentication system (2FA) needs to be installed to access patient records, when users provide additional information to log in (e.g. retinal scans, phone text codes, DNA samples, fingerprints, etc.), not just logins and passwords. IoT devices use a wide variety of protocols and standards, therefore, familiarity with these variations is a must and intimate knowledge of the IoT devices purchased is necessary to ensure that each device is capable of authentication in a secure manner. Some may need a manual update (lacking OTA functionality) and others may have locked settings that cannot be changed from the default. Therefore, it is possible to limit access to gadgets and systems and maintain tight controls over device-to-device to communication devices.

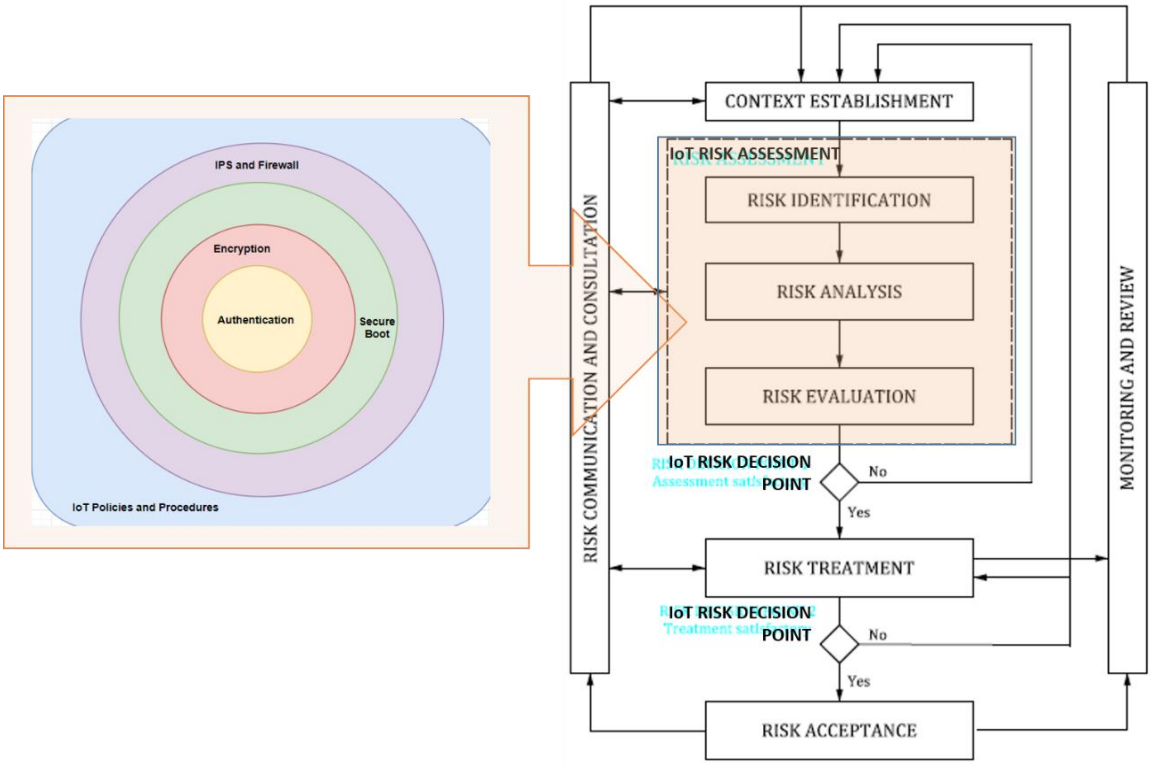

Figure 2. IoT in Healthcare Security Risks Management Propose Model

Encryption:Another basic safety sanitation practice is encryption. It's very easy to get access to health records through mobile devices, but this procedure also requires security risks. To minimize the risk of data breach and avoid negative results it is important to encrypt data (both during transit and stored). As far as storage encryption is concerned, healthcare institutions should ask their sellers to use hardware level encryption. Unlike software-based encryption solutions for mobile devices that reduce performance by exploiting these resources like CPU cycles and memory, hardware-level encryption, as a rule, has no remarkable effect on performance. Thus, encryption should be at the core of every IoT device in order to reach a state in which data is fully encrypted in storage and transit alike.

