Security in Internet of Things: Issues, Challenges, and Solutions

Chapter · July 2019

DOI: 10.1007/978-3-319-99007-1_38

3 authors:

Hanan Aldowah
Universiti Sains Malaysia
29 PUBLICATIONS **796** CITATIONS
SEE PROFILE

Shafiq Ul Rehman
University of Petroleum & Energy Studies
35 PUBLICATIONS **501** CITATIONS
SEE PROFILE

Irfan Umar
Universiti Sains Malaysia
85 PUBLICATIONS **1,020** CITATIONS
SEE PROFILE

Security in Internet of Things: Issues, Challenges and Solutions

Hanan Aldowah[1(✉)], Shafiq Ul Rehman[2], and Irfan Umar[1]

[1] Universiti Sains Malaysia (USM), Penang, Malaysia
hanan_aldwoah@yahoo.com, irfan@usm.my
[2] Singapore University of Technology and Design (SUTD), Tampines, Singapore
shafiq_rehman@sutd.edu.sg

Abstract. In the recent past, Internet of Things (IoT) has been a focus of research. With the great potential of IoT, there comes many types of issues and challenges. Security is one of the main issues for IoT technologies, applications, and platforms. In order to cover this key aspect of IoT, this paper reviews the research progress of IoT, and found that several security issues and challenges need to be considered and briefly outlines them. Efficient and functional security for IoT is required to ensure data anonymity, confidentiality, integrity, authentication, access control, and ability to identify, as well as heterogeneity, scalability, and availability must be taken into the consideration. Considering these facts, by reviewing some of the latest researches in the IoT domain, new IoT solutions from technical, academic, and industry sides are provided and discussed. Based on the findings of this study, desirable IoT solutions need to be designed and deployed, which can guarantee: anonymity, confidentiality, and integrity in heterogeneous environments.

Keywords: Internet of Things · Security threats · Challenges Solutions

1 Introduction

Internet of Things (IoT) is the emerging technology and it is considered to be the future of Internet [1, 2]. By allowing the devices/things self-configuring capabilities based on standard and interoperable communication protocols to identities, and use intelligent interfaces, over the dynamic global network infrastructure [1, 2]. The concept of IoT can be considered as an extension of the existing interaction between the humans and applications communicating through a new dimension [3]. Due to the advancements in mobile communication, Radio Frequency Identification (RFID) innovation, and Wireless Sensor Networks (WSNs), things and mechanisms in IoT can communicate with each other regardless of time, place or form [4]. The major breakthrough of IoT is in the formation of smart environments: smart homes, smart transport, smart items, smart cities, smart health, smart living, and etc. [5, 6]. Furthermore, in business perspective, IoT has enormous potential for various types of organizations and companies, including IoT applications and service providers, IoT platform providers and

F. Saeed et al. (Eds.): IRICT 2018, AISC 843, pp. 396–405, 2019.
https://doi.org/10.1007/978-3-319-99007-1_38

integrators, telecom operators and software vendors [2, 3]. Moreover, IoT will have a major impact in learning experience; especially in higher education system [7].

With the rapid increase in IoT application use, several security issues have raised sharply. As devices and things are becoming part of Internet infrastructure, therefore these issues need to be considered. When almost everything will be connected on Internet, these issues will become more prominent; with continuous Internet global exposure will literally disclose more security vulnerabilities. Such security flaws will be subsequently exploited by hackers, and later can be misused in uncontrolled environments with billions of IoT devices [2]. In addition, the IoT will also increase the potential attack surfaces for hackers and other cyber criminals.

A study conducted by Hewlett Packard [8] revealed that 70% of the most commonly used IoT devices contain serious vulnerabilities. IoT devices are vulnerable to security threats due to their design by lacking certain security features such as insecure communication medium, insufficient authentication and authorization configurations. As a matter of fact, when IoT become everywhere, everyone whether individuals or companies will be concerned. Additionally, crosslinking of objects presents new potentials to influence and to exchange. This leads to a variety of new potential risks concerning information security and data protection, which should be considered. Further, lack of security will create resistance to adoption of the IoT by companies and individuals.

