Chapter

Privacy of IoT-Enabled Smart Home Systems

Avirup Dasgupta, Asif Qumer Gill and Farookh Hussain

Abstract

Digital ecosystems are going through a period of change due to the advancement in technologies such as Internet of Things (IoT) as well as proliferation of less expensive hardware sensors. Through this chapter, we present current emerging trends in IoT in different industry sectors as well as discuss the key privacy challenges impeding the growth of IoT to reach its potential in the smart home context. The majority of the existing literature on IoT smart home platforms focuses on functionalities provided by smarter connected devices; however, it does not address the concerns from a consumer's viewpoint. Thus, the key questions are: What are the privacy concerns related to IoT, particularly from a "smart home device" consumer viewpoint? What are the existing remedial approaches for privacy management? This chapter proposes a framework to assist smart home user and IoT device manufacturer to make informed privacy management decisions. The findings of this research intend to help practitioners and researchers interested in the privacy of IoT-enabled smart systems.

Keywords: IoT, smart sensors, data governance, privacy, framework

1. Introduction

In last few years, we have observed a growing interest in IoT applications, which are being developed for the industries and ecosystems such as healthcare, smart home, manufacturing and agriculture ecosystems [1]. Presently, it is anticipated that there are about 16 billion IoT units installed worldwide generating vast amount of data. According to forecast reports from Frost and Sullivan, the number of interconnected objects is expected to increase above 60 billion by 2024 [2]. Aggregated data collected from different sensors are being used by organizations increasingly to gain data-driven business insights.

The growth of IoT has been possible due to the advancement of technologies like cheaper hardware sensors, ipv6, wireless coverage, smartphones and processing power of CPU [3]. While the use of IoT worldwide has been high, the maturity level of the solutions using this technology is varied. In this chapter, we highlight the various components making up IoT, evolution of IoT and the concerns related to privacy. We particularly focus on the IoT uses in the smart home context.

IoT ecosystem stands on the building blocks of multiple underlying technologies such as sensing (sensors and actuators), connectivity (mobile), analytics and computing. A typical IoT ecosystem involves the following stages [4].

- Things are fitted with electronics, software, actuators and sensors. They can be battery operated, electricity powered or use RFID transponders. Things collect raw data from the environments. Each thing has a unique identifiable address and of varying computational capability and complexity.

- Data collected from things are processed by applications.

- Using various connectivity technologies such as Wi-Fi, Zigbee, NFC, Bluetooth, cellular (2G/3G/4G/5G) and low-powered WAN, data are transmitted.

- Applications collect data in real time from different things to store, process and analyze in computing platforms.

- Insights are derived from the collated data using robust analytics enabling informed business decisions to be taken involving process and people.

The term "Internet of Things" was officially introduced in 1998–1999 by Kevin Ashton of automatic identification center (Auto-Id) at Massachusetts Institute of technology (MIT). Kevin suggested that Internet-connected RFID technologies can be used in supply chains to keep track of items without human involvement [5]. The philosophy of IoT further gained momentum in 2005, thanks to the formal acceptance of IoT in a world summit on information society (WSIS) in Tunisia [6]. However, the concept of IoT applications can be traced back to 1982 when one of the first attempts of an IoT application was developed at Carnegie Mellon University. The Internet-connected coke machine was able to report the drinks contained and whether the drinks were cold [7] (**Table 1**).

Year	Discovery
1747	Electricity (lightning)
1819	Practical electromagnetism
1831	Faraday: Electromagnetic induction
1873	Maxwell: Theory of electromagnetism
1887	Hertz: Radio waves
1895	Marconi: Radio telegraph
1907	First public use of radio
1911	First mobile transmitter (Zeppelin)
1915	First wireless voice transmission
1927	First car radio
1928	First TV broadcast
1933	First mobile phone (Germany, in-car)
1950s	UNIVAC(UNIVersal Automatic Computer) Ia mainframe
1958	First hand-held mobile phone
1961	Cloud computing precursor (John McCarthy)
1969	Internet precursor (ARPANET)
1973	1G cellular mobile (NTT, Japan)
1981	First wireless IoT connection(Coke machine, GSM)
1982	International Internet
1988/89	World Wide Web
1990	2G cellular mobile (GSM)

Year	Discovery
1991	Bluetooth
1994	Wi-Fi (CSIRO, IEEE)
1997	3G cellular mobile (UMTS)
1998	4G cellular mobile (LTE)
1999	IoT term coined
2005	United Nations mention IoT
2008	5G cellular mobile
2008	Cloud computing term coined
2012	Cisco introduces fog computing
2020	Industry expects 20 billion IoT devices worldwide

Table 1.
IoT evolution (adapted from [3, 8, 9]).

