Open Access License Notice

Educating Consumers on the Security and Privacy of Internet of Things (IoT) Devices: A Quantifiable Security Compliance Measurement System to Aid in Purchasing Decisions

Mahmood Khadeer
mkhadeer@uw.edu

Marc Dupuis
marcjd@uw.edu

Samreen Khadeer
samreen@uw.edu

University of Washington Bothell
Box 358534
Bothell, WA 98011-8246

Abstract - As the adoption of technology grows, consumers have many avenues to buy IoT devices and install them for their needs yet they have very little information about the security of the devices. The companies that are manufacturing the devices have no incentive to invest in the security of the devices or to let consumers know the security status of their respective devices. The competitive cost and time pressure faced by manufacturers is causing consumers to suffer from the vulnerabilities in their devices. This project makes three contributions to the development of security verification for IoT devices. First, it develops a quantifiable security compliance measurement system to measure the security of consumer IoT (SCMSI) devices. The SCMSI framework uses the OTA recommended Trust Framework augmented with key design and development security concerns to develop the criteria to measure the devices. Second, a scoring model is developed for each of the security requirements in the SCMSI framework.

Third, a consumer facing pilot website is built to show the proof of concept of evaluating IoT devices and providing security ratings to consumers. Limitations and future directions are discussed.

Categories and Subject Descriptors

Security and privacy - Trust frameworks
Security and privacy - Security requirements
Security and privacy - Network security
Security and privacy - Usability in security and privacy

General Terms

Internet of Things, Consumer, Security, Privacy

Keywords

Internet of Things, IoT, security, privacy, framework, consumer devices, quantifiable security compliance measurement system

1 INTRODUCTION

The Internet of Things (IoT) refers to the network of physical devices embedded with sensors and connected to existing Internet infrastructure. The network connectivity provides the ability to collect and share data across devices. IoT adoption trends are growing rapidly. Unlike more established technological terms, there is no single definition of IoT. The analyst firm Gartner defines IoT as "The network of physical objects that contain embedded technology to communicate and interact with their internal states or the external environment" [1].

The International Data Corporation (IDC) forecasts a revenue growth to $1.3 trillion by 2019 [2] with over 75 billion IoT devices projected by 2020 [3]. The

key business drivers of this trend are reduction in cost, new revenue opportunities, and increased customer satisfaction and retention.

It has been suggested that technological advancements in hardware and software will make IoT security a fast growing area and the standards and API will become essential because IoT devices need to interoperate and communicate, as many business models will rely on sharing data with multiple devices and organizations [4].

In addition to all the benefits that are provided by the deployment of IoT devices there are inherent security risks that must be addressed. The expanded surface area provides hackers with new opportunities to disrupt lives and cause permanent damage.

As the adoption of technology grows, consumers have many avenues to buy IoT devices and install them for their needs yet they have very little information about the security of the devices. The companies that are manufacturing the devices have no incentive to invest in the security of the devices or to let consumers know the security status of their respective devices. The competitive cost and time pressure faced by manufacturers is causing consumers to suffer from the vulnerabilities in their devices.

The decentralized approach to security and privacy poses several challenges. A comprehensive integrated vision to address security and privacy is lacking. In order to realize this vision a lot of research needs to be done in the coming years in areas such as authentication of sensors, authentication of requests for access control, secure point to point connection, etc. [5]

With pervasive deployment of IoT devices by the health industry, manufacturing companies, and governments, many IoT devices currently in the market are completely insecure without the customers' knowledge. Many devices don't have SSL implemented and are missing encryption overall.

The fragmentation in the consumer market is huge. The devices are being produced around the world on a daily basis with minimal cost and no focus on security. Enterprises, although also a priority for security considerations, have tighter controls to evaluate the deployment of IoT systems. For example, Azure IoT and AWS IoT are secure platforms. Both Microsoft and Amazon invest in ensuring the security of the platform and interconnected devices that work with the platform. Hence the exposure for security risks is comparably lower for enterprises than for consumer IoT devices given the market landscape.

The security considerations remain incredibly low in the prevalent space of IoT. The diagram below illustrates the challenges that manufacturers face as it relates to cost, ease of use and security while developing IoT products.