Security issues and challenges can be addressed by providing proper training to the designers and developers to integrate security solutions into IoT products and thus, encouraging the users to utilize IoT security features that are built into the devices [2]. Our motivation to conduct this study is that most of the previous studies had focused on academic solutions only and had ignored other type of solutions from technical and industrial sides. However, these three sectors should work cooperatively and synchronously in order to reach integrated solutions as well as all the considerations from the three aspects should be taken into an account. Therefore, this paper provides a review on the main issues of IoT in terms of security as well as addresses some considerations that must be taken into account before and during the design stages to fill the gap of the literature regarding this issue by providing some solutions from three aspects including technical, academic, and industrial solutions. The main contribution of this paper is to provide the necessary insights on how certain utilization of such technologies can be facilitated by certain mechanisms and algorithms. This is believed to guide future studies to the use of certain solutions for certain problem based on the suggested algorithms and mechanisms by academic researchers with attention to technical and industrial solutions too.

The structure of the paper is organized as follows: the main issues and challenges related to IoT technology and its considerations are discussed in Sect. 2. The solutions proposed by academic researchers, technician, and industry experts are described in Sect. 3 whereas the discussion of the review findings is provided in Sect. 4. And finally, the conclusion, recommendations, and future work are outlined in Sect. 5.

2 Security Issues, Challenges and Considerations

IoT started to gain new momentum in current years as the consequence of the rapid growth of internet connected devices. However, security remains one of the major issues of the IoT [9] and the foremost concern raised by different stakeholders in Internet of Things which has the potential to slow down its adoption [10]. Therefore, it is considered one of the major issue which needs to be addressed to promote the IoT in real world [11]. Security is a fundamental quality of an IoT system and it is related to specific security features which are oftentimes a basic prerequisite for enabling Trust and Privacy qualities in a system [9]. IoT Security is the area to focus on securing the connected devices, protecting data, and networks in the Internet of things [12]. The computing devices and embedded sensors used in machine-to-machine (M2M) communication, smart home systems and in wearable devices are the main driving forces of IoT [13].

Weak security and poor security behaviors need to be considered from the outset and resilience designed in, in both individual devices and whole systems. Billions of additional connected devices in new locations and applications mean that the IoT world has increased the complexity of systems [14]. As the number of connected IoT devices continually increase, security issues are exponentially multiplied and there are many security concerns need to be considered as an entire system [15]. Moreover, traditional security mechanisms cannot be directly implemented to IoT technologies due to their designed system i.e. limited power as well as these large number of connected devices raise heterogeneity and scalability issues [9]. The security and safety of such systems can be endangered by a wide range of risks, both predictable and unpredictable, and therefore system elasticity should be a strong consideration.

Heterogeneity is one of the most critical issue, alongside with the security mechanisms that should be integrated into the IoT and has a considerable impact over the network security services that have to be implemented in the IoT [11]. Constrained devices will interact with various heterogeneous devices either directly or through gateways [16, 17]. Heterogeneity needs security to overcome the impossibility of implementing effective algorithms and protocols on all the devices in the IoT application fields [9]. In this case, it is essential to implement effective cryptographic algorithms that can provide a high throughput and adapt lightweight security protocols that offer an end-to-end secure communication channel. These protocols require credentials, thus optimal key management systems must be implemented to distribute these credentials and to help in establishing the necessary session keys between peers [11].

Addressing scalability for a large scale IoT deployment is another key issue. A significant challenge is to provide reliable solutions, which are scalable for the billions of things linked to many different local or global networks [9, 18]. Additionally, lots of them are mobile objects and finding the location of and verifying the correct identity of a specific item will be a major problem for the IoT infrastructure [9, 19]. Therefore, the development of applicable techniques that support heterogeneity and scalability, to anonymize users' data are key issues [20]. Moreover, providing

flexible subscription schemas and events management while ensuring scalability with respect to things and users is still considered an open issue.

Security threats are problematical issue for the IoT deployment as the minimum capacity of devices being used, as a matter of fact, physical accessibility to sensors, devices, and the openness of the systems, considering the devices/things will communicate wirelessly [21]. Security concerns like DoS/DDoS attacks, man-in-the middle attacks, heterogeneous network issue, application risk of IPv6, WLAN application conflicts also hinders the deployment of IoT security [22–24] as well as the application security issues including information access and user authentication, information, platform management and so on [15, 25–27].

According to the research [15], data security issues can be classified into four types as: confidentiality, integrity, authenticity, and data availability. These security issues can be resolved by employing security measures: Data confidentiality ensures data protection from unauthorized users, while data integrity maintains correctness/accuracy of data. Moreover, authenticity makes sure that only authorized entities can access network resources to restrict any invalid users from the networks, and data availability guarantees that there is no restrains of authorized access to network resources, services and applications [28].

