Systematic Review of Internet of Things Security

Amiruddin Amiruddin[1,2], Anak Agung Putri Ratna[1], and Riri Fitri Sari[1]

[1]Faculty of Engineering, Universitas Indonesia, Depok, Indonesia
[2]Sekolah Tinggi Sandi Negara, Bogor, Indonesia

***Abstract*:** The Internet of Things has become a new paradigm of current communications technology that requires a deeper overview to map its application domains, advantages, and disadvantages. There have been a number of in-depth research efforts to study various aspects of IoT. However, to the best of our knowledge, there is no literature that have discussed specifically and deeply about the security and privacy aspects of IoT in recent three years. To that end, this paper aims at providing a comprehensive and systematic review of IoT security based on the most recent literature over the past three years (2015 to 2017). We studied IoT security research based on the research objectives, application domains, vulnerabilities/threats, countermeasures, platforms, proto-cols, and performance measurements. We also provided some security challenges for further research.

***Keywords*:** Internet of Things, protocol, security, systematic review, vulnerabilities**.**

1. Introduction

Internet of Things (IoT) was first introduced by British technology pioneer Kevin Ashton in 1999, describing a system with physical objects in the real world with the help of sensors connected to the Internet. IoT is an internetworking of physical objects such as sensors, actuators, personal computers, software, intelligent devices, automobile, and network connectivity that enable them to collect and exchange data without human intervention. The emergence of IoT has led to extensive interconnections between people, services, sensors and objects. IoT has been applied in many areas such as smart grids, smart homes, smart transportations, smart cities, smart healthcare, smart metering, and smart energy management.

The side-effect of IoT's rapid development is the drastic increase in the possibility of threats and security attacks against objects or individuals [1] as a consequence of the connection of so many objects without security guarantees [2]. IoT security is currently a hot research topic for academia, industry, and government. Several research studies have been undertaken to discover and classify potential threats to IoT [3] and its solutions as in [4], but these studies were inadequate, touching only a few aspects or domains. Therefore, in this study we sought to more comprehensively review the security of IoT based on recent literature form the year 2015 to 2017.

Our research contributions are: providing a survey methodology that is general and easy to understand. Our methodology adopted the Jorgensen's survey methodology [5]; providing a comprehensive description on IoT security based on recent literature; and providing future research challenges on IoT security.

This research adopted a methodology used by Jorgensen [5] in conducting a systematic review on software development cost estimation. Despite different research topics, that method can be adopted for use in conducting systematic reviews devoted to IoT security. Our research methodology consists of 5 stages, started from Define, Identify, Classify, Analyze, and ended up with Report (DICARe). The explanation of each step is as follows:

1. Define. The stage determines the criteria of the reviewed papers, i.e. topic and / or subtopics and time ranges. The topic we selected was IoT or cryptographic, whereas the time span is 2015 to 2017. Given the rapid changes occurring in IoT technology, this time span was considered appropriate. So our survey focused on published papers within the last three years.
2. Identify. This phase is to identify papers written in English that match the topic and or subtopics that have been determined in the previous stage. The way of identification is done by assessing the title, abstraction, keywords, and conclusions of the paper.
3. Classify. The stage of grouping or mapping problems on a paper based on a particular approach. In this survey we used IoT Security as the theme, and provided classification based on application domain, vulnerabilities/attacks, counter-measures, platforms, protocols, and performance measurements.
4. Analyze. The stage of analyzing the results of grouping or mapping that has been done in the previous stage.
5. Report. The reporting stage of the survey results may include the findings, the advantages or benefits or the disadvantage of the research results you submit your paper print it in two-column format,

2. Related Works

In this section we described the results of the literature review on IoT security including application domains, vulnerabilities / threats, countermeasures, platforms and protocols used, and performance measurement.