Secure boot:A secure boot process prevents the execution of unauthorized code at the time of device power-up and prevents the exposure of embedded boot code and software IP. A secure boot process can be accomplished in many different ways, including using digitally signed binaries, secure and trusted boot loaders, boot file encryption, and security microprocessors. This practice also aims to prevent additional problems and to ensure the safety of IoT devices. With secure boot, it is assured that no configuration has changed when the device is switched on and no one tries to interrupt the device.

Intrusion prevention system and firewall: Since that most IoT attacks are delivered over the internet, intrusion prevention systems and firewall are crucial to identify and prevent anomalies from trying to gain access to your network. This means that hackers who try to access or close your IoT equipment will stop before they damage the system.

Education and Policies: With the emergence and use of new technologies, it is important to ensure all hospital IoT users are aware of new challenges, risks and know how to overcome them. In addition, patients represent an indispensable part of the healthcare enterprise (they are active users of IoT devices), so, raising awareness through clear and detailed instructions should not be ignored. In addition, it is vital to have a documented policy from the Ministry of Health to serve as a guiding framework in supporting and enforcing the secured IoT used.

5. CONCLUSIONS

This paper had covered about the description of the IoT, focusing in the healthcare enterprise, the risks of IoT concerns, followed by the proposed model for security risks management process in a healthcare environment. From the previous studies conducted, it is highly suggested that the future of IoT in healthcare are promising with strong potential to grow. Although progress may be slow due to various obstacles, however with good planning and model in place, this issue can be resolved. The IoT has certainly brought many advantages to the healthcare industry and eventually bring benefits to a human being as well.

Given HKL as the case study, this study proposes a new improved model to enhance its IoT Security Risk Management model to suit the complexity of its business. Since this is still at the preliminary and design phases, it is expected that this model shall evolve once it receives the feedback from the IT and business personnel in HKL. In the future, this IoT Security Risk Management Model can be implemented to other hospitals in Malaysia as a way achieving the expected standard of IoT security risk defined.

ACKNOWLEDGEMENT

The research is financially supported by Universiti Teknologi Malaysia (UTM) PAS Grant Q.K130000.2738.03K32.

REFERENCES

[1] P. Kaviya, "Intelligent Healthcare Monitoring in IoT," *International Journal of Advanced Engineering, Management and Science*, vol. 4, 2018.
[2] K. Domdouzis, B. Kumar, and C. Anumba, "Radio-Frequency Identification (RFID) applications: A brief introduction," *Advanced Engineering Informatics*, vol. 21, pp. 350-355, 2007.
[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (Iot): A Vision, Architectural Elements, and Future Directions," *Future generation computer systems*, vol. 29, pp. 1645-1660, 2013.
[4] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678-708, 2015.
[5] P. A. Laplante and N. Laplante, "The Internet of Things in Healthcare: Potential Applications and Challenges," *IT Professional*, pp. 2-4, 2016.
[6] S.-y. Ge, S.-M. Chun, H.-S. Kim, and J.-T. Park, "Design and Implementation of Interoperable IoT Healthcare System Based on International Standards," in *Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual*, 2016, pp. 119-124.
[7] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, et al., "Health Monitoring and Management using Internet-of-Things (Iot) Sensing with Cloud-Based Processing: Opportunities and Challenges," in *2015 IEEE international conference on services computing (SCC)*, 2015, pp. 285-292.
[8] [M. Maksimović, V. Vujović, and B. Perišić, "A Custom Internet of Things Healthcare System," in *Information Systems and Technologies (CISTI), 2015 10th Iberian Conference* on, 2015, pp. 1-6.
[9] Montbel, H. Chi, W. Zhou, and S. Piramuthu, "Internet of Things (Iot) in High-Risk Environment, Health and Safety (EHS) Industries: A Comprehensive Review," 2017.
[10] J. A. Lewis, "Managing Risk for the Internet of Things: Center for Strategic & International Studies", 2016.
[11] L. Botti, V. Duraccio, M. G. Gnoni, and C. Mora, "A Framework for Preventing and Managing Risks in Confined Spaces Through IoT Technologies," in *Safety and Reliability of Complex Engineered Systems-Proceedings of the 25th European Safety and Reliability Conference, ESREL*, 2015, pp. 3209-3217.
[12] T. Wu and G. Zhao, "A Novel Risk Assessment Model for Privacy Security in Internet of Things," Wuhan University Journal of Natural Sciences, vol. 19, pp. 398-404, 2014.
[13] J. Finkle, "J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking," Reuters. Published October, vol. 4, 2016.

