Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 141 (2018) 199–206

Procedia
Computer Science

www.elsevier.com/locate/procedia

The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2018)

Towards Security on Internet of Things: Applications and Challenges in Technology

Kazi Masum Sadique*, Rahim Rahmani, Paul Johannesson

Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden

Abstract

The Internet of Things (IoT) paradigm refers to the network of physical objects or "things" embedded with electronics, software, sensors, and connectivity to enable objects to exchange data with servers, centralized systems, and/or other connected devices based on a variety of communication infrastructures. IoT data collected from different sensors, nodes and collectors are transferred to the cloud over the internet. IoT devices are used by consumers, healthcare, businesses as well as by the governments. It is being forecast that 31 billion IoT devices will be deployed all over the world by the year 2020. As the use of IoT devices is increasing every moment several IoT vulnerabilities are introduced. The results and analysis indicate that massive deployment of IoT with an integration of new technologies are introducing new security challenges in IoT paradigm. In this paper, IoT security challenges and open issues are discussed which provides a ground for future research.

Keywords: Internet-of-Things; IoT security challenges; Trust in IoT; IoT data privacy; Distributed intelligence; Blockchain; 5G wireless technology; Software defined network (SDN); Network function virtualization (NFV); Machine learning

1. Introduction

The Internet connects us to the physical world through personal health monitors, proximity networks, smart homes, smart cars, and automation networks. These new networks provide tremendous opportunity, but also bring tremendous

* Corresponding author. Tel.: +46-736781636.
E-mail address: sadique@dsv.su.se

10.1016/j.procs.2018.10.168

risks [1]. IoT makes it possible to sense and control objects creating opportunities for more direct integration between the physical world and computer-based systems. IoT will usher automation in many application domains, ranging from manufacturing and energy management (e.g. SmartGrid) to healthcare management and urban life (e.g. SmartCity) [2]. In near future, 5G network will be the base infrastructure for the IoT devices with massive data capacity and massive device connectivity, which will allow 'zero distance' gap between machines and people [69] and 'zero latency' [70]. However, because of its fine-grained, continuous and pervasive data acquisition and control capabilities, IoT raises concerns about security. Deploying existing security solutions to IoT is not straightforward because of device heterogeneity, highly dynamic and possibly unprotected environments, and large scale.

2. Background and motivation

Internet of Things (IoT) technology enables the Internet to reach out into the real world of physical objects. Technologies like RFID, short-range wireless communications, real-time localization and sensor networks becoming increasingly pervasive, making the IoT a reality. We are experiencing a paradigm shift, in which everyday objects become interconnected and smart [3]. However human understanding and experience of the use of interacted smart things and smart systems have not developed at the same pace, these create challenges with enormous technical, security, privacy and trust consequences. A wide range of researchers from academia and industry as well as business, government agencies, and cities are exploring this technology from three main perspectives scientific theory, engineering design and the user experience. This shift aims to empower users by providing them with the knowledge required to understand and control their environment as well as by offering new accessible and interactive interfaces/applications that go beyond the traditional. The future focus is to implement artificial intelligent in all areas of IoT, including traffic management, power, monitoring, industrial production, building, agriculture, environment management, smart home, remote medical treatment etc. to have a smart networked society where recourses should be efficiently utilized with a positive effect on population [6]. All these innovative IoT development introduces new security challenges and open research areas to be addressed. Security of IoT needs to be addressed based on the characteristics of the IoT environment where it is applied [6].

