A Study on Privacy Issues in Internet of Things (IoT)

Naqliyah Zainuddin
Info. Security Mgmt
CyberSecurity Malaysia
Cyberjaya, Malaysia
naqliyah@cybersecurity.my

Maslina Daud
Cyber Security Proactive
CyberSecurity Malaysia
Cyberjaya, Malaysia
maslina@cybersecurity.my

Sabariah Ahmad
Info. Security Mgmt
CyberSecurity Malaysia
Cyberjaya, Malaysia
sabariah@cybersecurity.my

Mayasarah Maslizan
Info. Security Mgmt
CyberSecurity Malaysia
Cyberjaya, Malaysia
mayasarah@cybersecurity.my

Syafiqa Anneisa Leng Abdullah
Info. Security Mgmt
CyberSecurity Malaysia
Cyberjaya, Malaysia
anneisa@cybersecurity.my

2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP) | 978-1-7281-8621-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/CSP51677.2021.9357592

***Abstract*—Internet of Things (IoT) is an interconnected wireless network where smart nodes (IoT devices) interact with each other in order to exchange data through the communicating medium. IoT have rapidly increased in popularity, demand, and commercial availability within the past several years. Various IoT applications generate a huge amount of data from different types of resources, including smart cities, manufacturing industries, health institutions, and governments. Due to the pervasive nature of IoT and the limitless opportunities that this technology provides, security and privacy becomes two key concerns for the users of these smart offerings. Most of the privacy threats disclosing the private information to unwanted party and gives rise to serious implications in various IoT application. Thus, this paper will analyze existing literature related to various privacy threats in IoT, privacy issues in different applications of IoT and present summary of the study.**

Keywords—Internet of Things, IoT, privacy threat, privacy issues, privacy challenges, smart homes, smart medical, smart city

I. Introduction

This IoT consists of various devices that generate, process, and exchange vast amounts of critical data as well as privacy-sensitive information. The natural characteristic of IoT environment is the prevalence of devices, sensors, readers, and applications which have the potential to collect a multiplicity of data types of individuals as they move through such environments [1]. These devices offer various advantages, including reduced energy consumption, more effective health management, and better living spaces that react adaptively to fit users' lifestyles.

IoT involvement in our daily lives is witnessing drastic growth and development which can be noticed in IoT applications such as smart cities, smart cars, smart homes, and various automation. Each 'thing' in the term 'Internet of Things' refers to a device, and there are many types of connectable devices, from cameras, scales, sensors, and home management systems, all the way to heart monitoring implants to cars or sensors monitoring livestock [2].

In order for users to enjoy the provided services thru various applications of IoT, they have to access these services, provide and exchange a lot of personal information in an open, unsafe and interconnected environment. Due to the pervasive nature of IoT enabled smart services and the limitless opportunities that this technology provides, apart from security, privacy becomes another key concern for the users of these smart offerings [3].

[4] defined users' privacy as the right of what, how, to what extent and with whom their information will be shared with others. In order to come out with a privacy safeguard framework, [5] has classified privacy concerns based on data activities to unauthorized collection, unauthorized use, unauthorized sharing, unauthorized access, insecure transmission and insecure storage. The collection of massive amounts of available data and powerful analytic tools that transfer meaningless data to information lead to raise an individual's concern about the privacy [6]. [7] highlighted that the perspective of the usefulness of the IoT is dependent on how well it can respect the privacy choices of people. Privacy is an important issue in IoT application on account of the ubiquitous character of the IoT environment.

Thus, this paper will analyze existing literature related to various privacy threats in IoT (section II), privacy issues in different applications of IoT and summary of the study (Section III).

II. Common Privacy Threats in IoT ecosystem

In a typical IoT ecosystem, all smart devices and people are interconnected at any time and any place. However, most of these devices connected to the internet are not equipped with efficient security mechanisms and are vulnerable to various privacy and security threats [8].

[9] emphasized that privacy in the IoT is the threefold guarantee to the data subject for (i) awareness of privacy risks imposed by smart things and services surrounding the data subject, (ii) individual control over the collection and processing

978-1-7281-8621-4/21/$31.00 ©2021 IEEE

of personal information by the surrounding smart things, (iii) awareness and control of subsequent use and dissemination of personal information by those entities to any entity outside the subject's personal control sphere.

