Beyond the Convenience of the Internet of Things: Security and Privacy Concerns

Sophia MOGANEDI[1], Jabu MTSWENI[2]
[1]*CSIR, Meiring Naude Road Brummeria, Pretoria, 0001, South Africa*
Tel: +27 012 841 2361, Email: SMoganedi@csir.co.za
[2]*CSIR, Meiring Naude Road Brummeria, Pretoria, 0001, South Africa*
Tel: +27 012 841 4319, Email: JMtsweni@csir.co.za

Abstract: The significant growth of the Internet of Things (IoT) is revolutionizing the way people live by transforming everyday Internet-enabled objects into an interconnected ecosystem of digital and personal information accessible anytime and anywhere. As more objects become Internet-enabled, the security and privacy of the personal information generated, processed and stored by IoT devices become complex and challenging to manage. This paper details the current security and privacy challenges presented by the increasing use of the IoT. Furthermore, investigate and analyze the limitations of the existing solutions with regard to addressing security and privacy challenges in IoT and propose a possible solution to address these challenges. The results of this proposed solution could be implemented during the IoT design, building, testing and deployment phases in the real-life environments to minimize the security and privacy challenges associated with IoT.

Keywords: Internet of Things, Personal Privacy, Security, Interconnected Devices, Vulnerabilities.

1. Introduction

Internet of Things (IoT) refers to the networked interconnection of everyday objects, which are often equipped with ubiquitous intelligence [1]. The concept of IoT has been evolving for many years [2][3][4]. The IoT context consists of more Internet-enabled devices and services that can interconnect to exchange data and useful information [5]. The existence of IoT connects the whole world into one massive information exchange chain where smart objects connect to the Internet and communicate with each other with minimum user involvement [6][7]. The IoT domain includes the overall infrastructure (hardware, software, and services) supporting the networking and communication of Internet-enabled objects that are active participants in processing digital information, exchanging of data including personal identities, physical properties and information sensed from surrounding environments [8]. All these things can be connected by networking and communication technologies [9].

Technologies such as Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID), cloud services, and machine to machine interfaces (M2M) serve as a building block to this new IoT paradigm [2]. The combination of these technologies remove the restrictions on the cyber space and the human space by integrating the best of both worlds to bring forth the IoT space [6].

With the growing presence of WiFi and 4G-LTE wireless internet access, the evolution towards ubiquitous information and communication networks is already evident [10]. Most importantly, data is accessible anywhere and anytime and the physical space can be controlled from a distance because of the physical objects connected to the Internet [11]. “Anytime, anywhere, any media” has been the communication goal for the IoT [12].

According to [13], the IoT continues to push forward an environment where embedded sensors and actuators are self-configured and can be controlled remotely through the Internet. This is achieved through the formation of a smart environment and self-conscious devices: smart transport, smart items, smart cities, and smart health, smart living and so on [5][14][15]. Apart from the convenience and benefits brought by the IoT services, there are security and privacy concerns at different layers from the hardware, software, and networks [5]. This paper details the security and privacy challenges in the IoT domain. Then, investigate to analyze existing solutions that attempt to address the discovered challenges. Lastly, proposes an appropriate solution that addresses the limitations in the existing solutions.

The remainder of this paper is organized as follows: Section 2 presents the research approach that was employed for this study. Section 3 discusses the related work with regards to existing IoT solutions and highlight their limitations.Section 4 presents the security challenges in the Internet of Things. Section 5 presents personal privacy concerns presented by Internet of Things. Section 6 highlights the components that should be taken into consideration in order to address the security and personal privacy challenges in the Internet of Things domain. Section 7 proposes a security model that could be employed for designing, building, testing, and deploying IoT in real-life environments.

2. Research Approach

This study employed a systematic literature review in order to investigate the limitations of existing solutions that aim to address security and privacy challenges in the IoT domain. A systematic literature review is, therefore, a piece of research in its own right and, by its nature, is able to address much broader questions than a single empirical study [16]. The systematic literature review was employed by a search for IoT research papers that addresses the security and privacy in the IoT domain using security and privacy as search criteria. The aim of using this type of research approach was to identify any gaps in previous studies and its relevance to the current study [17].