2.1. IoT security vision

As explained in the previous section, connected IoT devices are the driving force for a smart world, where things play a vital role in our everyday life. Connected nodes are mostly RFID (Radio-frequency identification) tags or wireless sensors. Though TCP/IP (Transport control protocol/Internet protocol) is the main protocol used for Internet communication, IoT devices may need to use a short-range communication protocol to connect itself with a central node/hub from where data is transferred to the server/cloud [3]. The short-range communication protocols include near field communication (NFC), Bluetooth, IEEE 802.15.4, Wi-fi, ZigBee, and 6LoWPAN [4]. There are three basic layers in a typical IoT architecture: sensing/perception layer, transport/network layer, and application layer. Each of this layer has its own security issues to be considered [6], [7]. The sensing/perception layer holds the physical IoT devices those senses/share different parameters with its respective environment. If attackers get control of these devices, they will be able to extract sensitive information from it [6]. The transport/network layer is based on the internet infrastructure that allows the data to be transferred between the sensing/perception layer, and application layer [8]. The application layer includes storage, analysis, and representation of the data to the end user. The hardware and software at these different layers are mostly managed and maintained by different entities. For example, the physical hardware at the sensing/perception layer could be maintained by one provider. The Network layer could be managed by another network provider and data at the application layer could be stored by a cloud provider and accessed from a software which is built by another software developer company. Secure data transfer at the communication level and trust between all these entities are crucial.

3. Related work

There are many published papers on IoT security but not that many discussed the IoT security issued related to the current trend in IoT. In our study, we have considered papers related to security in IoT devices, IoT architecture, protocols for secure IoT communications and current trends in IoT security. Babar et al. suggested an embedded security framework and architecture that lightweight standardized protocol support with physical protection of secret keys and secure operating system [9]. As we have discussed earlier that physical nodes are connected through short distance communication protocol like Wi-Fi, 6LoWPAN and so on. Researches showed that these technologies are also vulnerable. Varadarajan and Crosby developed and evaluated an algorithm for end-to-end security for IoT using IPSec technology that enhances the security for 6LoWPAN [10]. Granjal et al. tested different cryptographic algorithms (AES, 3DES, SHA1, SHA2) on real wireless sensor nodes to achieve security for WSNs using IPSec and VPv6 in respect to encryption times and energy consumption [5]. Mostly protected Wi-Fi networked are secured using Wi-Fi protected access (WPA/2) could be the victim of key reinstallation attack [53]. All these solutions are specifically for the communication layer of any IoT solutions but not a complete security solution for IoT.

Table 1. IoT security survey papers based on discussion areas.

Area of discussion	Paper references (discussed)	Paper references (not discussed)	Partially Discussed
Security	[11-50]	[22]	
Privacy	[11-22], [24-39], [42-48], [50]	[40], [41], [49]	[23]
Trust	[11-15], [17], [18], [20], [21], [26], [28], [29], [31], [33], [34], [42-44], [46-48]	[16], [19], [22], [25], [27], [30], [32], [41], [45], [49], [50]	
Distributed Intelligence		[11-50]	
SDN/ NFV	[27], [33], [34], [36], [37]	[11-25], [28-32], [35], [38-50]	[26]
Blockchain	[31], [33]	[11-25], [27-30], [32], [34-50]	[26]
Machine learning		[11-50]	

We have analyzed forty IoT security survey papers based on seven parameters: security, privacy, trust and consideration of distributed intelligence, used in an application, use of software defined network (SDN), network function virtualization (NFV), blockchain technology and machine learning. From the table, we can see that none of the research introduces distributed intelligence to secure IoT infrastructure. We also see that none of the paper discussed the use of machine learning concepts to enhance IoT security. From the above table, we can also find that several researchers didn't discuss trust in IoT infrastructure and trust between different entities present at different layers of IoT.

4. Security threats and challenges in IoT

To design and implement complete security solutions for IoT paradigm, identification of threats and challenges of IoT networks, IoT devices, IoT applications and IoT is significant. Internet Engineering Task Force (IETF) has identified several IoT security threats [54]: (1) cloning of IoT devices by untrusted manufacturer, (2) substitution of things with malicious lower quality things, (3) man-in middle attack during commissioning and due to lack of proper authentication and authorization mechanisms in place, (4) firmware replacement with malicious code by an attacker, (5) privacy threat against sensitive data, (6) denial-of-service attack, (7) routing attack, (8) eavesdropping attack on poorly configured IoT network, and (9) extraction of security parameters from the physically unprotected IoT devices. The following key IoT Security challenges [55] need to be addressed in future IoT security research:

Device identity: A unique identity of IoT devices is crucial. Domain Name Servers (DNS) assign names to the connected IoT devices. But DNSs are also vulnerable of different attacks, i.e. man-in-middle attack, DNS cache positioning attack and so on. Attackers may reuse a stolen/hijacked device identity and perform a different kind of malicious activity within the network.