Industry	Use case
Smart City	Smartbin offers Smart Waste Monitoring through Smart Sensors & Route Optimization Technologies [10].
Transport	Spanish train operator RENFE uses Siemens' high-speed train and monitors train developing abnormal patterns and sends them back for inspection to prevent failure on the track [11].
Agriculture	Semios uses sensors and machine vision technology to track pest populations in orchards, vineyards, and other agricultural settings [12]
Financial Sector	Progressive Insurance uses Snapshot to determine Insurance premium for car drivers [13].
Healthcare	Abilify MyCite (aripiprazole tablets with sensor) has an ingestible sensor embedded in the pill that records that the medication was taken [14].
Government	US municipality has implemented smart meter monitoring for the entire town's residential and commercial water meters. The project involved placing water meter sensors on 66,000 devices that used to be manually read and recorded [15].
Utility	US oil and gas company is optimizing oilfield production with the Internet of Things. In this IoT example, the company is using sensors to measure oil extraction rates, temperatures, well pressure and more for 21,000 wells [15].
Environment	Autonomous sailboats and watercraft are already patrolling the oceans carrying sophisticated sensor instruments, collecting data on changes in Arctic ice [16].

Table 2.
IoT applications.

IoT has produced a number of sophisticated solutions that are growing in popularity among businesses. Many sectors have already graduated to this technology, and are putting IoT to use for digitizing their daily activities. The prominent adapters of IoT are Smart City, Retail, and Manufacturing. Some of the most notable applications rolled out in the marketplace are given in **Table 2**.

Although, there is a growing interest in IoT applications in different industry sectors, challenges in adoption exist. The key questions are: What are the privacy concerns related to IoT, particularly from a "smart home device" consumer viewpoint? What are the existing remedial approaches for privacy management? This chapter aims to address the above-mentioned questions. The remainder of this chapter is organized as follows. Section 2 presents various privacy concerns of IoT before proposing a novel framework to address IoT concerns from a consumer's perspective in Section 3. This is followed by an initial validation of the framework in Section 4 before we draw conclusions in Section 5.

2. Review of privacy literature with specific IoT focus

Privacy is defined by Clarke as the attention that individuals have in sustaining a personal space, free from interference by other people and organizations [17]. An intrinsic part of privacy issue is the exposure of sensitive data such as Personal Identifiable Information (PII) to non-intended recipients. Personal Identifiable Information (PII) comprises of details such as title, first name, last name, date of birth, address, and phone number, constituting some of the sensitive personal information (SPI). In addition, financial and health details and the geophysical location of an IoT user are also considered as sensitive information.

Internet of Things devices may collect data including sensitive data and store the data for further use for commercial purposes. It comprises of several stakeholders such as customer whose PII is collected; manufacturers who develop the sensors and other networking components and third parties who create IoT mobile apps or use the data for commercial advantage. According to McKinsey global report from 2015 [18], consumers are cautious about embracing IoT-based systems, particularly due to lack of privacy and the data at risk. OECD reported [19] that privacy incidents are growing in both number and sophistication. Similar concerns are expressed by several academic articles which suggest lack of privacy including unauthorized surveillance or eavesdropping [20] as a major concern for individuals.

Some researchers or practitioners confuse privacy with security. While security deals with the management of controlling who can access information, privacy is predominantly focused on granular control of what data can be collected, who can access what, when they can access specific data, and how long the data should be retained.

Protecting user's privacy comprises of technical, human and legal aspects. Other relevant aspects can also be considered.

2.1 Potential scenarios of privacy violation in smart home

Smart home segment comprises of connected appliances like TV set, thermostat, refrigerator, oven, home security, self-guided vacuum cleaners, cleaning and maintenance devices. Additionally, cameras, motion sensors and light sensors also collect data. Most of these data contain private and/or sensitive information such as locations, addresses, pictures and network access information. The data can be accessible to device manufacturer, mobile application owner, third-party vendors or public depending on use cases. There are several scenarios involving data collection such as:

- Movement of individuals (unauthorized surveillance) using motion sensors, camera and GPS tracker.
- Monitoring of actions of customers.
- Sharing of health data publicly from wearable devices or implantable devices such as Abilify MyCite, and Bluetooth-enabled oximeter [18].
- Sharing of data (e.g., financial, health, PII, Payment Card Information and geophysical data) to third party without explicit consent [21].
- Search query of user shows his preference traits (**Figure 1**).

There are very few contributions that address privacy in the context of smart home [22]. While several studies conducted surveys and interviews with IoT end user consumers to investigate the factors affecting privacy including data processing and information risk [23], none proposed a feasible solution to fix them.

Figure 1.
Key data exchanges in smart home.

2.2 Legal aspects of privacy in IoT era

Government organizations are taking significant interest in IoT security, privacy and interoperability from legal aspects. This is in alignment with the studies which advocated further collaboration and dialogs between the regulators and manufacturers of IoT devices to develop appropriate methods to tackle the relevant problems [24]. From regulatory perspective, some of the most important legislative requirements are HIPAA for healthcare, MA risk for supply chain management, California's Senate Bill 327, IoT Cybersecurity Improvement Act of 2017 and General Data Protection Regulation (GDPR).

