BRIEFING NOTES

BN-74-Emerging technology and military application-Aug2021

PRIVACY ISSUES IN IOT DEVICES: SYSTEM ARCHITECTURES AND DATA PRIVACY PROTECTION LAWS

Authors: Mehdi Taheri[1] and Kash Khorasani[2]
1 Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada
2 Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

ABSTRACT

In this report, the problem of privacy in developing IoT devices is studied. Data privacy protection laws have been legislated in different countries to protect individual's privacy. Privacy acts in jurisdictions such as Canada, European Union (EU), and Australia are provided and discussed in this work. Given that one can develop IoT devices according to different communication network architectures, namely centralized, decentralized, and distributed, suitable data privacy protection regulations for each architecture is required. Hence, we propose sets of regulations for each of the mentioned IoT architectures are proposed separately.

INTRODUCTION

Based on estimations of Cisco systems, between 2008 and 2009, ratio of things or objects connected to the Internet over people connected to the Internet became more than one, and a new type of systems, called Internet of Things (IoT), was born [1]. IoT is a system of interlinked objects, animals, people, computing devices, digital systems, and mechanical devices that can communicate to each other and are able to form a network of devices [1]. This concept was described as packets of data that are transferred between different nodes, which these nodes can be home appliances or sections of a factory, such that these nodes are integrated as an automated system [2].

There is a wide range of applications for IoT such as smart home, wearable technology, remote health monitoring, emergency notification systems, smart traffic control, vehicular communication systems, industrial IoT, Internet of Military Thing (IoMT), Internet of Battlefield Things (IoBT), and smart grids [1]. Due to the opportunities that the IoT can provide in integrating the physical world into computer-based systems, it provides us with improvement in efficiency, and economic benefits. It was estimated that by 2020, there will be 30 billion devices connected to the internet and the market value of IoT will reach $ 7.1 trillion [3, 4].

The success of the idea of connecting different devices to improve their efficiency massively depends on collecting, storing, and processing data. This has been done by acquisition of data from devices and storing them into a cloud network, which exposes the whole system to security and privacy problems since there is one point of vulnerability for the multiple devices. A major concern in adopting IoT in our life is related to security of these devices. IoT systems usually have low available computation power, so that this constrain makes them unable to implement firewalls or to utilize strong cryptography methods on their communications with other devices.

In general, there are 4 security requirements for IOT systems, 1) data confidentiality, which implies that the unauthorized access to transmitted and stored data should be blocked; 2) data integrity which means companies must detect any corruption of transmitted and stored data; 3) non-repudiation, in which the sender of a message should not be able to deny sending it; 4) data availability, which implies that the authorized parties should have access to the transmitted and stored data even under denial-of-service (DOS) attacks [5].

Privacy threats in IoT, which is considered as a big data infrastructure, are of main concerns since these devices use personal information of individuals that can be used for social control or political manipulations [6]. One of the major challenges in developing IoT devices is to protect users' privacy and ensure that the collected information from users cannot be utilized to identify each user individually. Privacy and protection of data privacy has always been a concern in developing software and websites. For instance, the Platform for Privacy Preferences (P3P) is an effort that helps users to protect their information and choose their preferred information that they are willing to be collected by websites [7]. When users enable P3P on their browsers and visit a website, they will be notified if the website attempts to collect their information such as cookies. However, considering the distributed nature of IoT devices, we require a different approach to tackle the problem of data privacy protection in these systems.

IoT systems can collect, process, and transmit data to other devices over public and private networks. There are various network architectures and methods that these devices utilize to transmit and process data. The mentioned methods can be categorized into two groups, namely centralized in which IoT devices send the collected data to a central server or a cloud platform for processing and storage, decentralized and distributed in which IoT devices use the computation power of nearby or edge servers to process data where the encrypted data will be transmitted to a certain number of servers and each part of the decryption key information is shared with one of the servers for security purposes.

In addition to the impact of network architecture in IoT systems, a key factor in the protection of individuals' privacy is the enacted data protection laws in different jurisdictions. Privacy protection laws for private and public sectors have been legislated in many countries and regions such as Canada, Australia, and European Union (EU) to determine the lawful and unlawful collection, use, and disclosure of users' data. IoT systems with various communication network architectures are required to comply with different regulations and laws to protect users' privacy. Hence, in this report, we aim to propose two sets of regulations that should be followed to protect individuals' privacy who are users of IoT devices with centralized, decentralized, and distributed architectures.

DATA PRIVACY PROTECTION LAWS IN DIFFERENT JURISDICTIONS

In this section, enacted laws regarding data privacy protection in Canada, EU, and Australia are provided. Privacy laws in the mentioned three jurisdictions are comprehensive in the sense that they can be easily utilized by entities and companies in various fields to protect individuals' privacy.

A. Canada

In Canada, a federal law for the private sector named Personal Information Protection and Electronic Documents Act (PIPEDA) has been legislated that considers the consent of users as a fundamental element in collecting, using, and disclosing individuals' information [8]. Also, in the domain of the federal public sector, the Privacy Commissioner of Canada, which has been selected and ordered by Parliament to have the authority and role of guardian of privacy in Canada, has enforced the Privacy Act [9].