This approach was in line with answering the questions of security and privacy concerns in the IoT solutions. The literature review findings formed the basis of this study in a sense that the limitations in the existing solutions are addressed by the proposed solution.

3. Related Work

The objective of this section is to briefly highlight research studies published with regard to addressing the security and privacy challenges in the IoT domain. Limitations of the previous studies that attempted to address these challenges are the basis of this study with regards to privacy and security in the IoT domain.

Research related solutions proposed by [18]–[20] focus on the basic security functions that could be possible countermeasures for software attacks on IoT. However, these solutions did not consider major security attacks from hardware to software level. In [21], the IoT embedded security framework is proposed that promotes the embedding of security throughout the software development life cycle while having three basic considerations namely; environment factor, security objective, and functional security requirements. This framework focuses only on the software development cycle. However, limitations are presented with regards to IoT device performance and security. Therefore, quality of the performance and security are found to be based on the cost factor. This means that enhancement on performance or strengthening of security could cost more, whilst improved performance could also lead to low security and vice verse.

The study done in [22] proposed a fuzzy logic approach to determine the IoT security level and decide on the access control mechanisms in various stages of the system model. This approach only attempts to address security at the cloud level by determining the security level of the local cloud without the assistance of third-party management. This proposed fuzzy logic did not consider security from the device perspective where the data is originally collected.

The systematic approach for IoT security proposed in [23] explores the role of each actor and its interaction with main actors of the scheme. The main focus of this approach for security is on the interaction of the actors which are enumerated as classical nodes namely person, process and technological ecosystem. The security limitation of this approach is that the node person is taken as a vital element in the IoT security, not considering that IoT allows many activities to be tracked, monitored, and connected, and a lot of personal and private information can be collected automatically [9]. The person node only applies security practices when interacting with the device. The technological ecosystem refers to technological choices that are made relating to elements which include system architecture, communication protocols, access control method, etc. However, is it not mentioned on how this choice improves on security in the IoT domain.

The related work discussed above focus on limited security aspects within the IoT domain. The output from this investigation illustrates security and privacy limitations within the Internet of Things. The Internet of Things domain can be attacked in numerous ways, from hardware to software. The research presented in this paper looks to improve on the existing solutions by proposing a generic security model that could address security and privacy challenges from the hardware to software perspective in the IoT domain traversing the whole Open Systems Interconnection (OSI) model layers.

4. Security Issues in IoT

There are five common information security requirements that are pertinent in all information systems: data confidentiality, integrity, authenticity, non-repudiation and access control, and these security requirements also apply to the IoT domain [13][24]. The Internet is composed of different components, such as sensing devices, networking components, and data storage devices. These can undergo different types of attacks launched on any component with the potential to reduce the reliability or trustworthiness of the devices [25].

Recent research studies report that a myriad of vulnerabilities exist in numerous IoT devices [7][26][27]. Due to the recent attacks on IoT systems, exploited vulnerabilities demonstrate the need for a comprehensive security architecture that protects the systems and the data from end to end [28]. The study that was done by [29] presents three possible reasons for these vulnerability and security weakness as follows:

- The IoT extends the ‘Internet’ through the traditional Internet, mobile networks, and sensor networks.
- Everything is connected to the Internet.
- These ‘things’ communicate with each other.

As stated by [30] "Without a strong security foundation, attacks, and malfunctions in the IoT devices will overweigh the benefits of using these devices". This is because security and privacy in the current IoT devices are applied as add-on feature instead of being made a priority and considered from the beginning of design and integrated into the Internet of Things [31]. These devices make a lot of communication with each other and the transmission of data becomes vulnerable to the network security challenges. This is because at a network security level there are several common types of attacks that can exploit the data during transmission [32]. As stated by [29], distributed denial of service (DDoS) is a common attack method in the network and it is particularly severe in IoT. During DDoS,

the network gets flooded with a counterfeit request which leads to congestion in the network [33]. This kind of attack gains more attention because of the potential damage by causing the energy dissipation of the devices [34].