Firmware issue: Firmware updating and installation of security patches to IoT devices could be challenging. Everyday new security vulnerabilities are introducing to the Internet. Users of IoT devices may need to keep track of the updates installed on the devices. All IoT devices don't support live update. Users may need to unmount the device to install firmware and/or updates. A new device management system could be introduced to reduce the issues related to a firmware update. An automatic update may help but as discussed many of the devices don't support over-the-air update, so challenges exist.

Authentication and authorization: IoT networks consist of a huge number of devices. These devices need to be able to flexibility connect the network at any time. As IoT devices produce and/or process sensitive data, it must authenticate itself to receive and transmit data to the gateway. Security vulnerabilities increase by the use of default passwords, set by the manufacturers without changing it also by the use of weak passwords on any device. Authorization is equally important as authentication. IoT devices need to be able to read and write to a specific area of database and not the others. Attackers may get read/write access to sensitive data area if the device is compromised.

Management of huge IoT devices: As the number of devices in IoT networks are increasing every day, the management of these devices is becoming more and more complicated. A huge number of devices introduces new security vulnerabilities. Still, now, no generic management system has introduced.

Implementation of security algorithms: IoT devices are mostly small with limited power, processing, and memory capabilities. Implementation of complex cryptographic algorithms in this limited capability devices is quite impossible. Even encryption and deception could be hard due to device capabilities. These devices may be the victim of side channel attacks. Attackers may apply reverse engineering to restripe plain data transmitted over the network. Implementation of lightweight encryption algorithms on these devices may reduce the possibility of eavesdropping. Research opportunities exist for the design, implement, and test of new lightweight algorithms which will protect the data in IoT networks.

Communication security: Secure communication is very important for the transfer of sensitive IoT data in real-time over the Internet. As discussed earlier many IoT devices don't encrypt data before transmission over the internet. Secure private networking can reduce the vulnerabilities but as IoT data needs to be sent and received over a large network in many cases secure private network couldn't be a proper solution. The packaging of IoT data at an intermediate level like, at an edge network may also reduce the challenges. Future research opportunities exist to address this challenge.

Application security: Users data from the IoT nodes are stored in cloud, web and/or mobile devices. User data could include bank account information, health data, location information and more. Even secure communication will not protect the user data if the attacker gets access to the data from the web, cloud or mobile devices. So, the security of the IoT data stored in cloud web and mobile devices is also challenging.

Digester recovery and incident management: IoT devices could be placed in anything. Failure in an IoT node may introduce a huge problem. Proper digester recovery plan and incident management are very curtailed for real-time IoT devices where sensitive information is handled by the IoT sensors.

Vulnerability detection and management: Detection and management of different security vulnerabilities of IoT nodes are challenging. As IoT networks consist of many IoT devices it is not very easy to detect an affected node. Further research possibility exists to introduce new frameworks to address this challenge.

Availability and service disruption: IoT devices must always available to monitor/gather data. IoT devices may be compromised, physically damaged or stolen which will cause service interruption. High availability of IoT devices is very important for real-time monitoring systems.

Data privacy and integrity: Privacy and integrity protection is challenging. Only allowed user should have access to users' personal data. Proper permission from the user is required before access to the data by someone else. Data must be securely disposed of when it is no more needed.

Human factors: Handling of lazy users of IoT devices are challenging. For example, if a user of a car doesn't change a damaged device it could be a life threat for him or anybody else.

5. Open issues and discussion

Any security solution should consider three basic properties: confidentiality, integrity, and availability. Confidentiality of data or information means that the access to the data is restricted for the unauthorized persons. Integrity assures the originality of data. It means that the data is not changed by any unauthorized person. Availability refers to the presence of data for access at any time. It means the data is accessible at any time [51]. Internet of Things is no more a set of few connected nodes. IoT is moving forward every day with its rapid implementation in all most all sectors including smart city, smart agriculture, intelligent traffic management, self-driven car, intelligent logistics, smart buildings, intelligent power network, smart GPS navigation, environmental management, industrial monitoring, remote medical treatment and so on [6]. Secure IoT systems need to ensure confidentiality, integrity, and availability of sensitive data produced from all these smart systems.