Data privacy requirements are complex and differ by jurisdictions in regard to the definition of data and the relevant laws/regulations. In Europe, GDPR was introduced on May 25, 2018. GDPR is a new regulation approved by EU parliament, Council and European Commission. It aims to safeguard the personal data rights of EU citizens and residents in this era of new technological advancements. As per GDPR, organizations are required to

- Get explicit and affirmative consent before processing personal data. This includes financial, economic and health data and online information.
- Notify within 72 hours to the regulator and individual about any data breaches.
- Facilitate customers and employees' right to the removal of data from their system.
- Give the right of portability, and increased right of access and right to be forgotten by customer.
- Maintain records of processing activities.

GDPR non-compliance instances may incur penalties up to 2–4% of global revenue or 20 million Euros [25] to organizations based on the infringement. GDPR applies to any company, irrespective of their geographic location, that offers goods and services to European citizens and handles their data including IoT ecosystem-generated data.

In USA, California Senate Bill 327 [26] was introduced recently which allows the State of California ability to bring enforcement complaints against those companies that do not build adequate security safeguards into their Internet-connected IoT

devices [27]. It provides the state the right to hold IoT device makers more accountable for consumer's data security. IoT Cybersecurity Improvement Act of 2017 [28] requires: (i) that IoT devices are patchable, (ii) that devices do not contain known vulnerabilities, (iii) that devices rely on standard protocols, (iv) that devices do not contain hard-coded password and (v) technical aspects of privacy in IoT era.

At present, different privacy-enhancing technologies (PETs) exist to protect privacy. Prevention, by means of access restrictions, is an effective way to safeguard customer privacy. In [29], the authors put forward a concept of using access control list (ACL) and data classification model, to classify data according to its sensitivity and assign tag value to each category. In [30], the authors presented the idea of using Certification Authority (CA)-based encryption to confirm the authenticity of sensor. Some authors argue that it adds overheads and hence it cannot be used as a viable solution. Instead, they proposed incorporating a chaos-based cryptographic scheme and Message Authentication Codes (MAC) for data transmission. In a recent research, authors from IT service firm Tata Consultancy Services recommended that the IoT stakeholders can adopt Preventive Privacy (3P) Framework [31] in order to build trust and confidence among end users.

Privacy by Design (PbD) is defined as another popular approach that enables privacy to be "built in" to the design of the information systems and business processes, ensuring that privacy is considered before, and throughout, the development and implementation of all initiatives that involve personal information [32]. Dr. Ann Cavoukian first proposed it in Canada in the 1990s. PbD is one of the highly recommended approaches to protect individual's privacy [31, 33] concerns in IoT. Unfortunately, even though the USA Federal Trade commission (FTC) and the European Commission accepted PbD to be effective [34], not all manufacturers consider PbD when developing IoT devices and applications.

2.3 People aspects of privacy in IoT era

According to a survey conducted by Cisco in 2017, "human factors" such as organization, culture and leadership contributed to the success of IoT implementations 75% of the time—which was higher than technical aspects [35]. A number of stakeholders are involved in IoT digital ecosystem such as the end users, product suppliers, Internet service providers, cloud storage functionalities and retailers. As mentioned earlier, a significant aspect of the value of IoT for consumers refers to: aggregating data collected from many source systems, generating new knowledge and making fact-based choices. The utilization of data to add value is best explained by the well-known DIKW hierarchy from Ackoff [36]. DIKW is a four-layer hierarchy comprising of data, information, knowledge and wisdom where each layer adds certain characteristics over and above the previous one. **Table 3** shows DIKW in an IoT context.

Hierarchy level	Description
Data	Most basic level of facts. Collected from things and used for storage and processing.
Information	Computing platform adds context to data (who, what, where, when) ingested.
Knowledge	This layer answers the question on how data are used. Analytics is applied in computing platform.
Wisdom	Evaluated understanding of when and why data are used

Table 3.
DIKW in an IoT context.

3. Consumer-centric approach

While IoT organizations are aware of the need for adopting PET and incorporating PbD, there is little guidance available on how to do so. Though there are PbD-driven frameworks available [34], no concrete solutions to establish auditing mechanism or control method systems have been developed (**Table 4**).

The lifecycle of an IoT service or product is shown in **Figure 2**.

Figure 3 summarizes: what can be done, at the minimal level, by consumer to safeguard his/her privacy. This provides the basis for the further development of

	Pre-purchase		**Setup/post purchase**	**Decommission**
Awareness omni channels	**Research + solution purchase**		**Use + feedback**	
• Web • Social • Mobile • In-store • Media • Advertising • Direct Marketing	• Products which provide audit mechanism while dealing with PII [20] • Products which notify user to provide dynamic consent for data use [37] • Products which stop working properly when consent is not given by user [38] • Firmware upgrade and patchability of IoT devices [24] are available. • Products transparent on how disclosed data are used by the developer of the IoT system or application [39] • Established reputed product with no or negligible data breach history		• Setting up, configuring and registering to IoT services • Signing Consents authorizing data to be collected and used by IoT service provider. • Update Firmware and mobile applications	• Remove authoriza-tion of IoT vendor to use your data • Deregister and destroy data.

Table 4.
Consumer's perspective of IoT product lifespan.