Next sub-sections briefly discuss the privacy threats such as eavesdropping, data leakage, impersonation, data tampering [10], [3], [11], [12] and jurisdiction risks [13].

A. Data Leakage

In IoT ecosystem, objects such as smart devices are tightly coupled with human beings, since they are involved in too many systems around us such as cars, homes, and hospitals to provide infinite services and solutions.

[14] defined eavesdropping as an attack that threatened the privacy when an intruder intercepting, reading, and modifying messages for further investigation. In eavesdropping, intruder may only listen to the information while it is being transmitted between the two nodes over the network. In this attack, information remains the same but its privacy compromises [15]. Threats posed by eavesdropping may significantly increase when packets convey access control information (e.g., object identifier, object configuration, and shared key) [14].

In IoT, devices are connected with each other in order to communicate and exchange data. The amount of data generated by these connected devices has witnessed a massive growth and may include sensitive and private information. Hence, IoT devices may leak private user data, both from the cloud (where data is stored) and between the devices themselves.

In this regard, protecting privacy of these data is a key issue because unauthorized devices handling can lead to leakage threatening of information [16]. [17] highlighted that data leakage may take place during data storage, data transmission and data sharing, which may lead to serious issues beyond financial loss for the providers of a particular IoT services.

B. Impersonation

According to [12], an impersonation attack is an attack in which an adversary is disguised as a legitimate party in a system or communications protocol. An adversary could try to impersonate and act on behalf of a legitimate user [18] by gaining access to users' credentials or to any other information that provide access to the IoT resources.

Impersonation threatened the privacy of the data when the attacker tries to fake the identity of a trusted individual to gain access to some sensitive data [19].

C. Data Tampering

Integrity of the data collected from smart devices must be protected to prevent it from being tampered by unauthorized parties. Data tampering and manipulation is an insidious threat that not only affects data privacy but, if left undetected, could have imputable consequences to brand reputation, national security or public health [20].

For example in smart meter application, a user might want to pay less than the amount of power user used, so user is likely to tamper the data [21].

D. Jurisdiction Risk

In IoT, cloud application often involves outsourcing to multiple parties (and sub-parties) who operate in multiple jurisdictions, frequently without full transparency to the user of the cloud service [22]. Besides, cloud computing also often implies data transfer to, and backup in, many places [13].

Some personal data elements are considered more sensitive than others, although the definition of what is considered sensitive personal information may vary depending upon jurisdictions and even on particular regulations [23]. Even if the same information is involved, there may be different data protection requirements in different contexts due to factors including location and trust in the entities collecting and processing it [23]. [24] emphasized that, the concerns of cloud customers over sensitive data is often overlooked and underestimated as cloud providers continue to transfer data to other jurisdictions.

Thus, this situation may threatened the privacy of the data due to improper use or disclosure of personal information that is stored and accessible in multiple locations, by multiple parties and across multiple jurisdictions.

III. Privacy Issues in Smart Things

As discussed in previous section, smart things containing numerous internet connected devices raises substantial privacy issues. The following sub-sections will discuss on privacy issues in various IoT applications.

A. Smart Home

Smart home devices are hardware units typically comprising sensors, actuators, gateways, and smart objects. The connected home may contain sensitive data (e.g. personal photos, videos, and digital diaries), and devices such as IP cameras that may be remotely activated and accessible from anywhere.

In a smart home [15], windows, home ventilations, doors, lightings, air conditioning, refrigerators, washing machine, oven etc. can be manipulated by remote platforms or programs. Residents also can interact with IoT devices and manage their smart home through different platforms such as PCs, smart phones, and tablets.

[25] highlighted that smart homes expose the residents to privacy risks as personal information becomes remotely accessible in new ways. [26] added that a passive network observer can infer sensitive information about consumers from the network behaviour of their smart home devices, even when those devices use encryption. Besides, [27] emphasized that an attacker can illegally obtain unencrypted information generated by a smart home using wireless data intercept tools.

B. Smart Meter

A smart grid is a system built on advanced ICT based infrastructures that manages electricity in a sustainable, reliable, and economic manner [28]. Smart meter is one of the key devices that enable the smart grid concept by monitoring a household's electricity consumption and reporting it to the utility provider i.e., the entity that sells energy to customers, or to the distribution system operator, i.e., the entity that operates and manages the grid, with high accuracy and at a much faster pace compared to traditional meters [29].