5. Privacy Concerns

The concept of privacy is a very broad and diverse notion for which literature offers a variety of explanations and perspectives [35][36]. This section focuses specifically on personal privacy in the IoT context. Privacy is recognized as a fundamental human right, preserved in the 1948 United Nations Universal Declaration of Human Rights and the European Convention on Human Rights [37] and also anchored in the constitutional law in most countries today [36]. The purpose of the United Nations Universal Declaration of Human Rights legislation is to allow consumers an unlimited access, right to control and have responsibility for, the delineation of, and the right to enforce boundaries over their personal data [11][35][36].

The production of the IoT expands the end devices in the network and these devices introduced the human life into the Internet bringing more convenience. However, much of the consumer's information is collected, stored, processed and transmitted [38]. One of the most important outcomes of this emerging field is the creation of an unprecedented amount of data where data storage, ownership, and expiry of data becomes crucial issues [10]. This data could be leaked at any time and used by unauthorized consumers if the security of personal privacy is not ensured [39]. Therefore, it becomes a matter of importance to know which type personal information needs to be protected in order to preserve personal privacy [37], because concerns over privacy spread wide, particularly as wireless devices can track user's actions, behaviors, health status, location, and ongoing preferences [40]. When this information is not protected, this could put a dent in the users' desire to buy these devices and explore the IoT devices' full potential [41].

6. Considerations of IoT Security and Privacy

The objective of this section is to highlight components that need to be considered when addressing security and privacy challenges in the Internet of Things domain. These components look into the high-level operation of an IoT device. To better illustrate some of these components with regards to IoT, the purpose of each component is addressed in order to demonstrate its high-level importance in the IoT domain.

6.1. Data collection

With people having smart devices everywhere and sharing their life on social networks, an increasing penetration of people's private and public lives has been witnessed by the technology that enables data collection and with its identification, tracking, and profiling [36]. IoT devices sense the physical environment, collect real-time physical data and reconstruct a general perception of it [42]. The data in IoT are always mass, distributed, and time-related and position related [3],[43]. At the same time, the data sources of the IoT are heterogeneous [43]. There is a vast amount of real-time data collected by the IoT devices. This generated, processed and exchanged data carries a vast amount of security, safety-critical as well as privacy-sensitive data [44].

6.2. Data storage

The IoT data are collected from various data sources in different structures and formats [45]. IoT enables the collected data to be stored both in physical devices and cloud storage [46]. The cloud storage is convenient for the users because the maintenance of the cloud infrastructure is not their responsibility. Cloud storage provides a better utilization of

resources using virtualization techniques and reduces the storage load of the device [47]. However, the cloud has a lot of shared storage and if data is not segmented accordingly; then a user with hacking intentions could access other users' data.

6.3. Data communication

The IoT devices have the ability to communicate a lot of data with other objects (anywhere and anytime) [48]. However, it is expensive to transmit a vast amount of raw data in the complex heterogeneous networks, so IoT needs a compression and data fusion techniques to reduce the data volume [49]. The collected data are transmitted through the wireless networks whereby the signals are exposed in the public place and if there is a lack of protection measures, the signals could be monitored, intercepted and disrupted easily [32].

Due to a large amount of data transmitted, security issues such as DoS/DDoS attacks, forgery or man-in-the-middle attacks, and heterogeneous network attacks and others also affect the transport security in the IoT domain during communication [39].

7. Proposed IoT Security Model

The objective of this section is to present and discuss the proposed IoT security model illustrating how this model could achieve the highlighted limitations of the existing solutions discussed in Section 3.