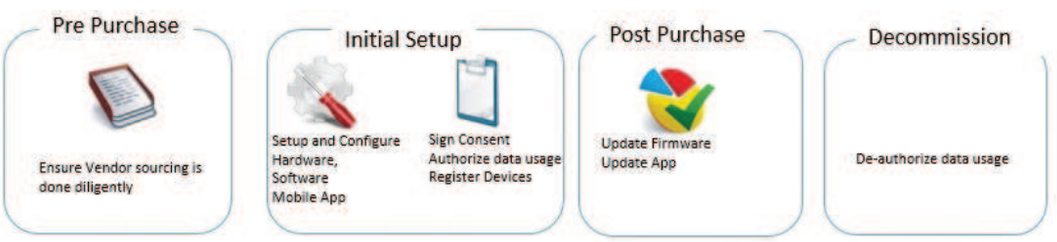

Figure 2.
IoT product lifecycle.

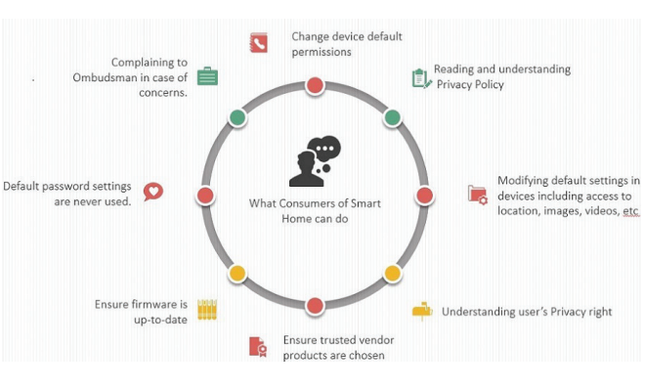

Figure 3.
Mitigation options for consumers (based on [31, 46, 47]).

Consumer questions	Risk factors
Who has access to the data? Will third parties have access to the data? What information can be inferred from the data?	Unacceptable usage of data without consent such as spamming
Will my data be shared outside my country?	Data sovereignty constraints
How will I be informed in case my data are compromised?	Data detection and notification of breach
Are there any known breaches or vulnerabilities about this device?	Outdated Firmware
What happens when I stop using the product or service?	De-authorization
Can my location be tracked from data?	Unveiling of physical address
What can I do if my PII is compromised?	Password renewal
How can I rectify my data?	Outdated information
Can I get a copy of my data or access my data?	Portability
Can I ask you to remove my digital footprint captured by the IoT service?	Unaligned data erasure

Table 5.
Key questions in IoT for consumers.

an IoT privacy tool or framework, which can address the concerns of the consumer [31, 40–45] compiled in **Table 5**.

4. Proposed framework

As mentioned in earlier section, the existing frameworks are relevant primarily for thing manufacturer and do not involve end thing consumers. Through this chapter, we seek to provide answers to the questions mentioned in **Table 5** by leveraging a four-phased data governance-driven 4I framework (Identify, Insulate, Inspect and Improve). The Identify phase of the 4I framework (**Figure 4**) comprises of seven key dimensions such as risk, compliance, policy, process, people, data asset and technology (**Table 6**).

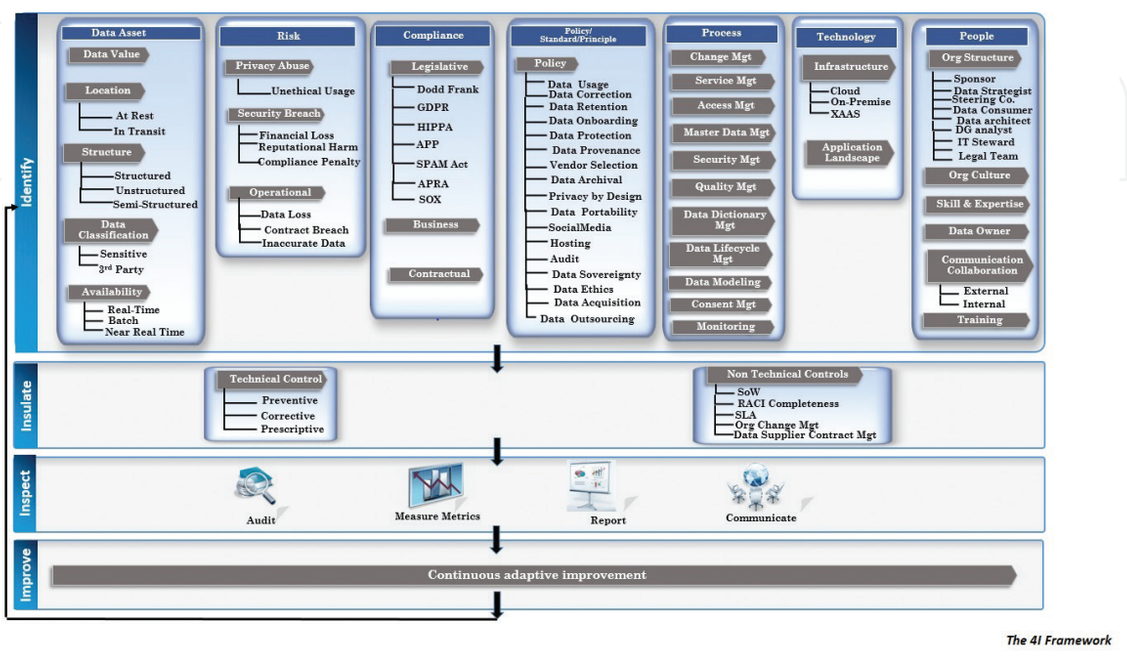

Figure 4.
The 4I framework.