2.1 Application Domains of IoT Security

The IoT has a wide and diverse application field. Thus, we considered to map briefly the areas where IoT security has been applied based on the current literature. We found application domains of IoT security as follows: ambient assisted living [6], approximate computing [7], big data [8, 9], smart building [1], smart city [10], cloud service [11-15], edge computing [16], energy [1], environmental monitoring [1] [17, 18], fog computing [19, 20], general [21-39], general sensing [2, 40-46], healthcare [1, 40, 41, 47-58], smart home [10, 40, 51, 59, 60], industrial [33], mobile service [59], Personal Area Networks (PAN) [2, 56, 61], production management [1, 18, 62], radio access [63], smart grid [51, 64], transportation [1, 47, 51], universal [65].

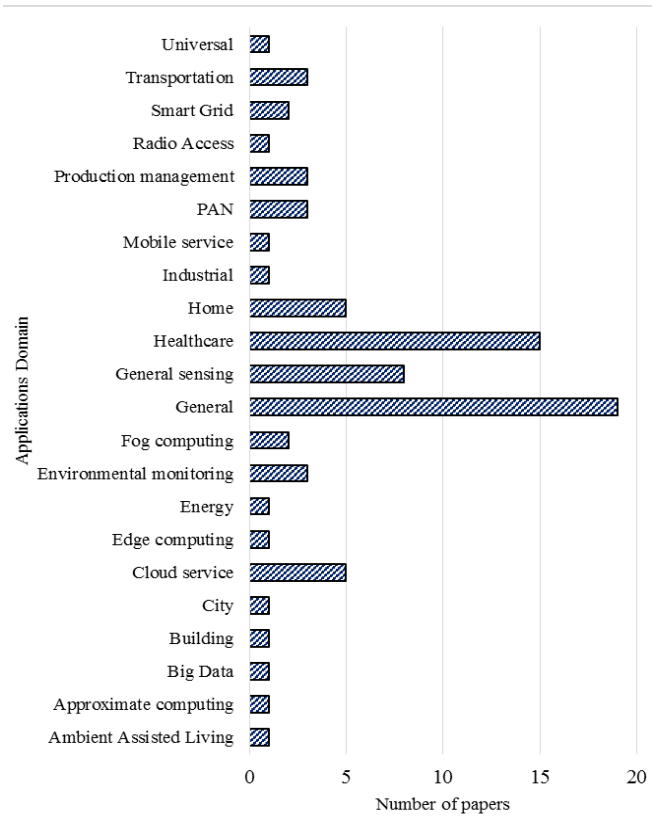

Figure 1. Distribution of paper by IoT security domain of applications

We can see in Figure 1 that the top five fields where IoT security have been paid more attention are general (24%), healthcare (19%), general sensing (10%), home (6%), and cloud service (6%). This reflects the potential market of IoT security. However, based on this, we can see that some new application domains of IoT security e.g. radio access, industrial, big data, and approximate computing, have not get enough researcher's attention. Therefore, it can be the next research target.

2.2 Vulnerablities/Threats of IoT Security

Along with technology advances, there are always security challenges. IoT security vulnerabilities or threats range on wide surface as follows: access control [19, 22, 66-68], bad output [69], brute force [21, 70], cloud attacks [71], computation overhead [33, 72, 73], cryptanalysis [64, 74], cryptography [2, 56, 75, 76], data attacks [1, 18, 19, 22, 47, 49, 51, 53, 62, 67, 77-81], development attacks [45, 52, 69, 75, 76, 82, 83], device attacks [1, 7, 24, 50, 54, 55, 62, 66, 67, 69, 70, 77, 80, 84-86], disruption [2, 47, 51, 69, 86-88], Denial of Service [1, 2, 48, 49, 51, 66, 77, 80, 87-90], eavesdropping [2, 40, 47, 51, 62, 79] [88], firmware attacks [70, 75-77], gateway attacks [12, 66, 80], impersonation [1, 2, 49, 51, 66, 77, 91], key management [22, 70, 88, 92], machine learning [64], malicious code [20, 76, 77] [86, 88], MITM [19, 22, 66, 88], network attacks [1, 21, 51, 68, 70, 75, 80, 93], node attack [1, 2, 40, 43, 47, 80], password issues [22, 66], performance [10], physical attacks [1, 67, 68, 75, 94], quantum computing [95], replay [51, 62, 66, 80, 89], resource attacks [2, 44], social context [59], software management [19, 67, 70, 77, 96], storage attacks [1, 19, 68, 97], surveillance [1, 2, 62, 79], unauthorized attacks [47] [1, 23, 78], user manipulation [60, 77].