Each IoT device is manufactured for a unique purpose within the cyber space domain. However, these devices are the same in a sense that they collect a vast amount of data, process it and save it and in some cases share it with other IoT devices or systems as discussed in the previous section (cf. Section 6). The main technological challenges while implementing IoT is that all kinds of devices should be widely accepted thus providing interoperability between them [33]. In addition, [32] states that IoT security features should have three characteristics:

- **Comprehensive perception:** objects using Radio-Frequency Identification (RFID), sensors and two-dimensional barcode to obtain information anywhere at any time.
- **Reliable transmission:** the ability of the IoT platforms to safely transmit information of objects through the wireless or wired networks to the data center on a real-time basis.
- **Intelligent processing:** the ability of the IoT platforms to analyze the obtained information before submitting to the application.

IoT should, therefore, convey security characteristics that will fulfill the basic security requirements during real-time data transmission.

Figure 1 below presents how security and privacy should be considered in order to protect the devices and personal privacy of users.

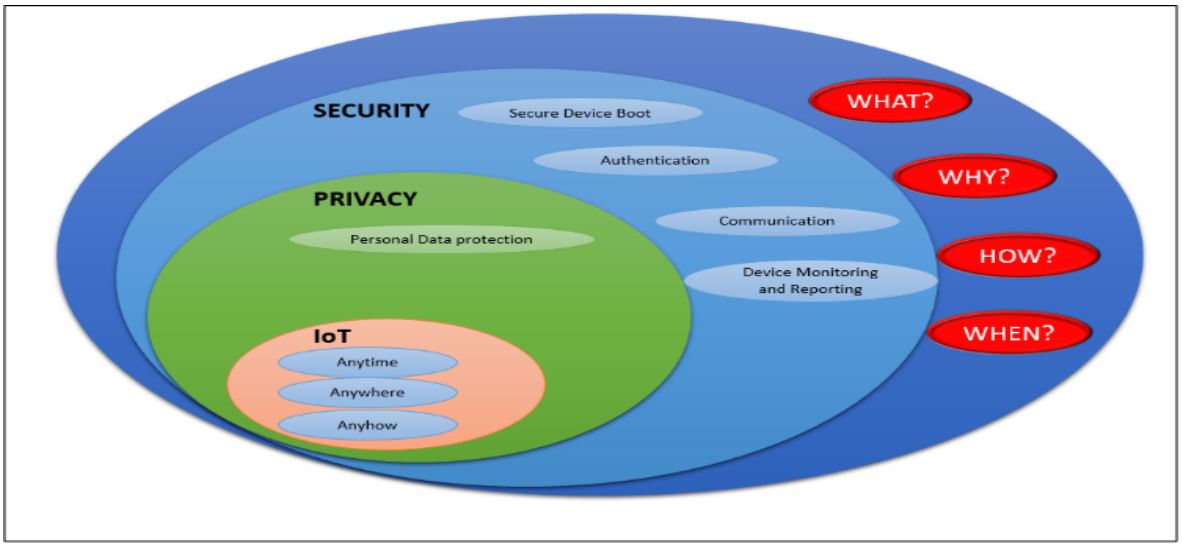

Figure 1. Proposed IoT Security Model

The proposed IoT security model aims to identify the following components with regard to employing security and privacy in the IoT domain:

- What – this component identifies what needs to be secured and protected.
- Why – identifies the reason for securing the IoT devices and preserving the personal privacy.
- How – identifies mechanisms and methods that can be used to secure the IoT devices and preserve the personal privacy.
- When – this last component identifies the stages of security and privacy consideration and implementation.

The following aspects are addressed by the proposed Security Model:

a. **Device Protection**: Only trusted and authentic programming code or logic should be executed on the device. This can be achieved by following software development best practices in order to deploy trusted and authentic code. The devices should have the ability to be remotely managed in order to enhance on the remote vulnerability remediation.

b. **Device Boot**: Devices which require being configured should enforce booting for the very first time and prompt the user to change the default security settings. IoT should also provide an auto-update mechanism for device's firmware and/or software to counter any recently discovered vulnerabilities at the hardware level.

c. **Authentication**: These IoT devices will be communicating with other devices. Therefore, authentication is vital to ensure that the device in use is only communicating with known and trusted devices. Authentication process should be established every time the devices is making a connection to other devices.

d. **Communication**: Interconnected devices should provide a trustworthy communication. IoT allows simultaneous connection of the devices and the communication causes an increase in data traffic. Confidentiality and integrity of the data during communication should be established and maintained. This means authentication and data encryption should be integrated for secure communication purposes.