5.1. Open issues

Based on the IoT security challenges pointed above we have identified the following open issues for future research:

- IoT end device identity for proper authentication and authorization
- Trust between different components in IoT paradigm
- Privacy of user data generated by IoT end devices
- End to end IoT data security with proper security enforcement and standardization

5.2. Discussion

To achieve security in IoT, it is very important to have a simplified generic presentation of any IoT system. We have suggested a generic six layers simplified presentation of the Internet of Things (IoT) paradigm and security requirements at each layer in Table 2.

Table 2. Layer representation of IoT and its security requirements.

Layer name	Security requirement
Physical sensor objects layer	End device security
Local communication layer	Local communication security
Gateway objects layer	Gateway data security
Internet Communication layer	Internet security
Cloud storage and data analysis layer	Cloud data security
IoT application layer	Application security

Any typical IoT application can be replaced with the above layered model. But IoT is moving forward with real-time decision making, for example, a self-driven car needs to decide immediately whether it should break or continue driving when it senses a person at a pedestrian crossing few meters away from the vehicle. In this situation distributed intelligence for IoT comes into play.

Securing IoT devices based on artificial intelligence and machine learning is a new area of research. An artificial neural network-based security approach was tested in a testbed in lab environment [52], data was collected from the edge network and analyzed. correct sensor value and incorrect delay, incorrect sensor value and correct delay, and incorrect delay and incorrect sensor value were also detected. Further research is possible to enhance this concept and test the designed system in a large lab environment. To enhance the security of IoT devices, malware detections, access control, authentication and secure overloading in techniques using machine learning also suggested in recent research [56]. Further research is possible in this area as well.

As we discussed in the challenge section trust between entities is very critical to secure IoT devices. As the devices communicate with other devices deployed by a different vendor, only trusted device should be able to pair and transfer data to the other party. To achieve trust, the unique identity of devices is very important. Sharma et al. proposed a trust management framework for IoT also suggested a machine learning based model for it [57]. As IoT devices should be able to join and leave the network at any time, further research is possible to achieve dynamic trust in IoT network.

Network automation and intend based networking is another new area where network connectivity and components are managed by software that supports artificial intelligence and machine learning [58], [59]. The combination of software defined networking with intend based network to enhance the quality of network with improved usability could be an interesting area of research. These are new research areas and standardization is important [60]. The use of intend based networking together with SDN for IoT devices and securing is also an open area of research. The use of network function virtualization (NFV) and software defined network (SDN) to secure of IoT is also a new area of research [61-63]. Many open issues need to be addressed. Use of Blockchain in IoT Security suggested in current research [64-68]. This is an open research area on the Internet of Things where distributed intelligence with blockchain technology will enhance IoT security.

To support massive capacity and massive connectivity with flexibility and intelligence, the core network of 5G will include cloud-based computing with a combination of SDN and NFV [69], [71]. The 5GEx concept will allow multi-domain and multi-technology communication between different network entities [71]. As per researcher, 5G network will increase machine to machine (M2M) communication and it will also increase the number of applications, which will allow human to interact with the machines in an efficient manner [72]. The security of 5G is an open area of research.

6. Conclusions

Internet of things is a multidisciplinary area, where technology meets people to enrich the quality of living with an improved working environment and efficient productivity. As the number of IoT devices is increasing, many new technology areas are integrating with IoT, for management, connection, and collaboration with the central server/gateway. We have discussed twelve security challenges for IoT paradigm. The use of the distributed intelligence will allow instance decision making and will reduce unnecessary data transfer to the cloud. A simplified generic model with six layers has been introduced in this paper which can represent any IoT system. A proper implementation of distributed intelligence on this layered model will ensure complete security for IoT. Application of machine learning in IoT is growing in all sector of IoT, including security of IoT. Though machine learning algorithms are enhancing IoT paradigm it also introduces security issues. A compromised IoT node could be trained with misleading data and it may behave unexpectedly and can be very harmful. To protect IoT nodes from unauthorized access, trustworthy IoT infrastructure is required. The massive amount of sensitive data should be produced from the future IoT systems. For the security, privacy and trust in future IoT networks and IoT data use of machine learning algorithms, distributed intelligence, network function virtualization, software defined network, blockchain technologies, and the 5G wireless network will increase. Use of all these emerging technologies introduce open security issues to address in further research.