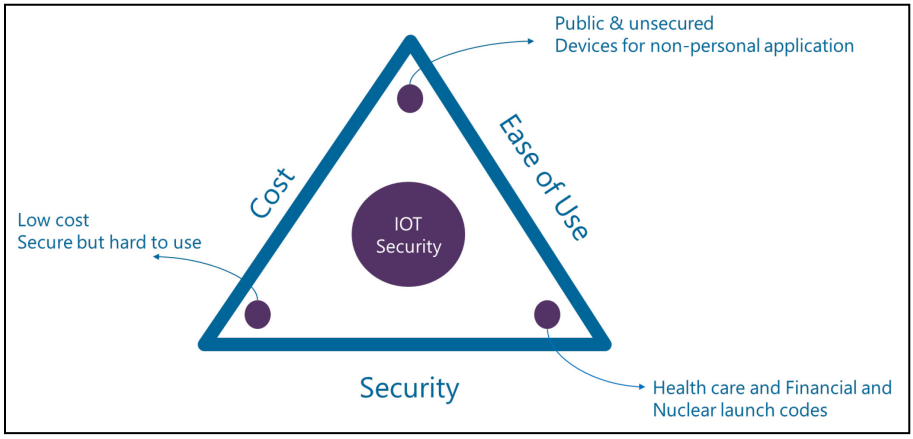

Figure 1: Dashboard displaying the security compliance measurement rating (SCMR) for a typical consumer device.

In the diagram, the further distance from the plane, the focus on the attribute value lessens. As demonstrated in Figure 1 above, the lower left corner indicates a focus on low cost, and secure, but hard to use devices. The top corner indicates a focus on low cost, unsecure, but easy to use devices. The right corner indicates a

focus on highly secure, easy to use devices where cost is not an issue (e.g., health care, financial sector, military applications).

This research is intended to close the gap of knowledge for consumers regarding the security of the IoT devices that they are using by providing consumers and industry partners a simple way to determine the security of a consumer IoT device.

The IoT consumer device has three main components which need to be interconnected. They include the device itself (hardware), application that enables the device (e.g., app on phone), and a cloud service. The proposed framework addresses the security requirements of the IoT device covering all three areas.

For the purposes of the research, the consumer will visit the Security Compliance Measurement System for IoT (SCMSI) website and select a category of device and all of the devices that are assessed in that category are displayed. The consumer will then select the desired device and the system will display a dashboard with the security rating. The dashboard will also display the score secured by that device in the four categories of evaluation: Design and Development; Security of the Device; User Credentials of the Device; and Privacy, Disclosures, and Transparency. If a device is not in the system database, the consumer will be presented with a form to add a new device. After gathering the information from the consumer, the request will be prioritized, and the device will be added to the database and the consumer will receive a notification.

The SCMSI will provide consumers with the ability to know the security rating of the device they are purchasing easily, enabling them to make informed purchasing decisions. As consumers become more knowledgeable and purchase products with higher security protocols, manufacturers will in turn invest more in the security measures of their IoT devices to remain competitive in the market.

In summary, this project makes three contributions to the development of security verification for IoT devices. First, it develops a quantifiable security compliance measurement system to measure the security of consumer IoT devices. The SCMSI framework uses the OTA recommended Trust Framework augmented

with key design and development security concerns to develop the criteria to measure the devices. Second, a scoring model is developed for each of the security requirements in the SCMSI framework. Third, a consumer facing pilot website is built to show the proof of concept of evaluating IoT devices and providing security ratings to consumers.

2 BACKGROUND

The IoT space being so new and upcoming, not much work has been done in certifying IoT devices. The two industry bodies that have provided guidance from the security perspective for IoT consumer devices are the Online Trust Alliance (OTA) and the Open Web Application Security Project (OWASP). The OTA provides a Trust Framework [6] and OWASP offers a top 10 list of IoT security issues [7]. However, neither of these provide a methodical way to develop a scoring model for IoT devices.

Another body that has started providing guidance on IoT security is the National Institute of Standards and Technology (NIST). However, the framework focused heavily on cyber-physical systems. This framework provided a common blueprint for the development of safe, secure, and interoperable systems mostly targeted towards industrial applications such as smart energy grids. In the future, we will monitor the progress NIST makes as it relates to consumer IoT devices and incorporate it into our work in areas such as risk management and the development of safe and secure interoperable devices [8].

To inform the focus areas for building a robust security framework for consumer IoT devices, we reviewed not only the frameworks currently being developed, but also recent activity in the industry to inform the SCMSI framework.

As IoT expands in the global Internet based exchange of goods and services, it poses new security and privacy challenges, requiring specific measures to be put in place to architect solutions that are resilient to attacks and put in place secure data authentication and access control mechanisms [9]. Every day smart objects are becoming a part of our lives as consumers are getting more into deploying various

IoT devices. This requires us to consider specific and varying needs of the consumers in addition to the IoT device requirements. The framework for architectural design needs to expand the traditional Architecture Reference Model (ARM) by putting a strong emphasis on security, trust, and privacy [10].