However, according to [30] the smart meter's ability to monitor a user's electricity consumption in almost real-time entails serious implications about consumer privacy. This is supported by [29] where power consumption profiles may reveal sensitive information on the state of their businesses to their competitors. Not only to businesses, living pattern of individuals will also be observed by perpetrators that can pose serious threats when they should or should not be at home at a certain time. Such important privacy concerns in the use of smart meters has raised significant public attention and they have been highly debated in the media and by politicians, and, if not properly addressed, they could represent a major roadblock for this multi-billion dollar industry [30].

C. Smart Medical

Health and wellness is one of the most promising application areas of IoT technology. Recently, there have been an increasing number of attacks where the victims have been hospitals or health institutions. IoT in healthcare provides an environment where a patient's vital parameters get transmitted by medical devices onto secure cloud based platforms where it is stored, aggregated and analyzed [15].

Smart medical devices are attractive targets for cybercriminals as the devices often employ weak security measures, causes security compromise that lead to privacy breaches and safety threats in the real world. Types of attacks on medical devices includes eavesdropping in which privacy of the patient is leaked, integrity error in which the medical information is being altered, and availability issues which include battery draining attacks [8].

In IoT, Radio Frequency Identification (RFID) plays a lead role because it identifies any number of objects simultaneously [1]. RFID setup consists of several RFID tags and one or more RFID readers. [31] discussed that privacy threats brought by RFID in smart medical devices where criminals can identify RFID tags in wearable monitoring devices so as to locate and track patients, or illegally collect and utilize patients' health data for analysis and mining. It is important for entities that have been using RFID to protect information related to the RFID tags used. The protection should consider not only while using the tags, but also after using them, as discarded RFID may carry a lot of private information of hospitals or patients, which can be easily collected by others [31].

D. Smart City

A smart city is an interconnected entity of IoT and intelligent systems to provide quality services to its citizens in various sectors such as public safety, healthcare, transportation and energy [5]. Smart city applications benefit people and the city in a variety of aspects such as energy, environment, industry, living, and services.

Despite the benefits a smart city offer to its population, a smart city is vulnerable to privacy leakage and information inferring by outside attackers, due to on how private information is collected, transmitted, and processed. [32] highlighted that the disclosed privacy in a smart city may contain a user's identity and location in transportation, health condition in healthcare, lifestyle inferred from intelligent surveillance, smart energy, home and community, and so on.

[28] also gave an example how a vehicle's license plate can be connected to the vehicle owner's identity where the trajectory of a vehicle can easily be traced even if all communications between the vehicle and infrastructure are encrypted and each device is authenticated by others. [28] added that this is against the common notion of privacy, which includes the right of people to lead their lives in a manner that is reasonably secluded from public scrutiny, whether such scrutiny comes from a neighbour's prying eyes, an investigator's eavesdropping ears, or a news photographer's intrusive camera.

E. Cloud

Cloud-based services are often considered as the essential infrastructure in IoT ecosystem as it offers support for data storage, data processing, and data sharing [33]. As IoT applications allow data to be locally stored on IoT objects or remotely on the cloud depending on their storage capabilities, protecting the data at rest is of paramount importance in preserving its integrity [34].

If the data integrity of a single IoT application at rest has been compromised, then there is a huge risk of dealing with cascading effects on the privacy of the data [35]. For example, [35] stated that a thermostat deployed in a smart home relies heavily on a smoke detector's data to shut a heating system down in case of danger. However, access of the smoke detector's data by unauthorised parties may put the entire smart home at risk.

As a summary, Table 1 shows the mapping of privacy threats in various IoT applications based on discussion in the reviewed papers.