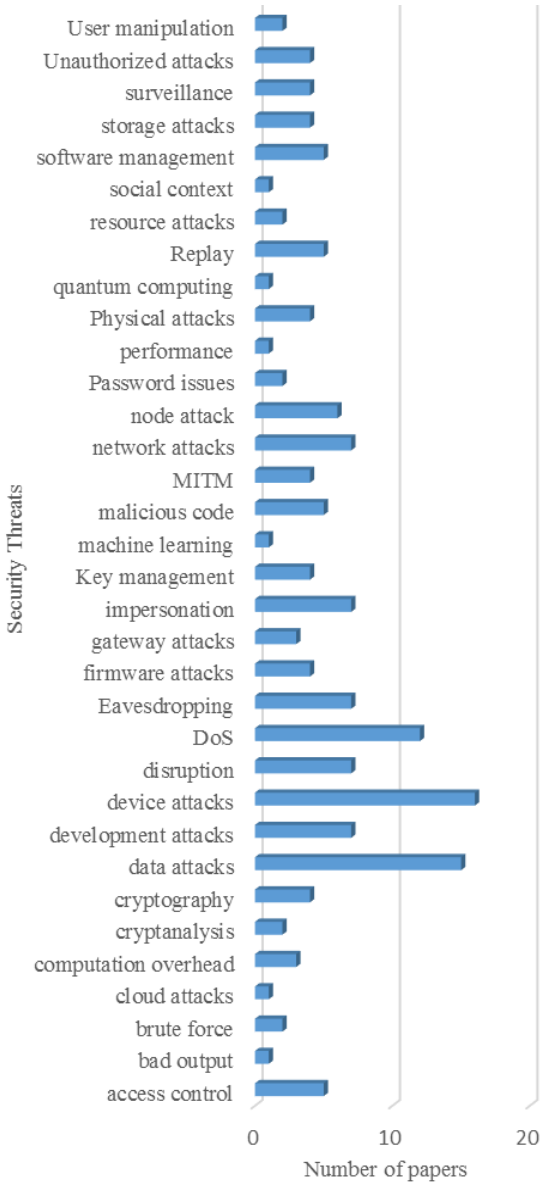

Figure 2. Distribution of paper by IoT security Threats

As we can see in Figure 2, the main vulnerabilities/threats that have been paid more attention to deal with in IoT security research are device attacks (10%), data attacks (9%), Denial of Service (DoS) (8%), eavesdropping (4,4%), disruption (4,4%), network attacks (4,4%) and development attacks (4,4%). However, there are several new types of vulnerabilities or attacks that have not been widely studied and discussed in literature such as social context which can be used for social engineering, quantum computing that can be used to easily break modern cryptographic algorithms, machine learning to direct targeted individuals or information, and bad output that can be used as entry point of analysis. Thus, those can be interesting to investigate in the future.

2.3 Countermeasures on IoT Security Threats

The Countermeasures on IOT security vulnerabilities are varied and depend on many aspects such as the type of application and protocol used as follows: access control [20, 67, 74, 77, 78, 85, 92], aggregation & correlation [97], anti-malware [70, 77], architecture [24, 48, 53, 82, 85], authentication & authorization [6, 19, 20, 23, 48, 55, 62, 64,