Moreover, in 2018, the Privacy Commissioner of Canada released two guidance documents on obtaining meaningful consent and inappropriate data practices to give directions to organizations about their responsibilities and obligations regarding the privacy [10]. The guidance document on meaningful consent sets some guiding principles for organizations such as emphasizing and explaining certain key elements and providing them in a user-friendly manner, giving a clear option to the users to say yes or no, and the entities should be accountable and be able to demonstrate their compliance with law [9]. The second guidance document sets certain "no-go zones" that are considered offside of PIPEDA. The "no-go zones" are as follows [9]:

- Any unlawful collection, use, and disclosure of individuals' personal information.
- Unfair and unethical categorization of individuals that is against human rights law.
- Collecting, using, and disclosing individuals' information that are utilized for purposes which are known and might cause harm to the users.
- "Publishing personal information with the intended purpose of charging individuals for its removal."
- Screening employees by asking and using their social media accounts' passwords.
- Using video and audio functionality of the users' devices with the purpose of surveillance.

B. European Union (EU)

The EU Data Protection Directive (DPP 1995) was enacted in 1995 by EU. The main subjects considered in DPP are as follows [11]:

- Individuals must be informed by service providers about the main purposes for which their information is collected and the third parties with access to the collected information.
- Individuals must be given the option to opt-out if their information will be used for purposes other than those originally collected. Moreover, for sensitive information such as political opinions, medical conditions, and ethnic origin, individuals must be given the opt in option before the disclosure of information to third parties.
- Service providers are responsible for ensuring the security and integrity of individuals' personal information.
- Users must be able to correct their personal information after its submission.
- Governments and organizations are not allowed to use personal information and records for purposes other than the original ones unless they have explicit permission.
- Governmental data protection agencies should be created.
- Personal data and information of EU citizens can only be transferred to those countries outside the EU that have "adequate [data] protection" rules.

Moreover, in 2018 the EU General Data Protection Regulation (GDPR) was enacted and executed in all EU members. The GDPR has been developed by considering various fundamental data protection principles such as "fairness and lawfulness, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality" [12]. One of the key elements considered in GDPR is the emphasis on data protection by design. The latter can be achieved by improving the transparency and informing users about how their information is processed and stored. In addition to transparency, organizations should be accountable and demonstrate their actions for protecting individuals' personal data.

C. Australia

In Australia, the Privacy Act 1988 is considered as the main set of rules to handle personal information by Australian Government agencies and organizations with more than $3 million annual turnover (APP entities) [13]. The foundation of Australian privacy law is based on 13 privacy principles, which determine the minimum standards for collection, use, and disclosure of individuals' personal information. The mentioned principles are discussed below [13].

1. APP entities are required to handle and manage individuals' personal information in an open and transparent manner.

2. Users should have the option to either not identifying themselves or use a pseudonym.

3. APP entities may collect solicited personal information only if it is reasonably necessary.

4. If APP entities receive unsolicited personal information that is not contained in a Commonwealth record and they could not have collected it, the information must be destroyed or de-identified.

5. APP entities are required to take reasonable steps to ensure that individuals are aware of matters such as purposes and circumstances of data collection, entity's privacy policy, and consequences of not collecting personal information.

6. The collected information can only be used or disclosed for the primary purpose for which it was collected. Moreover, for other purposes, APP entities are required to get the consent from users.

7. The collected personal information from individuals must not be used or disclosed for the purpose of direct marketing.

8. APP entities are accountable for users' personal information that they disclose to overseas recipients and they must take reasonable steps to ensure that the recipients follow the Australian Privacy Act.

9. Organizations must not use or disclose identifiers that are used by the government.

10. Reasonable steps must be taken by APP entities to ensure that the collected information is accurate and up to date.

11. APP entities are required to protect the collected personal information from misuse, loss, unauthorized access, and disclosure.

12. If individuals request access to their personal information, APP entities should grant them the access.

13. APP entities must take reasonable steps to correct individuals' personal information they hold.

DATA PRIVACY PROTECTION REGULATIONS SUITABLE FOR EACH IoT ARCHITECTURE

In this section, various privacy protection regulations and considerations for each IoT architecture, namely centralized, decentralized, and distributed are discussed. The proposed privacy protection regulations are developed according to the enacted data privacy protection laws provided in Section I. Hence, our proposed privacy protection regulations are in comply with the data privacy protection laws in Canada, EU, and Australia.

A. Centralized IoT

IoT devices with a centralized architecture utilize a central cloud platform for storage of data and computational purposes. Various sensors installed on the IoT devices are capable of collecting user's information as well as information about user's surrounding environment, such as body temperature, heart rate, speed, and luminous flux. In this architecture, the collected information, will be transferred through communication networks and stored on the cloud computing server. Moreover, the transmitted data will be processed on the cloud platform and a corresponding command will be sent to be executed on the IoT device. Given the data flow in a centralized IoT architecture, one can consider the following as required steps to protect individuals' privacy:

1. Service providers are required to ask for the consent of users before collecting and using their personal information. Moreover, it should be clearly explained to users that why and for what purposes their personal information is collected.