Dimension	Description
Risk	Risk dimension comprises of the factors that influence both the IoT end user and thing manufacturer. It includes attributes such as lack of consent data breach, legal penalties, service level agreement violation, and lack of upgradability, interoperability and security [20, 41, 48, 49].
Compliance	Includes legal requirements (e.g., user consent), controls and baselines to be operationally compliant. There are a number of regulations such as SOX, GDPR, SPAM Act, Australian APP Privacy law, HIPPA and COPPA which are relevant for IoT [50].
Policy, standards and principles	This dimension spans the lifecycle from inception to deletion of data including items such as data sharing, acceptable use of data, data classification and storing rules. A well-defined and enforced governance providing the structure that works for the benefit of everyone concerned by ensuring that the IoT stakeholders adhere to accepted ethical standards [44, 51].
Data asset	Describes the benefit of the data and the salient features of the data [52, 53].
Process	Defines how various interfaces and functionalities are to deliver a functioning and solution [54].
People	The different stakeholders and their accountability in the IoT ecosystem such as consumer, ombudsman, policy maker, IoT thing manufacturer, IoT cloud provider, Internet service provider and the IoT service operators. People dimension also includes leadership and organization structures [55, 56].
Technology	This dimension includes hardware infrastructure, platforms and software agents that notify potential compliance violation through monitoring and workflows [34, 53].

Table 6.
Key dimensions of the Identify phase of the 4I framework.

Identify stage or phase refers to the key risks, requirements and context. Insulate stage refers to the precautionary measures taken to prevent lapses using technologies and non-technical risk remediation techniques. Inspect stage contains the essential toolkits such as maturity models, audit mechanisms, software agents required to continuously monitor, report and assess the IoT Data Governance Maturity from risk and value perspectives. The final stage focuses on continuous improvement.

4.1 The 4I framework applied to privacy context

To illustrate how the proposed 4I framework will work in an IoT-enabled home, a use case involving smart refrigerator is discussed in this section. Currently, when consumers buy an IoT device directly from vendors or service providers, they may have very little understanding when agreeing to the privacy policy (PP) and terms and conditions (T&C) before they start using the product or services or application. However, there are several risks associated with the data collected to render the services.

For example, the smart refrigerator can track our food preferences, search and order food from online stores [31]. Various traits of the fridge owners' eating behaviors can be inferred based on the search queries. If these data are sent to third-party business, they can use the information for the purpose of undesirable targeted advertisements. This can lead to the potential breach of privacy violating regulatory laws if explicit consent was not obtained from the consumer (**Figure 5**).

The **Identify** phase of the 4I framework discerns the potential risks associated with the consumer's data shared among the data processors in data supply chain. For example, it reviews the laws such as GDPR to understand the data protection rights of a smart home user [57] and ascertains the risk related to privacy and security breach. Policies related to data retention, service level agreement with vendors and data management are implemented in the **Insulation** phase of the framework. For instance, an agent called checkmyprivacyrules (CPMRs) can be installed at user's home router to ensure privacy policy and laws like GDPR are not violated based on a search query (**Figure 6**).

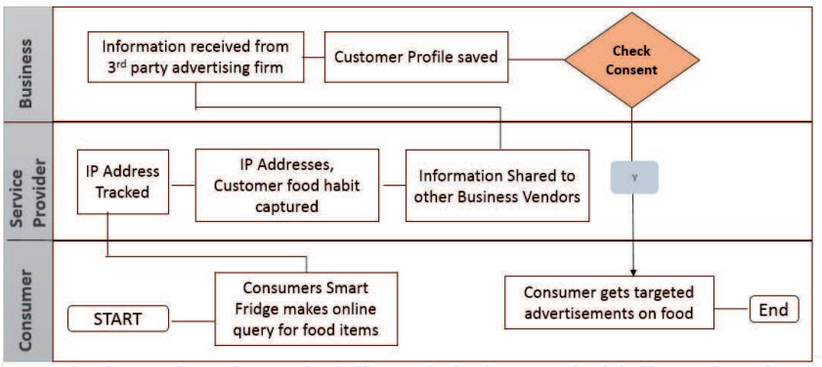

Figure 5.
Business process in smart home refrigerator.