Additionally, IoT devices are increasingly connected to the cloud, which is becoming a natural enabler. Cloud security needs to be considered from the perspective of cloud tenants, end users, and cloud providers working across a range of IoT technologies. The key areas to consider are secure communications, access controls for IoT clouds, and identifying sensitive data [11].

Furthermore, the growing proliferation of IoT devices is creating a large surface area for attackers. They now have a broad spectrum of targets from which to choose and their objectives have shifted to the capturing of any system, as opposed to a specific system. They can leverage the interconnectivity between systems to sabotage them and cause extensive damage [12].

Thus, the threat to IoT is real and needs attention. Today, there is very little information available on certifying security measures on consumer IoT devices. Although there are many papers which describe the security issues that are likely to arise in consumer devices, nearly all lack information to help consumers identify the security of a typical IoT device. In the subsequent sections we will discuss the OTA Trust Framework and the OWASP security guidance for consumer IoT devices. The SCMSI model that was developed for this project was built on top of the OTA Trust Framework.

2.1 OTA IoT Trust Framework

The IoT Trustworthy Working Group (ITWG) was established in January 2015. The multi-stakeholder group was assigned with the responsibility of developing a framework to address security, privacy, and viability of IoT products. The scope of the Trust Framework was primarily for the connected home and consumer facing wearable technologies. The framework emphasizes that the security in IoT devices must be considered holistically from product development to security by design.

The ITWG further developed expanded guidance with examples and resources to test device security [6].

The IoT Trust Framework is categorized into three sections: *Security, User Access and Credentials, and Privacy, Disclosures, and Transparency*.

- *Security*: The security section has 10 requirements that consist of the overall security of IoT devices
- *User Access and Credentials*: This section has five requirements that address user access and control.
- *Privacy Disclosures and Transparency*: This section has 15 requirements including privacy disclosure and transparency related areas.

2.2 Consumer IOT Security Guidance from OWASP

OWASP provides basic level security guidance to consumers when they purchase IoT devices [7]. The guidance is by no means comprehensive. There are 10 basic recommendations from OWASP for consumers. They include areas such as web interface security, authentication and authorization, network security, transport encryption, privacy concerns, cloud interface security, mobile interface security, security configuration capability, software and firmware update, and physical security.

The OTA IoT Trust Framework provides a comprehensive list of requirements to verify security of IoT devices. The OWASP provides generic guidance on security to consumers. The remaining issue is that consumers don't have enough knowledge to verify that the device they are acquiring has adequate security protocols. Consumers need a simple mechanism to determine the security rating of a device so that they can make intelligent purchase decisions.

Both the OTA Trust Framework and the OWASP guidance do not provide any information on the relative importance of each requirement from the security perspective. Also, they don't provide any guidance on how to evaluate IoT devices.

Additionally, the SCMSI model presented here provides a conceptual website where a consumer can easily find out the security ratings of devices before purchase. The relative ratings from the security perspective was developed in discussion with three industry experts. The ratings will also be shared with the OTA to gather additional feedback for ongoing improvement of the system. The proposed quantifiable security compliance measurement system for IoT devices will provide consumers with easy to access information on the security of devices they intend to purchase.

3 IOT SECURITY COMPLIANCE FRAMEWORK

This project explored the opportunity to develop a quantifiable security compliance measurement system for IoT devices. This task was accomplished by first developing a detailed framework of critical security requirements for IoT devices including the 30 requirements defined by the OTA Trust Framework. For each of the requirements, they were rated on a relative scale of importance: 1-low importance, 3-medium importance and 7-high importance. Each requirement was given base points and then multiplied by the importance factor to determine the security compliance measurement rating.

Devices will be checked against each of the 47 requirements and they can either comply or not. Once they comply they will get the full score of that requirement. If they don't comply or partially comply they are assigned a zero score against that requirement. All the scores are summed up to a maximum score of 1000.

The concept was verified and piloted with 12 IoT devices on the basis of publicly available information in three categories: Home security, Personal Wellness, and Smart Appliances. The results are shown on the pilot consumer website that is available at: https://scmsi.azurewebsites.net.