TABLE I. PRIVACY ISSUES IN IOT APPLICATION

Privacy Threat	IoT Applications	Discussion on Privacy Issues
Data Leakage	Smart Grids [29]	Power consumption profiles may reveal sensitive information about the state of their businesses to their competitors.
	Smart Homes [25]	Private data becomes accessible without the householders' awareness.
	Smart Home [26]	A passive network observer can infer sensitive information about consumers from the network behaviors of their smart home devices, even when those devices use encryption.
	Smart Home[36]	• pairing and discovery protocols that leak information about devices in the home; • insecure communication leaking sensitive information about the home and the residents; • vulnerabilities in the devices that can allow an attacker to remotely spy on residents or disrupt their lives.
	Smart Medical [31]	Discarded RFID may carry a lot of private information of hospitals or patients, which can be easily collected by others.
Eavesdropping	Smart Homes [25]	Eavesdrop on the wireless transmission of sensors and detect

Privacy Threat	IoT Applications	Discussion on Privacy Issues
		activities such as showering, toileting, and sleeping.
	Smart Medical [31]	Criminals can identify RFID tags in wearable monitoring devices so as to locate and track patients, or illegally collect and utilize patients' health data for analysis and mining.
	Smart Cities [28]	Users (especially adolescents and the elderly) are not familiar with privacy issues, and they become perfect targets for attackers when they interact with many smart cities' services through their smartphones, tablets, and computers, revealing personal data such as gender, age, and location.
Impersonation	Smart Homes [25]	Malicious actor may remotely take over control of the home devices using them to hack the household or as a platform to launch attacks to other domains, e.g., to overload the energy grid.
	Smart Toys [37]	Third party advertisers can infer a great amount of information about a child based on their location and other context information, collecting detailed behavioral profiles that may be used for unknown or unwanted purposes.
Data Tampering	Smart City Applications [32]	• malicious attackers may generate false data to manipulate sensing results such that services, decisions, and control in a smart city are influenced and not "intelligent" enough; • malicious attackers could also launch denial-of-service attacks, disrupting the sensing, transmission, and control to degrade the quality of intelligent services in a smart city; • information collected and managed by smart home applications may pave the way to disclosing residences' highly privacy-sensitive lifestyle and even cause economic loss; • attackers could still infer and violate privacy in many other ways, such as side channel attack and cold boot attack.
Jurisdiction Risk	Cloud [13]	• increased risk of improper use and disclosure of personal information that is stored and accessible in multiple locations, by multiple parties, across multiple jurisdictions; • risk of disclosure to foreign law enforcement or regulatory authorities created by storage and processing of data outside of the home country of individuals from whom the information was collected; • compliance with an organization's data retention and destruction obligations; and,
		• meeting an organization's transparency obligations with regard to its privacy and data protection practices, when often the full knowledge of how and where data is stored, processed and shared can be obscured in the Cloud environment.

IV. CONCLUSION

IoT has gained significant attention over the last decade. With the increase number of interconnected devices and the growth of IoT, privacy aspect of IoT systems have become a challenge and an important part of IoT systems apart from security.

This study presents literature review conducted on existing works on privacy related issues in the context of IoT application. The findings of this paper have provided an initial finding for us to continue our research and development in privacy initiatives related to smart things in IoT environment.

Besides, we hope that this study will assist researchers, policymakers, and device manufacturers to consider privacy by design approach in offering solutions that contributes to the growing interests in the privacy implications of IoT devices.

REFERENCES

[1] A. S. Kumar, S. Brittoraj, and M. Rajesh, "Implementation of RFID with Internet of Things," no. 1, pp. 193–197, 2019.

[2] T. Anscombe, "IoT AND PRIVACY BY DESIGN IN THE SMART."

[3] P. Podder, "Review on the Security Threats of Internet of Things," vol. 176, no. 41, pp. 37–45, 2020.

[4] C. Kalloniatis and Æ. E. Kavakli, "Addressing privacy requirements in system design : The PriS method Addressing privacy requirements in system design : the PriS method," no. September, 2008.

[5] A. A. Alghanim and A. S. City, "Privacy Analysis of Smart City Healthcare Services," pp. 0–4, 2017.

[6] B. Alsamani and H. Lahza, "A Taxonomy of IoT : Security and Privacy Threats," pp. 72–77, 2018.

[7] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "applied sciences IoT Privacy and Security : Challenges and Solutions," pp. 1–17, 2020.

[8] M. A. Razzaq, M. A. Qureshi, and S. Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study," vol. 8, no. 6, 2017.

[9] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things : threats and challenges REFERENCE MODEL FOR THE," no. June 2013, pp. 2728–2742, 2014.

[10] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "1 Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures," vol. 53, no. 3, 2020.