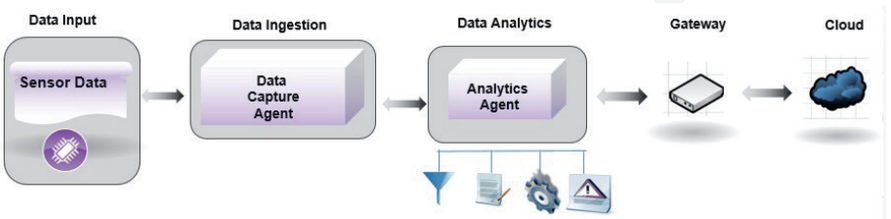

Figure 6.
Smart home 4I (filters, policies, rules, permissions) (adopted from [58]).

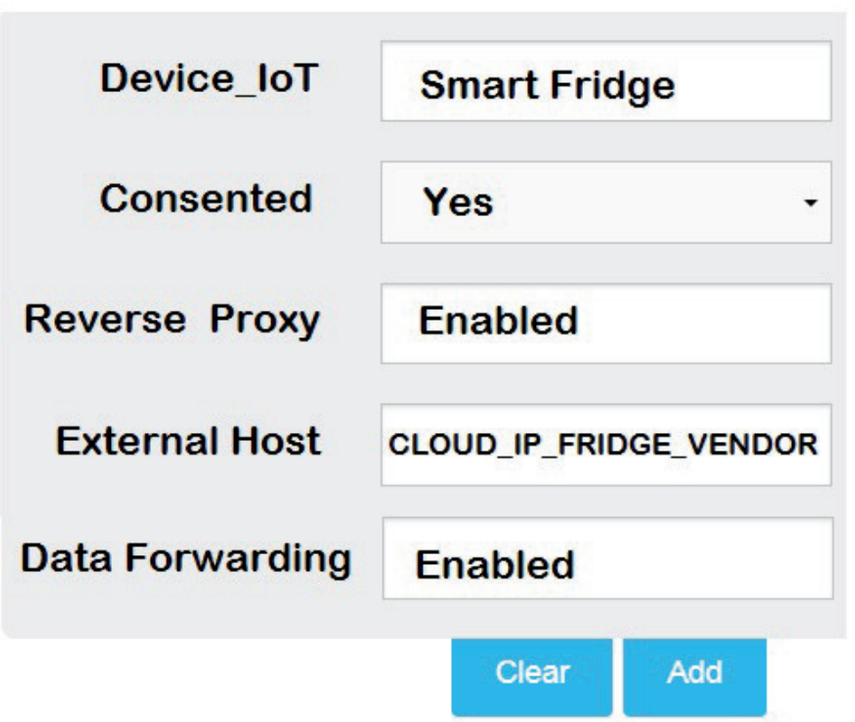

Figure 7.
Web configuration to add privacy rule for smart fridge.

Figure 7 shows a screen where smart fridge user can setup who can access the data. With the above settings, smart fridge can send data to cloud if

a. Device has latest firmware updates. This can be verified from Firmware update version captured periodically from Vendor Website by the agent installed in the router

b. Intended address to push data in the packet states matches external host IP address

c. Consent is set to "Yes"

d. Reverse Proxy is enabled. This will ensure even if the ISP or business gets IP address, it will not be accurate.

Listing 1 shows the Pseudo code of the agent.

CheckMyPrivacyRules (Di)	Di is the set of all smart IoT devices in a "Smart Home" and Di ⊂ D
*Di - > device_*	
Rij - > rule j for device Di	Rij is the ruleset j applied to Device Di before it leaves home network
Begin	
For each Di in domain D	Pi is the packet send by Di to the router.
For each rule Rij	
If substring(Pi)- = Rij.	
Transmit Data;	
Else	
Send SMS/email to user	
Stop polling Di	
Endif	
Endif	

Listing 1.
Pseudocode for CPM.

The Inspection phase comprises of performing audit reviews periodically to assure the compliance of the process, systems and data flow. The **Inspect** phase can comprise of automated data quality checks and data access log monitoring. In the I**mprove** phase, continuous improvement is done to ensure the continuous adaptation in response to changing data privacy requirements and landscape. For example, improving the agent to ensure software is not only patched to current version, but also data are secured using tokenization techniques [59] can be an outcome of this final phase of the 4I framework.

5. Conclusion

IoT's business growth potential is undeniable. Advancement in IoT has opened up new prospects for growth in the diversified areas such as health, energy, transport and smart home. In this chapter, we provided an overview of the IoT technology and real-life examples of usage of this technology. Next, we discussed the privacy problems in IoT from a consumer's perspective. A review of the related work was presented along with research gaps. Next, we proposed and provided an overview of a data governance-driven 4I framework. Finally, we provided the pseudocode and demonstrated the applicability of the 4I framework to address the privacy concerns in a smart home refrigerator context. This involved the policies, rules and configurations using time-tested data governance principles. In future, we intend to further test and improve the 4I framework in the overall context of data governance in digital ecosystem.

Acknowledgements

This research is supported by an Australian Government Research Training Program Scholarship.

Conflict of interest

There is no conflict of interest.