3.1 SCMSI Framework Detail Security Requirements

The SCMSI framework was developed by leveraging the 30 principles of the OTA IoT Trust Framework. Seventeen additional design and development

requirements were added as well. The SCMSI framework consists of: 1) Design and Development 2) Security (OTA) 3) User access and control (OTA) 4) Privacy, Disclosures, and Transparency (OTA). All four sections comprising a total of 47 key requirements comprehensively address critical security requirements for any consumer IoT device.

1. *Design and Development*: The design and development section has 17 key SDL requirements against which the IoT device will be evaluated for compliance.

2. *Security (OTA)*: The Security (OTA) section has 10 key requirements against which the IoT consumer device will be evaluated for compliance.

3. *User Access and Credentials (OTA)*: This section has 5 requirements that consist of the following user access and control related features.

4. *Privacy, Disclosures, and Transparency (OTA)*: This section has 15 requirements that comprehensively address all privacy and transparency related requirements.

3.2 SCMSI Framework Scoring Model

The developed framework as described above captured all key security requirements from SDL as well as OTA recommendations. However, in order to assess and compare the IoT devices, a scoring model is required. In the developed scoring model, a maximum of 1000 points were allocated towards 47 requirements. This was done following the six-sigma, other lean guidance, and discussing with experts.

All 47 requirements are verified for relative importance and given a multiplier of 7 for those which are of high importance, 3 for medium importance, and 1 for low importance. This relative importance rating was completed by three security industry experts. The summary of these ratings is shown in Table 1 below.

Expert	7 (High)	3 (Medium)	1 (Low)
1	18	15	14
2	21	16	10
3	13	19	15

Table 1: Security Expert Rating Summary

Expert KA rated 18 requirements of high importance. AM rated 21 requirements of high importance and SH rated 13 requirements of high importance.

Table 2 below describes the agreement on the requirements ratings by the experts.

Description	Number of Requirements
All three experts rated the same	27
At least two experts rated the same	16
All three had different ratings	4

Table 2: Requirements Ratings Agreement Summary

The majority of the ratings were exactly the same by all three experts. In 16 of the requirements at least two ratings matched. In 4 of them they all differed. In the SCMSI model, we used the same recommendation where all the three experts agreed, we used the majority recommendation of the two experts for 16

requirements, and we used medium importance for the 4 requirements where they all differed.

Table 3 describes the baseline points as well as the overall points after applying the agreed multiplier for each of the requirements.

Area	Baseline	Score with multiplier
Design and Development	200	760
Security (OTA)	300	1600
User Access and Credentials (OTA)	125	425
Privacy, Disclosures and Transparency	375	975
	1000	3760

Table 3: Total baseline points for all categories including multiplier

The following metrics were developed and verified by the security experts. Device ratings will be given as per Table 4 below.

Score	Rating	Color
>=750	A	Green
>=600 <750	B	Yellow

>=500 < 600	C	Orange
<500	F	Red

Table 4: Scoring Rubric for Consumer IoT Devices

Additionally, to verify the compliance against all 47 requirements the following were needed: the collaboration and cooperation of the manufacturer of the device, the device itself to test, and access to publicly available information. Table 5 shows the breakdown of validation methods necessary for each requirement.

Requirements Area	**C**	**CD**	**D**	**P**	**Total**
Design and Development	16	1			17
Security (OTA)	4	2	4		10
User Access and Credentials (OTA)	1	2	2		5
Privacy, Disclosures and Transparency (OTA)		3		12	15
Total	**21**	**8**	**6**	**12**	**47**

Table 5: Validation Dependency: Company, Device, & Public Information
C: Company Collaboration; CD: Company Collaboration and Device; D: Device; P: Public Information

Twenty-nine requirements need company collaboration to verify compliance and 18 require device access and publicly available information. The challenge and

opportunity presented is to work with the standards bodies such as the OTA and manufacturers to provide services for compliance verification for the devices.

3.3 SCMSI Model Applied to Sample IoT Devices

The SCMSI framework and the model were tested with a sample of IoT devices. IDC identifies three use cases that will become prevalent in 2016 [4]. Consumer segments will expand in three areas: 1) home security / home monitoring; 2) personal wellness, and 3) smart appliances. These three categories were selected to pilot the compliance measurement of consumer IoT devices. Four devices in each category were selected. These devices were evaluated against publicly available information as well as reviewing the latest trends [13].

a. *Home Security / Home Monitoring*: Consumer interest in home security IoT devices is growing.
b. *Personal Wellness*: Personal wellness IoT devices are gaining traction for personal fitness. Wellness trackers measure basic body metrics and consumer exercise and health information.
c. *Smart Appliances*: More and more home appliances are leveraging IoT technologies and becoming connected to the Internet.