66, 70, 78, 82, 84, 85, 92, 98], automata [93], binary function [42], certificate [11, 20, 68, 77, 82, 83, 92], circuit defense [1, 7], coding [66, 78, 79], configuration [1, 75], context-based [44], elliptic curve cryptography [11, 47, 48, 99] [100], encryption [7, 11, 19, 22, 47, 48, 55, 63, 66, 69, 70, 79, 92, 99-102], forward security [48], framework [12, 18, 44, 45, 54, 60, 76], freshness [48], fuzzy logic [43], game theory [81], general [1, 72], group signature [47], hardware security [99], HARM [40], Hash [21, 47, 66], Homomorphic [47, 78, 79, 97, 101], IPS/IDS [1, 43, 67, 68, 70], isolation [1], key management [6, 22, 67, 69, 73, 78, 92, 102, 103], matrix [42], pairing [86], participatory verification [59], password [22, 75], public key infrastructure (PKI) [20, 78, 92, 100], Privacy Preserving Data Mining (PPDM) [79], product solution [87], Physically Unclonable Function (PUF) [7, 64, 72, 86, 99], Scheduling [63], Software Defined Networks (SDN) [63, 71, 92], secure protocol [22, 41, 48, 49, 72, 77, 84, 85, 91, 96, 104], secure storage [92], signature database [71], signcryption [33, 46, 105], software update [1, 75], standard/policy [1, 76, 79, 80], tagging [1], threat modeling [52, 60], traffic monitoring [71, 75], training [71, 77], trust model [60, 95], virtualization [71], vulnerability analysis [1, 7, 10, 67, 71, 90, 106, 107], watermarking [7], well design [50].

Table 1. Countermeasures on IoT Security

No.	Countermeasures	Percentage
1	Encryption	11.4
2	Authentication & authorization	9.0
3	Secure protocol	6.0
4	Key management	4.8
5	Access control	4.2
6	Certificate	4.2
7	Framework	4.2

As we can see in Table 1, the top countermeasures that have been proposed by researchers in current literature are encryption (11,4%), authentication and authorization (9%), secure protocol (6%), key management (4,8%), access control (4.2%), certificate usage (4.2%), and security frameworks (4,2%). Unfortunately, due to the variety of countermeasures, our classification of the countermeasures of IoT security attacks are ranging in a large scope which may be overlapping on some cases. However, we hope that this classification will still serve as a useful reference for other researchers. Furthermore, a better classification will be the next research challenge.

2.4 Platforms of IoT Security

We found several platforms used, discussed, or proposed in current literature of IoT security such as Midgar [21], Kaa [84], SicsthSense, SecureSense [11], OpenIoT [78], Midgar, Xively, Exosite, SensorCloud, Etheros, Thingsworx, Carriots, Amazon Web Service, IBM IoT [10], OpenIOT, Hydra, GSN, Ptolemy Assessor Host [108] and are summarized in Figure 3. In fact, there are several other platforms discussed in literature other than the literature we have discussed in this paper (range from year 2015 to 2017). Further investigation on the platforms used in IoT security and classification based on open or proprietary platform is necessary. Thus, it can be a useful insight for other researchers especially for those who have difficulty in the use of proprietary platforms.

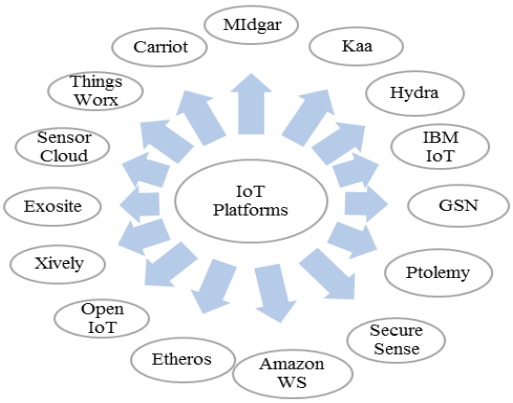

Figure 3. Platforms of IoT Security

2.5 Protocols of IoT Security

Based on current literature, we found several protocols used, discussed, improved, or proposed as follows: TLS/DTLS, MQTT [8, 59, 102, 109], DDS [8], ZigBee [110], HTTP/HTTPS [70], XMPP [109], LoRaWAN [89], 802.15.4 [41]. Figure 4 presents protocols of IoT security found on the current literature.