Furthermore, a larger number of IoT applications and services are increasingly vulnerable to attacks or data theft. To secure IoT against such attacks, advanced technology is required in several fields. The security of information and network should be equipped with properties such as identification, confidentiality, integrality and availability [29]. More precisely, authentication, confidentiality, and data integrity are the key problems related to IoT security [30]. Authentication is required for building a connection between devices and the exchange of number of public and private keys through the node to prevent steal data. In addition, confidentiality ensures that the data inside an IoT device is concealed from unauthorized objects, while data integrity prevents any modification to data in the middle by safeguarding that the data which arrived at the receiver node is unchanged and remains as transmitted by the source (sender) [2].

3 Securing New IoT Solutions from Technical, Academic, and Industry Sides (Architectures, Approaches, and Mechanisms)

In this section, we discuss some of the solutions proposed by Academic researchers, Technician, and Industry experts as counter measures to IoT security threats as follows:

3.1 Academic Solutions

Academics researchers have proposed some solutions in the field of network security. These solutions came in the form of architecture, new approaches and models, and mechanisms through which they endeavor to raise the quality of security in IoT environment. Some of these proposed solutions are:

One of the security solution proposed by [31] namely Dynamic Prime Number Based Security Verification (DPBSV). This solution is desirable for big data streams; it uses the concept of sharing a common key which is updated periodically by yielding a synchronized pair of prime numbers for real time security verification on big data stream. The study has conducted theoretical analyses and experimental evaluations to show the efficiency of its approach and to prove that DPBSV technique requires less processing time and can prevent malicious attacks on big data streams.

While most of the security challenges are often addressed by centralized approaches, a recent research work carried out by [32] have proposed an entirely distributed security approach for IoT. For the design and implementation of this security mechanism and its application in IoT environments, authors used an optimized Elliptic Curve Cryptography approach. Based on a lightweight and flexible design, this work presents an optimum solution for resource-constrained devices, providing the benefit of a distributed security approach for IoT in terms of end-to-end security. According to authors, this solution has already been tested and validated by using AVISPA tool and had been implemented on a real scenario over the Jennic/NXP JN5148 chipset based on a 32-bit RISC CPU [32]. The results have proved the feasibility of this work. Therefore, DCapBAC can be considered a security solution for IoT environments.

Sicari, Rizzardi [9] emphasized on design and deployment of appropriate solutions, which are platform independent and can provide resilient security measures. Considering the authentication and access control an approach has been proposed by [33], to establish the session key it uses an Elliptic Curve Cryptography (ECC) which is a lightweight encryption algorithm [34]. This technique specifies access control policies, managed by an attribute authority, which ensures to maintain mutual authentication among the user and the sensor nodes. Hence, can resolve the resource restrained issue at application level in IoT.

Particularly, in order to maximize the IoT benefits, it is mandatory to reduce the risks involved with security concerns. For that purpose, [35] proposed a comprehensive architectural design named as (ARMY) which proposed based on the Architectural Reference Model (ARM) to analyze the main security prerequisites during the design of IoT devices. The proposed architecture has been designed and implemented within different European IoT enterprises; to initiate and promote the development of security based IoT-enabled services.

Recently in 2017 researchers [36] proposed a Secure IoT (SIT) based on 64-bit block cipher. The architecture of the designed algorithm is integration of feistel cipher and a substitution-permutation network. Authors claim that SIT is a lightweight encryption algorithm and it can be deployed in IoT applications.

Moreover, emerging techniques such as software defined networking (SDN) and blockchain techniques are being adopted to provide security solution for IoT in heterogonous environments. For instance, In [37] researchers proposed an OpenFlow based SDN architecture for IoT devices. According to the researches the proposed architecture can perform anomaly detection to figure out the compromised devices in a network. To do so, network gateway executes dynamic traffic analysis. In case any abnormal traffic behavior is detected it will take the mitigation measures accordingly. Similarly, researchers in [38] proposed a multi-layered security architecture based on blockchain techniques to share and store the heterogeneous IoT data related to the

smart city environment. The proposed architecture is designed to address the scalability and reliability issues that are very challenging in heterogeneous environments