The results of the analysis of publicly available information for these products are shown in Table 6.

Sample Devices	SCMSI Points	SCMSI Rating
Home Security / Home Monitoring		
Kwitset 925 Electronic Lock	555	C

Sample Devices	SCMSI Points	SCMSI Rating
BeHome247 Security Package	635	B
Simple Safe Wireless Security System	465	F
NEST - Automated Thermostat	860	A
Personal Wellness		
Fever Smart Patch Thermometer	560	C
Atlas Wristband	565	C
Body Analyzer	335	F
Smart Wireless Pill Bottles	495	F
Smart Appliances		
Smart iKettle	365	F
Smart Light bulb - GE	490	F
Lefun Baby Monitor	460	F
Belkin Wemo switch	450	F

Table 6: Sample Pilot Data for Tested Devices – Only Public Information

The results overwhelmingly indicate that these devices have no focus on security when simply tested against publicly available information.

4 PILOT WEBSITE FOR CONSUMERS

A pilot website was created as a proof of concept. The website allows consumers to identify the security of their devices in a simple and straightforward way. The website is stored in Azure cloud and is located at https://scmsi.azurewebsites.net.

Step 1: Consumer Visits Website and Selects a Category

The home page describes the basic information about the security compliance measurement system with the three main device categories.

Step 2: Consumer Selects a Device of Interest

The consumer will be presented with a list of available IoT devices. If the device of interest is not available, then the consumer can send the details of the device to request to add the device to the list.

Step 3: Security Rating and Details of Device Displayed to Consumer

Once a device is selected, a dashboard with security details of the device will be displayed to the consumer. The dashboard will have the general information about the product, the SCMSI security rating, details of scores in each category, and a customer feedback section. Figure 2 shows the security details of a sample device.

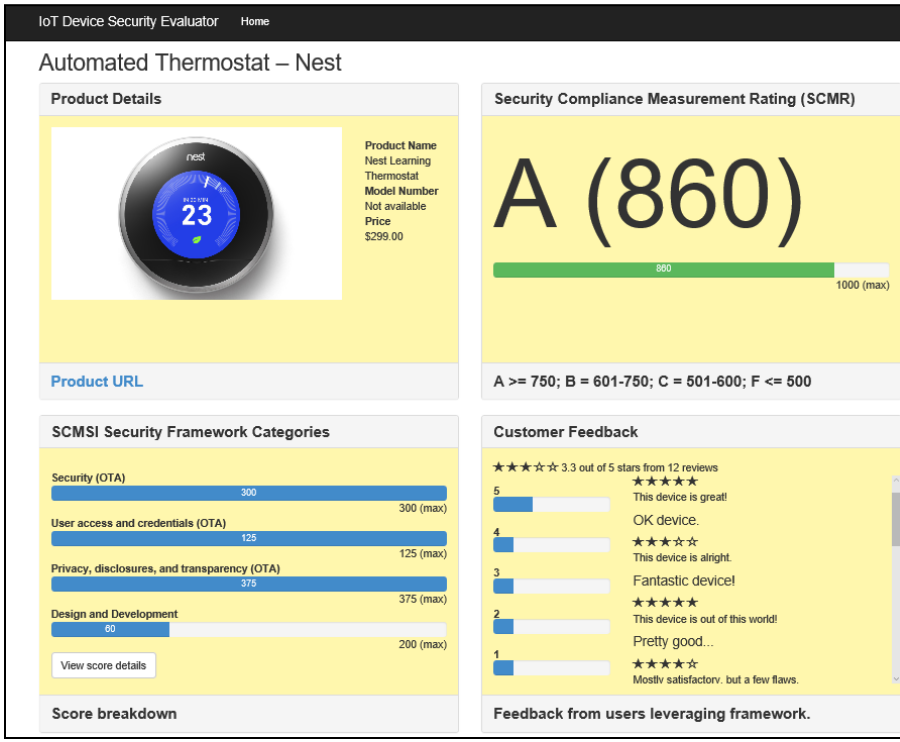

Figure 2: Sample Device Details – Automated Thermostat Nest

Step 4: View Score Details

The consumer can further review the scoring details of each category and the areas where the device failed to comply by selecting the "View Score Details" button. The requirements in pink indicate non-compliance and the requirements in green indicate compliance. Additionally, the consumer can request an email with the full details report.