Furthermore, the use of Public Key Infrastructure (PKI) in IoT plays a vital role as it supports and sustains trust in the IoT ecosystem. Considering an integration of PKI into IoT will have a great impact on the ecosystem as it meets the security principle of ensuring authentication for devices that will be communicating. PKI solutions provide

an encryption mechanism that can be used to secure data during communication. Secured and encrypted data could enhance the ecosystem trust and data integrity.

e. **Device Monitoring and Reporting**: Each device runs numerous applications that collect data about the device and the user. A privacy policy should be available to the users disclosing the type of data that is collected by the device and how it is processed and, where and how the data is stored before the user can use the device. This will also create a security awareness for the user prior to using the device.
f. **Personal Data Protection**: A lot of personal data in collected by the IoT devices and in some instances the user is not even aware of this. Personal data should be protected during data transmission and in storage by encrypting the data using generally accepted security standards with regard to encryption.
g. **Data Transmission Security**: This requires the network layer for data transmission to be secured from attacks such as DDoS, eavesdropping and other external interference or monitoring. Employing two-layer encryption mechanism to encrypt data on the device level with the Base Encryption Layer (BEL) before transmitting the data to the cloud storage, and performing the second encryption at the cloud storage level with a Surface Encryption Layer (SEL).

Table 1 below presents the comparative analysis illustrating the limitations of the existing solutions as discussed in Section 3 and the improvement of the proposed solution with regard to addressing the security and privacy challenges in the IoT domain.

The symbol **'x'** indicates that the solution does not address the security and privacy challenges in that component and specific letters (e.g. "a") refers to the aspects/components that the related solutions also consider as discussed above.

Table 1. Security and Privacy components addressed.

Related Solution & Proposed Solution	**Hardware security**	**Software Security**	**Data security (Encryption of data)**	**Cloud /Storage Security**	**Network Security**
IoT Security Model	a, b	a,b,e	c, d, e, f,g	d, f, g	g
[18]- Embedded security: New trends in personal recognition systems	x	a	c	x	x
[19]- A compiler-hardware approach to software protection for embedded systems	a	a	d, g	x	x
[20]- A data-driven approach for embedded security	x	x	d, g	x	x
[21]- Proposed embedded security framework for Internet of Things (IoT)	a	a	d	c	x
[22]- Security and trust in IoT/M2M – Cloud based platform	x	x	x	c,f	g
[23]- A systemic approach for IoT security	b	a	x	x	x

The proposed IoT Security Model is an improvement of the existing solutions because it addresses important aspects in the IoT domain. Firstly, it addresses hardware security

challenges by protecting the physical device from attacks by allowing only trusted applications or programming code to run on the device. Secondly, it advises for device reboot to be enforced to ensure that bootable devices do not use default credentials that can be used by hackers to gain access. Thirdly, implementation of encryption mechanisms will enable the protection of data that are collected, processed, stored and transmitted by the IoT devices.

8. Conclusion and Future Work

The Internet of Things promises a convenient communication at anytime, anywhere and unlimited access to information. The IoT have gained a lot of attention because of their affordability, capability, and convenience offered. This IoT ecosystem is evolving very fast and the cybersecurity attacks are advancing as well. The lack of security and privacy on the Internet of Thing raises concerns and questions the benefit of the IoT devices and services.

Firstly, this paper highlighted the security and privacy challenges within the IoT domain. Furthermore, investigated existing solutions that attempted to address the security and privacy challenges within the IoT domain. The security and privacy limitations presented by these solutions were noted. IoT Security Model was proposed to address the limitations presented by the existing solutions with regard to security and privacy. This model can be implemented in the IoT platforms designed, built, tested and deployed in the real-life environment to reduce the security and privacy challenges. Lastly, a comparative analysis was presented to illustrate the improvements of the proposed solution.