References

[1] Santucci, G. (2010). The internet of things: Between the revolution of the internet and the metamorphosis of objects. Vision and Challenges for Realising the Internet of Things, 11-24.

[2] Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2011). Internet of things strategic research roadmap. Internet of Things-Global Technological and Societal Trends, 1(2011), 9-52.

[3] Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). The internet of things. Scientific American, 291(4), 76-81.

[4] Sardeshmukh, H., & Ambawade, D. (2017, June). Internet of Things: Existing protocols and technological challenges in security. In Intelligent Computing and Control (I2C2), 2017 International Conference on (pp. 1-7). IEEE.

[5] Granjal, J., Silva, R., Monteiro, E., Silva, J. S., & Boavida, F. (2008, September). Why is IPSec a viable option for wireless sensor networks. In Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on (pp. 802-807). IEEE.

[6] Peng, S., & Shen, H. (2012). Security technology analysis of IoT. In Internet of Things (pp. 401-408). Springer, Berlin, Heidelberg.

[7] Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015, December). Internet of things (IoT) security: Current status, challenges and prospective measures. In Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for (pp. 336-341). IEEE.

[8] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7), 1497-1516.

[9] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011, February). Proposed embedded security framework for internet of things (iot). In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on (pp. 1-5). IEEE.

[10] Varadarajan, P., & Crosby, G. (2014, March). Implementing IPsec in wireless sensor networks. In New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on (pp. 1-5). IEEE.

[11] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.

[12] Fremantle, P., & Scott, P. (2017). A survey of secure middleware for the Internet of Things. PeerJ Computer Science, 3, e114.

[13] Ramadhan, A. (2016). A survey of security aspects for Internet of Things in healthcare. In Information Science and Applications (ICISA) 2016 (pp. 1237-1247). Springer, Singapore.

[14] Mostefa, B., & Abdelkader, G. (2017, December). A survey of wireless sensor network security in the context of Internet of Things. In Information and Communication Technologies for Disaster Management (ICT-DM), 2017 4th International Conference on (pp. 1-8). IEEE.

[15] Sain, M., Kang, Y. J., & Lee, H. J. (2017, February). Survey on security in Internet of Things: State of the art and challenges. In Advanced Communication Technology (ICACT), 2017 19th International Conference on (pp. 699-704). IEEE.

[16] Kraijak, S., & Tuwanut, P. (2015, October). A survey on internet of things architecture, protocols, possible applications, security, privacy, real-world implementation and future trends. In Communication Technology (ICCT), 2015 IEEE 16th International Conference on (pp. 26-31). IEEE.

[17] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

[18] Pawar, A. B., & Ghumbre, S. (2016, December). A survey on IoT applications, security challenges and counter measures. In Computing, Analytics and Security Trends (CAST), International Conference on (pp. 294-299). IEEE.

[19] Tank, B., Upadhyay, H., & Patel, H. (2016, March). A survey on IoT privacy issues and mitigation techniques. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (p. 2). ACM.

[20] Moinuddin, K., Srikantha, N., Lokesh, K. S., & Narayana, A. (2017). A Survey on Secure Communication Protocols for IoT Systems. International Journal Of Engineering And Computer Science, 6(6).

[21] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal, 4(5), 1250-1258.

[22] Benabdessalem, R., Hamdi, M., & Kim, T. H. (2014, December). A survey on security models, techniques, and tools for the internet of things. In Advanced Software Engineering and Its Applications (ASEA), 2014 7th International Conference on (pp. 44-48). IEEE.

[23] Ida, I. B., Jemai, A., & Loukil, A. (2016, December). A survey on security of IoT in the context of eHealth and clouds. In Design & Test Symposium (IDT), 2016 11th International (pp. 25-30). IEEE.