5 DISCUSSION AND CONCLUSION

The purpose of this paper is to increase consumer awareness of security for IoT devices and to provide consumers a simple process to identify the security of IoT

devices to assist with purchase decisions. This was accomplished by developing a quantifiable security compliance measurement system for IoT devices (SCMSI) leveraging the OTA IoT Trust Framework, a detailed measurement model, and a pilot website was created as a proof of concept where consumers could verify the security of desired devices.

5.1 Problem Definition

The Internet of things is emerging as one of the major trends shaping the development of technologies [14]. The anticipated growth of IoT devices as seen by IDC and others is creating new business opportunities. Security is a critical component for enabling the widespread adoption of IoT technologies and applications.

The primary contribution this paper makes is creating a quantifiable security compliance measurement system. This was accomplished by identifying key security requirements that ensure device security. A quantifiable measurement system was developed to rate the security of the devices. A consumer facing website was created to provide the device's security status to consumers in a simplistic way to raise awareness on security breaches and for manufacturers to be more invested in improving device security.

5.2 Limitations

First, the number of requirements that require company cooperation is cumbersome. It will be very challenging to collect security related information from companies unless there is a direct benefit to the company. Unless companies receive a benefit from participation, it is not likely that they will cooperate.

The second limitation is the lack of standardization and lack of compliance requirements to follow security standards when developing IoT devices.

Third, consumers are still unaware of the security space. Enticing them to go and use a website to find out information about security will be challenging.

5.3 Future Opportunities

There are three future research or expansion opportunities that will address some of the problems that are identified above. First, we could partner with the OTA to set up a certification service for manufacturers at a fixed fee per device subscription rate. Second, we could invest in testing the top 1,000 most popular consumer IoT devices, provide a comparison of the ratings against competitors' devices, and expose the security status to consumers. Growing popularity among consumers could drive manufacturers to proactively request device certification (at a fixed fee). Third, we could work with the Federal Trade Commission (FTC) or agencies to make these security standards mandatory or provide incentives to those manufacturers who follow these standards.

5.4 Conclusion

This is just the beginning of an opportunity to address the security of consumer IoT devices. The suggested SCMSI framework will be further refined as more and more devices are validated. The consumer website presents great potential for a business opportunity as well as creates awareness around the topic of the security of IoT devices. The framework and the model suggested is by no means complete. The work to enhance the model and the website will continue as the IoT space grows.

REFERENCES

[1] "The Internet of Things - Internet of Things Companies." [Online]. Available: http://www.gartner.com/it-glossary/internet-of-things/. [Accessed: 09-Jun-2016].

[2] "Internet of Things Spending Forecast to Reach Nearly $1.3 Trillion in 2019 Led by Widespread Initiatives and Outlays Across Asia/Pacific - prUS40782915," IDC, 10-Dec-2015. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS40782915. [Accessed: 09-Jun-2016].

[3] T. Danova, "75 Billion Devices Will Be Connected To The Internet By 2020 - Business Insider," 10-Oct-2013. [Online]. Available: http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10. [Accessed: 08-Jun-2016].

[4] T. Marcus, K. Monika, X. Suya, and K. Bob, "Worldwide Internet of Things 2016–2019 Forecast: Market Opportunity by Region and Narrowing the Lens on Use Cases," *IDC*, US, Market Analysis US41056415.

[5] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. Moreno, "A decentralized approach for security and privacy challenges in the internet of things," in *Internet of Things (WF-IoT), 2014 IEEE World Forum* on, 2014, pp. 67–72.

[6] C. Speizle, "IoT Trust Framework - Security, Privacy & Sustainability," *OTA Trust Alliance*, 02-Jun-2016. [Online]. Available: https://otalliance.org/initiatives/internet-things.

[7] "OWASP Top 10 for IoT Explained," *OWASP Top 10 for IoT Explained*, 08-Jul-2015. [Online]. Available: https://www.checkmarx.com/white_papers/owasp-top-10-for-iot-explained/.

[8] "NIST CPS public working group- CPS PWG Cyber-Physical Systems (CPS) Framework Release 1.0," *NIST CPS Public Working Group*. [Online]. Available: https://pages.nist.gov/cpspwg/.

[9] R. H. Weber, "Internet of Things–New security and privacy challenges," *Comput. Law Secur.* Rev., vol. 26, no. 1, pp. 23–30, 2010.

[10] J. B. Bernabe, J. L. Hernández, M. V. Moreno, and A. F. S. Gomez, "Privacy-preserving security framework for a social-aware internet of things," in *Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services*, Springer, 2014, pp. 408–415.