Future work pertaining to this research will focus on the implementation of the proposed solution in existing IoT platform deployed in the real-life environment. Limitation of this solution from a theoretical perspective is that implementation of a strong security will downgrade the performance of the IoT device, considering the physical features such as device memory, storage size, battery life and others.

References

[1] F. Xia, L. T. Yang, L. Wang, and A. Vinel, "Internet of Things," pp. 1101–1102, 2012.

[2] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[3] J. A. Stankovic, "Research Directions for the Internet of Things," *Internet Things Journal, IEEE*, vol. 1, no. 1, pp. 3–9, 2014.

[4] A. D. Miyazaki and A. Fernandez, "Consumer Perceptions of Privacy and Security Risks for Online Shopping," *J. Consum. Aff.*, vol. 35, no. 1, pp. 27–44, 2001.

[5] G. M. Abomhara, Mohamed and Koien, "Security and Privacy in the Internet of Things : Current Status and Open Issues," *Priv. Secur. Mob. Syst. (PRISMS), 2014 Int. Conf.*, pp. 1–8, 2014.

[6] P. Madhura, N. Bilurkar, P. Jain, and J. Ranjith, "A survey on Internet of Things: security and privacy issues," *Ijitr*, vol. 90, no. 11, p. 8887, 2015.

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

[8] B. Khoo, "RFID As an enabler of the internet of things: Issues of security and privacy," *Proc. - 2011 IEEE Int. Conf. Internet Things Cyber, Phys. Soc. Comput. iThings/CPSCom 2011*, pp. 709–712, 2011.

[9] L. Da Xu, S. Member, W. He, and S. Li, "Internet of Things in Industries : A Survey," vol. 10, no. 4, pp. 2233–2243, 2014.

[10] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision , architectural elements , and future directions," *Futur. Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[11] J. Veijalainen, D. Kozlov, and Y. Ali, "Security and Privacy Threats in IoT Architectures," *Proc. 7th Int. Conf. Body Area Networks*, no. International Conference on Body Area Networks, pp. 256–262, 2012.

[12] L. Zhou and H.-C. Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Netw.*, vol. 25, no. 3, pp. 35–40, 2011.