[24] Zhao, K., & Ge, L. (2013, December). A survey on the internet of things security. In Computational Intelligence and Security (CIS), 2013 9th International Conference on (pp. 663-667). IEEE.

[25] Krishna, B. S., & Gnanasekaran, T. (2017, February). A systematic study of security issues in Internet-of-Things (IoT). In I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017 International Conference on (pp. 107-111). IEEE.

[26] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication protocols for Internet of Things: a comprehensive survey. Security and Communication Networks, 2017.

[27] Yassein, M. B., Abuein, Q., & Alasal, S. A. (2017, May). Combining software-defined networking with Internet of Things: Survey on security and performance aspects. In Engineering & MIS (ICEMIS), 2017 International Conference on (pp. 1-7). IEEE.

[28] Al-Gburi, A., Al-Hasnawi, A., & Lilien, L. (2018). Differentiating Security from Privacy in Internet of Things: A Survey of Selected Threats and Controls. In Computer and Network Security Essentials (pp. 153-172). Springer, Cham.

[29] Hellaoui, H., Koudil, M., & Bouabdallah, A. (2017). Energy-efficient mechanisms in security of the internet of things: A survey. Computer Networks, 127, 173-189.

[30] Azni, A. H., Alwi, N. H. M., & Seman, K. (2017). Experimental research testbed for internet of things: A survey from security services perspectives. Journal of Fundamental and Applied Sciences, 9(3S), 231-244.

[31] Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. Information Security Journal: A Global Perspective, 27(3), 162-182.

[32] Javdani, H., & Kashanian, H. (2017). Internet of things in medical applications with a service-oriented and security approach: a survey. Health and Technology, 1-12.

[33] Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of Things Security: a top-down survey. Computer Networks.

[34] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of things security: A survey. Journal of Network and Computer Applications, 88, 10-28.

[35] Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8-27.

[36] Zolanvari, M., & Jain, R. (2015). IoT security: a survey.

[37] Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680-698.

[38] Ezema, E., Abdullah, A., & Mohd, N. F. B. (2018). Open Issues and Security Challenges of Data Communication Channels in Distributed Internet of Things (IoT): A Survey.

[39] Grabovica, M., Popić, S., Pezer, D., & Knežević, V. (2016, June). Provided security measures of enabling technologies in Internet of Things (IoT): A survey. In Zooming Innovation in Consumer Electronics International Conference (ZINC), 2016 (pp. 28-31). IEEE.

[40] Kamble, A., Malemath, V. S., & Patil, D. (2017, February). Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. In Emerging Trends & Innovation in ICT (ICEI), 2017 International Conference on (pp. 33-39). IEEE.

[41] Deogirikar, J., & Vidhate, A. (2017, February). Security attacks in IoT: a survey. In I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017 International Conference on (pp. 32-37). IEEE.

[42] Ghorbani, H. R., & Ahmadzadegan, M. H. (2017, November). Security challenges in internet of things: survey. In Wireless Sensors (ICWiSe), 2017 IEEE Conference on (pp. 1-6). IEEE.

[43] Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312.

[44] Oracevic, A., Dilek, S., & Ozdemir, S. (2017, May). Security in internet of things: A survey. In Networks, Computers and Communications (ISNCC), 2017 International Symposium on (pp. 1-6). IEEE.

[45] Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on (Vol. 3, pp. 648-651). IEEE.

[46] Nastase, L. (2017, May). Security in the Internet of Things: A Survey on Application Layer Protocols. In Control Systems and Computer Science (CSCS), 2017 21st International Conference on (pp. 659-666). IEEE.

[47] Balte, A., Kashid, A., & Patil, B. (2015). Security issues in Internet of things (IoT): A survey. International Journal of Advanced Research in Computer Science and Software Engineering, 5(4).

[48] Deshmukh, S., & Sonavane, S. S. (2017, March). Security protocols for Internet of Things: A survey. In Nextgen Electronic Technologies: Silicon to Software (ICNETS2), 2017 International Conference on (pp. 71-74). IEEE.