[14] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (Iot) Security: Current Status, Challenges and Prospective Measures," in *Internet Technology and Secured Transactions (ICITST)*, 2015 10th International Conference for, 2015, pp. 336-341.
[15] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," in *Service-Oriented Computing and Applications (SOCA)*, 2014 IEEE 7th International Conference on, 2014, pp. 230-234.
[16] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security Analysis on Consumer and Industrial IoT Devices," in *Design Automation Conference (ASP-DAC)*, 2016 21st Asia and South Pacific, 2016, pp. 519-524.
[17] H. Abie and I. Balasingham, "Risk-Based Adaptive Security for Smart IoT in Ehealth," in *Proceedings of the 7th International Conference on Body Area Networks*, 2012, pp. 269-275.
[18] W. AL-mawee, "Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users A Survey," 2012.
[19] S. Tyagi, A. Agarwal, and P. Maheshwari, "A Conceptual Framework for IoT-Based Healthcare System using Cloud Computing," in *Cloud System and Big Data Engineering (Confluence)*, 2016 6th International Conference, 2016, pp. 503-507.
[20] J. Pacheco and S. Hariri, "IoT Security Framework for Smart Cyber Infrastructures," in *Foundations and Applications of Self* Systems, IEEE International Workshops* on, 2016, pp. 242-247.
[21] D. A. KhAN, "A Framework For Integration of A Patients' Body Area Network With IoT," 2017.
[22] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure Integration of IoT and Cloud Computing," *Future Generation Computer Systems*, vol. 78, pp. 964-975, 2018.
[23] N. Azmi and L. M. Kamarudin, "Enabling IoT: Integration of Wireless Sensor Network for Healthcare Application using Waspmote," in *AIP Conference Proceedings*, 2017, p. 020010.
[24] B. S. "Institution, Information Technology. Security Techniques". *Information Security Management Systems: Requirements*. BS ISO/IEC 27001: 2013: BSI, 2018.

BIOGRAPHIES OF AUTHORS

Nur Azaliah Abu Bakar is Senior Lecturer at Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia (UTM AIS). She graduated with a Bachelor (Information Technology) in Information Systems Engineering from Multimedia University (MMU) Malaysia (2000). She then obtained her Masters in Information Technology from Universiti Teknologi Mara (UiTM) in 2004. In 2017 she was awarded a Doctor of Philosophy degree in Information Technology (Enterprise Architecture) by Universiti Teknologi Malaysia (UTM). She has 20 years' experience in ICT and has served in the Malaysian Public Sector as well as several multinational companies. Her the topics of expertise and research interests include, but are not limited to Informatics, Enterprise Architecture, Data Analytics, Business Intelligence and ICT Strategic Planning. She can be contacted via email address azaliah@utm.my

Wan Makhtariah Wan Ramli is candidate for Master of Science (Information Assurance) at Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia (UTM). She graduated with a Bachelor of Computer Science in Computer Networking from Universiti Teknikal Malaysia Melaka (2008). She has 11 years' experience in Cyber Security and has served in Public Sector as well as several ICT companies and currently working as Head of Security in a Cyber Security Firm. She can be contacted via email address wanmakhtariah@gmail.com

Noor Hafizah Hassan is a Senior Lecturer at Advanced Informatics Department from Razak Faculty of Technology and Informatics. She graduated with Bachelor in Computer Science (Software Engineering) in 2007 and obtained Master in Software Engineering in 2011 from University Malaya. She was awarded with Doctor of Philosophy (PhD) from Universiti Teknologi Malaysia (UTM) in 2016. She has 7 years' experience in teaching and research from private and public institution. Her research interests are on healthcare informatics, information security and software engineering, internet of things. Currently, her projects are on internet of things, blockchain technology and big data analytics. She can be contacted via email noorhafizah.kl@utm.my