IntechOpen

Author details

Avirup Dasgupta*, Asif Qumer Gill and Farookh Hussain
University of Technology Sydney, Ultimo, NSW, Australia

*Address all correspondence to: avirup.dasgupta@student.uts.edu.au

IntechOpen

References

[1] Bader A, Ghazzai H, Kadri A, Alouini MS. Front-end intelligence for large-scale application-oriented internet-of-things. IEEE Access. 2016;**4**:3257-3272

[2] Global Internet of Things (IoT) Device Market, Forecast to 2024; 2018

[3] Rose K, Eldridge S, Chapin L. The Internet of Things: An Overview. The Internet Society (ISOC); 2015. pp. 1-50

[4] Jalali S, Bhatnagar I, editors. Leveraging Internet of Things Technologies and Equipment Data for an Integrated Approach to Service Planning and Execution. 2015 IEEE Region 10 Symposium; 2015 13-15 May 2015

[5] Ma H-D. Internet of things: Objectives and scientific challenges. Journal of Computer Science and Technology. 2011;**26**(6):919-924

[6] Dong L, Mingyue R, Guoying M. Application of internet of things technology on predictive maintenance system of coal equipment. Procedia Engineering. 2017;**174**:885-889

[7] Department CMUCS. The "Only" Coke Machine on the Internet [Internet]. Available from: https://www.cs.cmu.edu/~coke/history_long.txt [Accessed: 2018-11-29]

[8] Minerva R, Chebudie AB, Rotondi D. Towards a definition of the Internet of Things (IoT) 2015 [Internet]. Available from: http://iot.ieee.org/definition.html [Accessed: 2018-11-29]

[9] Gill AQ. Adaptive Cloud Enterprise Architecture. Hackensack, New Jersey: World Scientific; 2015

[10] Sharma N, Singha N, Dutta T. Smart bin implementation for smart cities. International Journal of Scientific and Engineering Research. 2015;**6**(9):787-791

[11] Tracy P. Case study: Siemens reduces train failures with Teradata Aster 2016 [Internet]. Available from: http://www.rcrwireless.com/20160912/big-data-analytics/siemens-train-teradata-tag31-tag99 [Accessed: 2018-11-29]

[12] Kshetri N. The economics of the internet of things in the global south. Third World Quarterly. 2017;**38**(2):311-339

[13] Handel P, Skog I, Wahlstrom J, Bonawiede F, Welch R, Ohlsson J, et al. Insurance telematics: Opportunities and challenges with the smartphone solution. IEEE Intelligent Transportation Systems Magazine. 2014;**6**(4):57-70

[14] FDA approves pill with sensor that digitally tracks if patients have ingested their medication [press release]; 2018

[15] Alison Bolen SIE. 3 Internet of Things examples from 3 industries [Internet]. Available from: https://www.sas.com/en_us/insights/articles/big-data/3-internet-of-things-examples.html [Accessed: 2018-11-29]

[16] Hughes RB. The autonomous vehicle revolution and the global commons. SAIS Review of International Affairs. 2016;**36**(2):41-56

[17] Clarke R. Internet privacy concerns confirm the case for intervention. Communications of the ACM. 1999;**42**(2):60-67

[18] Manyika J, Chui M, Bughin J, Dobbs R, Bisson P, Marrs A. Disruptive Technologies: Advances that Will Transform Life, Business,and the Global Economy. San Francisco, CA: McKinsey Global Institute; 2013

[19] OECD. Managing Digital Security and Privacy Risk; 2016

[20] Hernández-Serrano J, Muñoz JL, Bröring A, Esparza O, Mikkelsen L, Schwarzott W, et al., editors. On the Road to Secure and Privacy-Preserving IoT Ecosystems. Cham: Springer International Publishing; 2017

[21] Mullen M. The Internet and Public Policy: Privacy and Consumer Protection; 2018

[22] Kraemer MJ, Flechais I, editors. Researching privacy in smart homes: A roadmap of future directions and research methods. In: Living in the Internet of Things: Cybersecurity of the IoT - 2018. 2018 28-29 March 2018

[23] Almusaylim ZA, Zaman N. A review on smart home present state and challenges: Linked to context-awareness internet of things (IoT). Wireless Networks. 2018

[24] Sivaraman V, Gharakheili HH, Fernandes C, Clark N, Karliychuk T. Smart IoT devices in the home: Security and privacy implications. IEEE Technology and Society Magazine. 2018;**37**(2):71-79

[25] Commission E. European Commission. Eu Data Protection Reform What Benefits for Businesses in Europe; 2016

[26] Jackson S. SB-327 Information privacy: connected devices; 2018

[27] California Bill Mandates Privacy By Design For IoT Devices. ICT Monitor Worldwide. 2017 04/28/2017 Apr 28

[28] Senators Mark Warner CG, Ron Wyden, and Steve Daines. Cybersecurity Improvement Act 2017 [Internet]. Available from: https://www.warner.senate.gov/public/_cache/files/8/6/861d66b8-93bf-4c93-84d0-6bea67235047/8061BCEEBF4300EC702B4E894247D0E0.iot-cybesecurity-improvement-act---fact-sheet.pdf [Accessed: 2018-11-29]