[49] Mali, A., & Nimkar, A. (2017, September). Security Schemes for Constrained Application Protocol in IoT: A Precise Survey. In International Symposium on Security in Computing and Communication (pp. 134-145). Springer, Singapore.

[50] Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of internet of things. arXiv preprint arXiv:1501.02211.

[51] Mark, R.-O. (2013). The Complete Reference: Information Security, Second Edition. McGraw Hill Education

[52] Canedo, J., & Skjellum, A. (2016). Using machine learning to secure IoT systems. 2016 14th Annual Conference on Privacy, Security and Trust, PST 2016, 219–222. https://doi.org/10.1109/PST.2016.7906930

[53] Vanhoef, M., & Piessens, F. (2017). Key Reinstallation Attacks. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17, 1313–1328. https://doi.org/10.1145/3133956.3134027

[54] Garcia-morchon, O., Keon, S., Hummen, R., & Struik, R. (2012). Security Considerations in the IP-based Internet of Things draft-garcia-core-security-04, (c), 1–45.

[55] Anna MG. (2017). Top 10 IoT security challenges. IBM developerWirks, https://developer.ibm.com/dwblog/2017/iot-security-challenges/

[56] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT Security Techniques Based on Machine Learning. arXiv preprint arXiv:1801.06275.

[57] Sharma, A., Pilli, E. S., Mazumdar, A. P., & Govil, M. C. (2016, November). A framework to manage trust in internet of things. In Emerging Trends in Communication Technologies (ETCT), International Conference on (pp. 1-5). IEEE.

[58] CISCO. (2018). Intent-Based Networking Building the bridge between business and IT, https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/nb-09-intent-networking-wp-cte-en.pdf

[59] Earls E. M., Moozakis C. (2018). Intent-based networking and network automation: A primer https://searchnetworking.techtarget.com/feature/Network-automation-and-intent-based-networking-A-primer

[60] Doyle L. (2018). What is the relationship between intent-based networking and SDN? https://searchsdn.techtarget.com/answer/What-is-the-relationship-between-SDN-and-intent-based-networking

[61] Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security Threats and Best Practices. IEEE Communications Magazine, 55(8), 211–217. https://doi.org/10.1109/MCOM.2017.1600899

[62] Sahoo, K. S., Sahoo, B., & Panda, A. (2016). A secured SDN framework for IoT. Proceedings - 2015 International Conference on Man and Machine Interfacing, MAMI 2015. https://doi.org/10.1109/MAMI.2015.7456584

[63] Salman, O., Elhajj, I., Chehab, A., & Kayssi, A. (2017). Software Defined IoT security framework. 2017 4th International Conference on Software Defined Systems, SDS 2017, 75–80. https://doi.org/10.1109/SDS.2017.7939144

[64] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022

[65] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), (March), 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634

[66] Banerjee, M., Lee, J., & Choo, K. R. (2018). A blockchain future for Internet-of-Things security: a position paper. Digital Communications and Networks, (October 2017), 1–12. https://doi.org/10.1016/j.dcan.2017.10.006

[67] Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain Based Data Integrity Service Framework for IoT Data. Proceedings - 2017 IEEE 24th International Conference on Web Services, ICWS 2017, 468–475. https://doi.org/10.1109/ICWS.2017.54

[68] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an Optimized BlockChain for IoT. Proceedings of the Second International Conference on Internet-of-Things Design and Implementation - IoTDI '17, 173–178. https://doi.org/10.1145/3054977.3055003

[69] Huawei. (2014). 5G : A Technology Vision. Huawei, White Paer, 1–16.

[70] Doppler, K. (2015). 5G the next major wireless standard, 1–15.

[71] Bernardos, C. J., Dugeon, O., Galis, A., Morris, D., Simon, C., & Szabó, R. (2015). 5G Exchange (5GEx) – Multi-domain Orchestration for Software Defined Infrastructures. Eucnc2015, (JULY).

[72] Fettweis, G., & Alamouti, S. (2014). 5G: Personal mobile internet beyond what cellular did to telephony. IEEE Communications Magazine, 52(2), 140–145. https://doi.org/10.1109/MCOM.2014.6736754