3.2 Technical Solutions

In order to mitigate ever-expanding security threats to companies, organizations, and governments have to change their perspective towards security. This paradigm shift is the one that addresses security through an essentially broader scope at every level of the interaction. Organizations must emphasize the nature of the challenges, risks, and technological advantages and disadvantages unique to the product or service environments. They must understand the internal skills, existing practices, strategies, governance, and controls related to security, what is lacking, and where the gaps lie. To support this change, Harbor Research [39] has developed a new approach consists of a three-step process to guide and help companies, organizations, and governments in their approach to IoT security. The design of such process is to aid companies in designing and implementing a comprehensive approach to security in IoT solutions, including conducting an impact assessment, considering five primary security functions, and defining lifecycle controls are as follows:

Step 1: Impact of Security Assessment in Heterogeneous Environments
Addressing the impact of security in diverse environments must be the foremost consideration during the solution design process. The proposed solutions should be compatible with various applications and platforms. The foundation of any IoT solution deployment depends on a proper security mechanism. Therefore, before designing and deploying an IoT security solution for heterogeneous environments, proper information of customers' environment, sensitive data, risk assessment, infrastructure etc. related to organizations need to be considered.

Step 2: Application of Primary Security Functions
To ensure a secure IoT deployment across the entire organizational network, the designed IoT security solutions must possess five key functionalities as: data encryption, network security, identification, user access and management, and analytics. By doing so, a secure end-to-end communication between the IoT devices, data centers and cloud architectures can be ensured.

Step 3: Lifecycle Controls
The entire lifecycle of IoT devices in each phase need to be considered as: during the Deployment phase of security solution, IoT devices need to be authenticated by verifying its software via digital signatures, certifications, and other security methods to ensure a secure communication across the network. During Operation phase, IoT devices need to be continuously monitored by the network which is responsible for penetration testing and vulnerability assessment. The network should provide real-time monitoring operation and response during the event of an attack. In Incident and Remediation phase, IoT devices need to be integrated with system-wide incident response policies. And finally, in Retirement and Disposal phase, IoT devices that possess sensitive data, information, certifications etc. must be deleted securely.

In 2014, an online study was conducted by Zebra Technologies on global wide companies, corresponding to various industrial sectors [40]. The study focused on identifying the organizations interested in IoT solutions. The results showed that companies are taking initiatives in deployment of IoT solutions. Moreover, many organizations consult the IoT experts in deployment of IoT solutions and applications. IoT solutions provide new opportunities for companies to transform their strategic, operational, and business activities.

Nevertheless, deploying these IoT solutions are challenging for the companies as IoT solutions relies on various technical elements one of them is deploying end-to-end IoT security solutions. Mostly companies design IoT solutions meant for specific purpose within an organization. Considering IoT as emerging technology, there is a need for interoperability, so that a unified standard is set to enable seamless integration across IoT devices, applications, and services among different vendors.

3.3 Industrial Solutions

Security is critical to IoT and need to be taken care of at every stage [10]. Through the literature review and the recommendations of many workshops and conferences that emphasized on implementing the proper security measures while designing the IoT devices. They came to a consensus that while designing the IoT devices companies should consider three major aspects. First, adopting security by design; second, engaging in data minimization; and third, increasing transparency among the consumers with notice and choice for unexpected services.

Security by Design

Security for IoT devices depends on various elements, such as the amount of sensitive data collection and mitigating costs of security vulnerabilities. Ramirez [41] presented some ideas to address these key issues, as suggested companies should consider follow key points: (1) perform security risk assessment during the design process; (2) test device security measures; (3) consider protection of sensitive data while transmission or storage; and (4) monitor IoT devices and regular software updates. Moreover, to ensure a desirable security measures, organizations must deploy administrative and technical privileges by conducting security training sessions for employees. According to [42], security measures that are considered from initiating a device, establishes a secure computing environment which are tamper resistant. The article affirmed that security for IoT device must be addressed for its entire lifespan process, from design to the operational phases including: (1) Secure booting, (2) Access control, (3) Device authentication, (4) Firewalling and IPS, and (5) Updates and patches.

Data Minimization

Data minimization is the strategy that organizations can use to maintain the data repository within organizations by defining its duration. As security and privacy solution, organizations that gather the personal information should follow this data minimization concept. In other words, organizations should obtain the data required for specific purpose and period only and should safely discard it after. Gathering and maintaining large data repository can induce a risk of data breach.