[13] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: An internet of things

application," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 68–75, 2011.
[14] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.
[15] A. Mohammed, I. Alkuhlani, and S. B. Thorat, "Internet of Things (IOT) Standards , Protocols and Security Issues," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, no. 11, pp. 491–495, 2015.
[16] R. E. Baumeister and M. R. Leary, "Writing Narrative Literature Reviews," vol. 1, no. 3, pp. 311–320, 1997.
[17] J. E. Wallace, "How to write a literature review," 2013.
[18] M. Fons, F. Fons, and E. Cantó, "Embedded security: New trends in personal recognition systems," *Proc. 2007 Ph.D Res. Microelectron. Electron. Conf. PRIME 2007*, pp. 89–92, 2007.
[19] O. Gelbart, E. Leontie, B. Narahari, and R. Simha, "A compiler-hardware approach to software protection for embedded systems," *Comput. Electr. Eng.*, vol. 35, no. 2, pp. 315–328, 2009.
[20] H. Saputra, O. Ozturk, N. Vijaykrishnan, M. Kandemir, and R. Brooks, "A data-driven approach for embedded security," *Proc. - IEEE Comput. Soc. Annu. Symp. VLSI - New Front. VLSI*, pp. 104–109, 2005.
[21] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for Internet of Things (IoT)," *2011 2nd Int. Conf. Wirel. Commun. Veh. Technol. Inf. Theory Aerosp. Electron. Syst. Technol. Wirel. VITAE 2011*, pp. 1–5, 2011.
[22] R. Stefanov, "Security and trust in IoT/M2M – Cloud based platform." .
[23] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, "A systemic approach for IoT security," pp. 351–355, 2013.
[24] H. Abie and B. Ilangko, "Risk-Based Adaptive Security for Smart IoT in eHealth," no. SeTTIT, pp. 269–275, 2012.
[25] R. Uttarkar and P. R. Kulkarni, "Internet of Things : Architecture and Security," vol. 3, no. 4, pp. 12–19, 2014.
[26] A. Cui and S. J. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan," in *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2010, pp. 97–106.
[27] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, 2015.
[28] E. Borgia, D. G. Gomes, B. Lagesse, R. Lea, and D. Puccinelli, "Special issue on 'internet of Things: Research challenges and Solutions,'" *Comput. Commun.*, vol. 89–90, pp. 1–4, 2016.
[29] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," *Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012*, vol. 3, pp. 648–651, 2012.
[30] and J. L. Rodrigo Roman, Pablo Najera, "The Internet of Things The Internet of Things," no. September, p. 6, 2011.
[31] L. Tan and N. Wang, "Future Internet: The Internet of Things," vol. 5, pp. 376–380, 2010.
[32] K. Zhao and L. Ge, "A survey on the internet of things security," *Proc. - 9th Int. Conf. Comput. Intell. Secur. CIS 2013*, pp. 663–667, 2013.
[33] S. Misra, "A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things," 2011.
[34] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. De Santanna, "Internet of Things in healthcare: Interoperatibility and security issues," *IEEE Int. Conf. Commun.*, pp. 6121–6125, 2012.
[35] K. Renaud and D. Gálvez-Cruz, "Privacy: Aspects, definitions and a multi-faceted privacy preservation approach," *Proc. 2010 Inf. Secur. South Africa Conf. ISSA 2010*, 2010.
[36] K. W. JH Ziegeldorf, OG Morchon, "Privacy in the Internet of Things: threats and challenges," *Int. J. Appl. Eng. Res.*, vol. 9, no. 22, pp. 5968–5974, 2014.
[37] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services 2 . Why is it important to take privacy into," pp. 44–52, 2009.
[38] C. Hu, J. Zhang, and Q. Wen, "An identity-based personal location system with protected privacy in IOT," *Proc. - 2011 4th IEEE Int. Conf. Broadband Netw. Multimed. Technol. IC-BNMT 2011*, pp. 192–195, 2011.
[39] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wirel. Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.
[40] J. Virkki and L. Chen, "Personal Perspectives: Individual Privacy in the IOT," *Adv. Internet Things*, vol. 3, no. 2, pp. 21–26, 2013.
[41] A. Meola, "How the Internet of Things will affect security & privacy," *Business Insider*. [Online]. Available: http://www.businessinsider.com/internet-of-things-security-privacy-2016-8. [Accessed: 01-Mar-2017].
[42] E. Borgia, "The Internet of Things vision : Key features , applications and open issues," *Comput.*

Commun., vol. 54, pp. 1–31, 2014.
[43] S. Bin, L. Yuan, and W. Xiaoyi, “Research on Data Mining Models for the Internet of Things,” 2010.
[44] S. Ahmad-Reza, W. Christian, and W. Michael, “Security and Privacy Challenges in Industrial Internet of Things Invited,” 2015.
[45] L. Jiang, S. Member, H. Cai, Z. Jiang, F. Bu, and B. Xu, “An IoT-Oriented Data Storage Framework in Cloud Computing Platform,” vol. 10, no. 2, pp. 1443–1451, 2014.
[46] M. Hossain, M. Fotouhi, and R. Hasan, “Towards an Analysis of Security Issues , Challenges , and Open Problems in the Internet of Things,” 2015.
[47] S. Subashini and V. Kavitha, “Journal of Network and Computer Applications A survey on security issues in service delivery models of cloud computing,” *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.
[48] A. Dohr, M. Drobics, D. Hayn, and G. Schreier, “The Internet of Things for Ambient Assisted Living,” pp. 804–809, 2010.
[49] Q. Jing, A. V Vasilakos, and J. Wan, “Security of the Internet of Things : perspectives and challenges,” pp. 2481–2501, 2014.