2. Users should be notified about third parties that have access to their personal information, also they must have the option to opt-out anytime they want. Moreover, entities must not use the collected personal information for purposes other than the original ones.

3. Reasonable steps must be taken by service providers to ensure the security of users and their personal information.

4. Users should be able to update and correct their personal information.

5. Individuals should have the option to not reveal their identities, unless it is necessary.

6. It should be explained to users that where their data will be processed and stored. Moreover, the stored personal information must be deleted when it is not needed anymore.

B. Decentralized and Distributed IoT

In the decentralized and distributed IoT architectures the task of data acquisition is handled in a distributed manner such that sensors in the network transmit measurements to local cloud servers or edge computing service providers (e.g., nearby smart devices and routers). Hence, the network traffic will be efficiently reduced in the decentralized and distributed architectures. The transmitted sensor data will be processed and, in some cases, stored in local servers on the edges of the network. Consequently, the generated command in servers will be sent to be executed by actuators in the IoT devices. In addition to privacy concerns which have been raised in centralized architectures, in decentralized and distributed architectures, the users' privacy may be violated by nodes in the network which are utilized to transmit data to edge computing platforms. Hence, in addition to the proposed regulations in previous subsection, service providers should consider the following in their design and systems architecture:

1. Entities must take reasonable steps to secure all the nodes in the system network.

2. Service providers must describe the data flow in the system for users and demonstrate the data flow and storage in the system as well as third parties which have access to users' personal information.

3. Either encryption methods or deidentification methods should be used before transmitting data among the nodes in the network.

HOW TO INFORM USERS ABOUT THE USE OF THEIR PERSONAL INFORMATION IN IoT

According to the privacy protection laws stated in previous section, in addition to obtaining the consent from users, one of the most important issues in privacy preserving is to inform users about the use of their personal information. Furthermore, service providers are considered responsible to inform users in a simple and understandable manner about the use of their data in IoT devices and third parties that have access to that data. The flow and use of data in IoT devices depend on the architecture of the system. For instance, in a centralized architecture, data is processed and stored on the cloud platform that can be disclosed to third parties.

In this report, we suggest that service providers illustrate data flow in the network by utilizing a graph-based information flow diagram. The information flow graph is capable of describing and illustrating where and by whom personal information of users is used. The information flow diagram can prevent data misuse by service providers as well as gaining the individual's trust. Moreover, since in certain IoT devices the personal information of individuals is transmitted to

servers after hiding the identity of users, one can show the anonymizing step in the information flow diagram.

CONCLUSION

In this report, the privacy problems in developing IoT devices were discussed. Data privacy protection laws in different jurisdictions such as Canada, European Union, and Australia were studied to show minimum requirements which service developers should provide in their services. Given that the structure of IoT communication network, namely centralized, decentralized, and distributed, affects the data flow and data processing in the IoT network, regulations suitable for each network structure have been proposed to preserve users' privacy in IoT systems.

REFERENCES

[1] Internet of things. [Online]. Available: https://en.wikipedia.org/wiki/Internetofthings#cite note-9
[2] R. Raji, "Smart networks for control," IEEE Spectrum, vol. 31, no. 6, pp. 49 – 55, 1994.
[3] A. Nordrum et al., "Popular internet of things forecast of 50 billion devices by 2020 is outdated," IEEE spectrum, vol. 18, no. 3, 2016.
[4] C.-L. Hsu and J. C.-C. Lin, "An empirical examination of consumer adoption of internet of things services: Network externalities and concern for information privacy perspectives," Computers in Human Behavior, vol. 62, pp. 516–527, 2016.
[5] S. Supriya and S. Padaki, "Data security and privacy challenges in adopting solutions for iot," in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2016, pp. 410–415.
[6] P. N. Howard, Pax Technica: How the Internet of things may set us free or lock us up. Yale University Press, 2015.
[7] World Wide Web Consortium and others, "The platform for privacy preferences 1.0 (P3P1. 0) specification," World Wide Web Consortium, 2002.
[8] (2000) Personal information protection and electronic documents act. [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html
[9] (2018) Privacy commissioner issues new guidance to help address consent challenges in the digital age. [Online]. Available: https://www.priv.gc.ca/en/opc-news/ news-and-announcements/2018/nr-c 180524/
[10] (2019) Regulation of artificial intelligence: The Americas and the Caribbean. [Online]. Available: https://www.loc.gov/law/help/artificial-intelligence/americas.php
[11] Gerhard Steinke, "Data privacy approaches from US and EU perspectives," Telematics and Informatics, Volume 19, Issue 2, pp. 193-200, 2002.
[12] Goddard M., "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact," International Journal of Market Research, 59(6), pp. 703–705, 2017.
[13] MARGARET JACKSON, "Data Protection Regulation in Australia after 1988," International Journal of Law and Information Technology, Volume 5, Issue 2, SUMMER 1997, Pages 158–191.