Notice and Choice
The aim of a privacy notice is to ensure that customers and users are aware of data practicing involves personal information. Moreover, users should be aware about the personal information sharing, gathering, processing, and its retention [43].

4 Discussion

From this study, we found that Internet of Things (IoT) need to be designed in a user-friendly manner yet with consideration of its security measures. We observed that security is one of the main issues and challenges in the deployment of IoT in heterogeneous environments. The concept of IoT is to connect everything to the global Internet and allow the devices and things remotely to communicate with each other, which raises new security problems related to the confidentiality, integrity, and authenticity of data being exchanged between the IoT devices. To restrain the adversaries to obtain sensitive information while allowing authentic users to share and gather this information. We found that further research is needed that can focus on designing security measures in IoT environments. In maintaining the data confidentiality, integrity, and authenticity proper encryption algorithms need to be used, which not only fulfills these security measures yet consumes less data processing time.

In brief, security in the IoT technologies is very important and full of challenges and intuitively usable solutions are needed as well as these solutions should seamlessly integrate into the real world.

5 Conclusion, Recommendations and Further Work

The aim of this study was to provide a review of the most critical aspects of IoT with specific focus on the security issues and challenges involved with IoT devices. Several problems and challenges related to the security of the IoT are still being faced. Research focuses are much needed in this area to address these security issues and challenges in IoT heterogeneous environments so that users can confidently use IoT devices to communicate and share information globally with safety assurance. In addition, this paper recommended some solutions from academic, technical, and industrial aspects. These solutions came in the form of architecture, new approaches and models, and mechanisms through which they aim to increase the quality of security in IoT environment. Furthermore, data security, and data protection must methodically be considered and addressed at the design stage. For this, there are three key aspects that organizations should take into consideration to enhance security in IoT devices: security by design, data minimization, and providing users with notice and choice for unexpected services. There are nevertheless remaining numbers of potential gaps in the overall ‘security’ framework where further research will be potentially beneficial. As conclusion, there are still many open questions and problems that need further thinking and harmonization. The IoT includes a complex set of technological, social, and policy considerations across various set of stakeholders. The technological developments that enables the use of IoT are real, growing, and here to stay. Efforts by governments,

engineering, production, industry, and academic world to provide processes for the effective and safe use of these developments clearly need further research work.

Acknowledgment. Authors would like to thank the Institute of Postgraduate Studies (IPS), Universiti Sains Malaysia (USM) for the financial support through the USM Fellowship.

References

1. Van Kranenburg, R.: A Critique of Ambient Technology and the All-seeing Network of RFID. The Netherlands Institute of Network Culture, Amsterdam (2008)
2. Abomhara, M., Køien, G.M.: Security and privacy in the Internet of Things: current status and open issues. In: International Conference on Privacy and Security in Mobile Systems (PRISMS). IEEE (2014)
3. Sundmaeker, H., et al.: Vision and Challenges for Realising the Internet of Things. Cluster of European Research Projects on the Internet of Things. European Commision, Brussels (2010)
4. Bandyopadhyay, D., Sen, J.: Internet of things: applications and challenges in technology and standardization. Wirel. Pers. Commun. **58**(1), 49–69 (2011)
5. Ul Rehman, A., Manickam, S.: A study of smart home environment and its security threats. Int. J. Reliab. Qual. Saf. Eng. **23**(03), 1640005 (2016)
6. Miorandi, D., et al.: Internet of things: vision, applications and research challenges. Ad Hoc Netw. **10**(7), 1497–1516 (2012)
7. Aldowah, H., et al.: Internet of Things in higher education: a study on future learning. In: Journal of Physics: Conference Series. IOP Publishing (2017)
8. Gen, H.P.-C.S.A. Controllers, R.: Hewlett-Packard Enterprise Development LP. Citeseer (2015)
9. Sicari, S., et al.: Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
10. Jha, A., Sunil, M.: Security considerations for Internet of Things. L&T Technology Services, Vadodara (2014)
11. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. **57**(10), 2266–2279 (2013)
12. Yue, X., et al.: Cloud-assisted industrial cyber-physical systems: an insight. Microprocess. Microsyst. **39**(8), 1262–1270 (2015)
13. Minoli, D.: Building the Internet Of Things with IPv6 and MIPv6: The Evolving World of M2M Communications. Wiley, Hoboken (2013)
14. Jan, S., et al.: Applications and challenges faced by internet of things-a survey. Int. J. Eng. Trends Appl. **ISSN**, 2393–9516 (2016)
15. Jing, Q., et al.: Security of the internet of things: perspectives and challenges. Wirel. Netw. **20**(8), 2481–2501 (2014)
16. Vasilomanolakis, E., et al.: On the security and privacy of internet of things architectures and systems. In: 2015 International Workshop on Secure Internet of Things (SIoT). IEEE (2015)
17. Botta, A., et al.: Integration of cloud computing and internet of things: a survey. Future Gener. Comput. Syst. **56**, 684–700 (2016)
18. Issarny, V., et al.: Service-oriented middleware for the future internet: state of the art and research directions. J. Internet Serv. Appl. **2**(1), 23–45 (2011)
19. Gubbi, J., et al.: Internet of Things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)