[11] E. Luo, Z. A. Bhuiyan, G. Wang, A. Rahman, J. Wu, and M. Atiquzzaman, "PrivacyProtector : Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems," no. February, pp. 163–168, 2018.

[12] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, S. Member, and K. Kim, "Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection," vol. 13, no. 3, pp. 621–636, 2020.

[13] P. D. Flaherty and G. Ruscio, "• STORMY WEATHER : JURISDICTION OVER PRIVACY AND DATA PROTECTION IN THE CLOUD — PART 2 •," vol. 13, no. 10, 2013.

[14] H. A. Abdul-ghani, “A Comprehensive Study of Security and Privacy Guidelines , Threats , and Countermeasures : An IoT Perspective,” 2019.

[15] S. E. E. Profile, “Internet of Things (IoT): Security and Privacy Threats,” no. June, 2016.

[16] D. K. Alferidah and N. Z. Jhanjhi, “A Review on Security and Privacy Issues and Challenges in Internet of Things,” vol. 20, no. 4, pp. 263–285, 2020.

[17] Y. Lu, S. Member, and X. Huang, “Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT,” vol. 16, no. 6, pp. 4177–4186, 2020.

[18] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-fovino, G. Steri, and G. Baldini, “Security and Privacy Issues for an IoT based Smart Home,” pp. 1292–1297, 2017.

[19] B. K. Mohanta, U. Satapathy, S. S. Panda, and D. Jena, “A Novel Approach to Solve Security and Privacy Issues for IoT Applications using Blockchain,” pp. 394–399, 2019.

[20] D. Kanngiesser, “These are the seven deadly sins of data tampering.” [Online]. Available: https://www.techradar.com/news/these-are-the-seven-deadly-sins-of-data-tampering. [Accessed: 19-Nov-2020].

[21] C. H. Lee and K. Kim, “Implementation of IoT System using BlockChain with Authentication and Data Protection,” pp. 936–940, 2018.

[22] D. Patrick, “Abstra ct:,” pp. 1–16, 2012.

[23] S. Pearson, “Privacy , Security and Trust in Cloud Computing Privacy , Security and Trust in Cloud Computing,” 2012.

[24] D. Kolevski and K. Michael, “Cloud Computing Data Breaches A socio-technical review of literature,” pp. 1486–1495, 2015.

[25] J. Bugeja, A. Jacobsson, and P. Davidsson, “On Privacy and Security Challenges in Smart Connected Homes,” 2016.

[26] N. Apthorpe, D. Reisman, and N. Feamster, “Closing the Blinds : Four Strategies for Protecting Smart Home Privacy from Network Observers.”

[27] P. Biocco and P. Hines, “A Study of Privacy Policies across Smart Home Companies.”

[28] R. Khatoun and S. Zeadally, “Cybersecurity and Privacy Solutions in Smart Cities,” no. March, pp. 51–59, 2017.

[29] G. Giaconi and G. Deniz, “Smart Meter Data Privacy,” pp. 1–36.

[30] G. Giaconi, G. Deniz, and H. V. Poor, “Privacy-Aware Smart Metering : Progress and Challenges,” no. January 2019, 2018.

[31] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu, “Privacy in the Internet of Things for Smart Healthcare,” no. April, pp. 38–44, 2018.

[32] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, “Security and Privacy in Smart City Applications : Challenges and Solutions,” no. January, pp. 122–129, 2017.

[33] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, “Twenty security considerations for cloud-supported Internet of Things,” no. 1, pp. 1–16.

[34] H. A. Abdulghani, N. A. Nijdam, and A. Collen, “SS symmetry A Study on Security and Privacy Guidelines , Countermeasures , Threats : IoT Data at Rest Perspective,” pp. 1–36, 2019.

[35] A. Mosenia, S. Member, and N. K. Jha, “A Comprehensive Study of Security of Internet-of-Things,” vol. 5, no. 4, 2017.

[36] E. Zeng et al., “End User Security and Privacy Concerns with Smart Homes This paper is included in the Proceedings of the End User Security & Privacy Concerns with Smart Homes,” no. Soups, 2017.

[37] P. C. K. Hung, M. Fantinato, and L. Rafferty, “A STUDY OF PRIVACY REQUIREMENTS FOR SMART TOYS,” 2016.