[29] Muzzammil H, Neha K. An improvised framework for privacy preservation in IoT. International Journal of Information Security and Privacy (IJISP). 2018;**12**(2):46-63

[30] Jie Y, Pei JY, Jun L, Yun G, Wei X, editors. Smart home system based on IOT technologies. In: 2013 International Conference on Computational and Information Sciences. 2013 21-23 June 2013

[31] Chaudhuri A, Cavoukian A. The proactive and preventive privacy (3P) framework for IoT privacy by design. EDPACS. 2018;**57**(1):1-16

[32] Commissioner for Privacy and Data Protection V, Australia. Guidelines for Sharing Personal Information; 2016

[33] Caron X, Bosua R, Maynard SB, Ahmad A. The internet of things (IoT) and its impact on individual privacy: An Australian perspective. Computer Law and Security Review. 2016;**32**(1):4-15

[34] Porambage P, Ylianttila M, Schmitt C, Kumar P, Gurtov A, Vasilakos AV. The quest for privacy in the internet of things. IEEE Cloud Computing. 2016;**3**(2):36-45

[35] Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing [press release]; 2017

[36] Jifa G, Lingling Z. Data, DIKW, Big Data and Data Science. Procedia Computer Science. 2014;**31**:814-821

[37] Infosys. IoT Connected World; 2018

[38] Cushing T. LG Will Take The 'Smart' Out Of Your Smart TV If You Don't Agree To Share Your Viewing And Search Data With Third Parties Techdirt; 2014 [Internet]. Available from: https://www.techdirt.com/articles/20140511/17430627199/lg-will-take-smart-out-your-smart-tv-if-you-dont-agree-to-share-your-viewing-search-data-with-third-parties.shtml [Accessed: 2018-11-29]

[39] Baldini G, Botterman M, Neisse R, Tallacchini M. Ethical Design in the Internet of things. Science and Engineering Ethics. 2018;**24**(3): 905-925

[40] Michael S. Smith. Protecting Privacy in an IoT-Connected World. Tech Trend; 2015

[41] Wachter S. Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR. Computer Law and Security Review. 2018

[42] Al-Ruithe M, Mthunzi S, Benkhelifa E, editors. Data governance for security in IoT & cloud converged environments. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). 2016 Nov. 29 2016-Dec. 2 2016

[43] Sicari S, Rizzardi A, Grieco L, Coen-Porisini A. Security, privacy and trust in Internet of Things: The Road Ahead; 2015

[44] Chauhan S, Agarwal N, Kar AK. Addressing big data challenges in smart cities: A systematic literature review. Info. 2016;**18**(4):73-90

[45] Zarkout B. Making the Case for Governance IoT Data; 2017

[46] Barcena MB, Wueest C. Insecurity in the Internet of Things. Security Response, Symantec; 2015

[47] Miettinen M, Marchal S, Hafeez I, Asokan N, Sadeghi A, Tarkoma S, editors. IoT SENTINEL: Automated device-type identification for security enforcement in IoT. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). 2017 5-8 June 2017

[48] Mansfield-Devine S. Data protection: Prepare now or risk disaster. Computer Fraud & Security. 2016;**2016**(12):5-12

[49] Maple C. Security and privacy in the internet of things. Journal of Cyber Policy. 2017;**2**(2):155-184

[50] van den Broek T, van Veenstra AF. Governance of big data collaborations: How to balance regulatory compliance and disruptive innovation. Technological Forecasting and Social Change. 2018;**129**:330-338

[51] Weber R. Governance of the internet of things—From infancy to first attempts of implementation? Laws. 2016;**5**(3):28

[52] Liu C, Yang C, Zhang X, Chen J. External integrity verification for outsourced big data in cloud and IoT: A big picture. Future Generation Computer Systems. 2015;**49**:58-67

[53] Karkouch A, Mousannif H, Al Moatassime H, Noel T. A model-driven framework for data quality management in the internet of things. Journal of Ambient Intelligence and Humanized Computing. 2018;**9**(4):977-998

[54] Singh VK, Guo J, editors. Improving service levels using internet of things infrastructure in data Centers. In: 2016 IEEE International Conference on Smart Computing (SMARTCOMP). 2016 18-20 May 2016

[55] Gantait A, Patra J, Mukherjee A. Defining your IoT governance practices: IBM; 2018 [Internet]. Available from: https://www.ibm.com/developerworks/library/iot-governance-01/index.html [Accessed: 2018-11-29]

[56] Al-Ruithe M, Benkhelifa E, Hameed K. Data governance taxonomy: Cloud versus non-cloud. Sustainability. 2018;**10**(1):95

[57] Sharma S, Chen K, Sheth A. Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems. IEEE Internet Computing. 2018;**22**(2):42-51

[58] Adler S. The IBM Data Governance Council Maturity Model: Building a Roadmap for Effective Data Governance. Somers, NY, USA: IBM Corporation; 2007

[59] Tokenization P. Securing Sensitive Data for PCI. HIPAA and Other Data Security Initiatives. 2011. p. 13