20. Jara, A.J., Kafle, V.P., Skarmeta, A.F.: Secure and scalable mobility management scheme for the Internet of Things integration in the future internet architecture. Int. J. Ad Hoc Ubiquitous Comput. **13**(3–4), 228–242 (2013)
21. Stankovic, J.A.: Research directions for the internet of things. IEEE Internet Things J. **1**(1), 3–9 (2014)
22. Haitao, L.B.C.H.W., Ying, F.: Security analysis and security model research on IOT. Comput. Digital Eng. **11**, 006 (2012)
23. Tan, Y., Han, J.: Service-oriented middleware model for internet of things. Comput. Sci. **38** (3), 23–45 (2011)
24. Henze, M., et al.: A comprehensive approach to privacy in the cloud-based Internet of Things. Future Gener. Comput. Syst. **56**, 701–718 (2016)
25. Suo, H., et al:. Security and privacy in mobile cloud computing. In: 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE (2013)
26. Wan, J., et al.: From machine-to-machine communications towards cyber-physical systems. Comput. Sci. Inf. Syst. **10**(3), 1105–1128 (2013)
27. Wan, J., et al.: VCMIA: a novel architecture for integrating vehicular cyber-physical systems and mobile cloud computing. Mob. Netw. Appl. **19**(2), 153–160 (2014)
28. Ning, H., Liu, H.: Cyber-physical-social based security architecture for future internet of things. Adv. Internet Things **2**(01), 1 (2012)
29. Kim, J.T.: Requirement of security for IoT application based on gateway system. Communications **9**(10), 201–208 (2015)
30. Kim, J.T.: Analyses of requirement for secure IoT gateway and assessment. International information institute (Tokyo). Information **19**(3), 833 (2016)
31. Puthal, D., et al.: A dynamic prime number based efficient security mechanism for big sensing data streams. J. Comput. Syst. Sci. **83**(1), 22–42 (2017)
32. Hernández-Ramos, J.L., et al.: DCapBAC: embedding authorization logic into smart things through ECC optimizations. Int. J. Comput. Math. **93**(2), 345–366 (2016)
33. Ye, N., et al.: An efficient authentication and access control scheme for perception layer of internet of things. Appl. Math. Inf. Sci. **8**(4), 1617 (2014)
34. Szczechowiak, P., et al.: NanoECC: testing the limits of elliptic curve cryptography in sensor networks. In: Wireless Sensor Networks, pp. 305–320. Springer, Berlin (2008)
35. Hernandez-Ramos, J.L., Bernabe, J.B., Skarmeta, A.: ARMY: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things. IEEE Commun. Mag. **54**(9), 28–35 (2016)
36. Usman, M., et al.: Sit: a lightweight encryption algorithm for secure internet of things. arXiv preprint arXiv:1704.08688 (2017)
37. Bull, P., et al.: Flow based security for IoT devices using an SDN gateway. In: IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE (2016)
38. Biswas, K., Muthukkumarasamy, V.: Securing smart cities using blockchain technology. In: IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS). IEEE (2016)
39. Harbor White Paper: Security for the internet of things. Harbor Res. **16**, 1–16 (2016)
40. Zebra Internet-Of-Things Solution Deployment Gains Momentum Among Firms Globally, A Forrester Consulting Thought Leadership Paper Commissioned By Zebra Technologies, October 2014
41. Ramirez, E.: Privacy and the IoT: Navigating Policy Issues. US FTC, Washington (2015)
42. Shipley, A.: Security in the Internet of Things. Wind River, September 2014 (2015)
43. Schaub, F., et al.: A design space for effective privacy notices. In: Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) (2015)