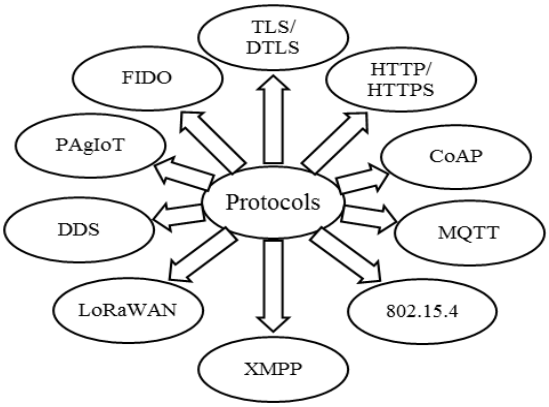

Figure 4. Protocols of IoT Security

2.6 Performance Measurements of IoT Security

We found several metrics of performance measurement of IoT security in current literature such as follows: Security cost, processing time [21], Data evaluation: timeliness, completeness, accuracy, precision [22], delay time [84], Transmission overview, communication latency, data header, run time, energy consumption, required memory [48, 111], theoretical evaluation, empirical evaluation [97], Computation time, additional encryption time [101], Attack probability, attack cost, average time to compromise, average connectivity [40], NIST Statistical Test [102], computational and communication cost, formal verification [66], compression and reconstruction validation [42], low jitter [63].

The types of measurements described in this sub-section as in Figure 5 are considered not sufficient. For example, there is no measurement of the randomness level of an encryption algorithms; and how to measure the performance of IoT security applications in the era of quantum [110] computing. IoT security measurements performed by [40] are still new

and can be further investigated to measure their validity.

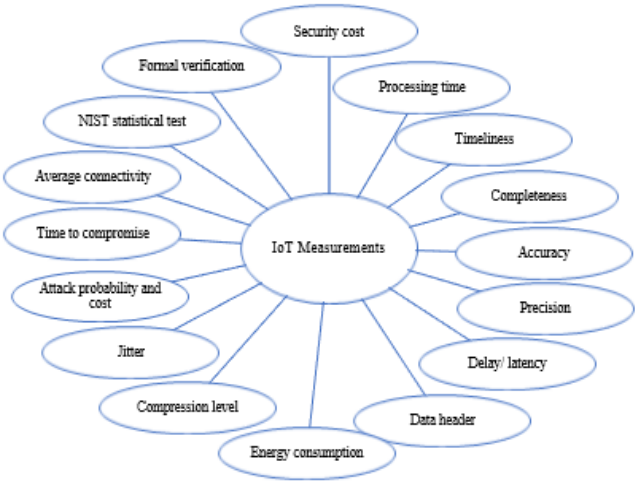

Figure 5. Performance measurements of IoT Security

3. Gap and Future Research Directions

3.1 Weaknesses of IoT Security

There are some fundamental weaknesses in IoT security application and implementation. In this study we especially highlighted the platforms, protocols, and security techniques in IoT applications.

Weaknesses on IoT platforms include: First, compatibility issues. Various IoT platforms are summarized in Figure 3 has not been covered by global standards in common for labeling and checking. Platform-making organizations need to agree to standards to make the IoT platform more effective and useful. Second, another weakness of the IoT platform lies in security. By sending all the platform information used, the danger of loss of protection also increases. Third, with the interconnection of devices, it will be very easy for malware to spread to all connected devices. If a device is attacked by malware, other devices connected will be infected as well.

IoT protocols as summarized in Figure 4 also have weaknesses including the following. MQTT has weaknesses in terms of encryption and authentication. CoAP has weaknesses in the use of DTLS, namely DTLS is not designed to support multicast. XMPP has a weakness in the simple authentication security layer (SASL) authentication, namely SASL does not provide adequate protection.

3.2 Limitations

There are several limitations to the application of IoT security, including the following:

1. IoT technology is still being developed, so that the proposed security mechanisms cannot be assessed properly. The IoT technology readiness determines the level of maturity of the platforms, protocols, and security techniques used.
2. Various types of platforms that are developed will not run effectively if they experience problems of compatibility. Consequently, the security mechanisms will not be meaningful if they are not able to bridge various platforms.
3. Some of the protocols suggested in the literature have not been implemented and are just theoretical analyzes. This means that the protocols need to be truly implemented in actual conditions so that its security performance can be measured.
4. In terms of security measurement, there is no parameter validation used. Some protocols use encryption algorithms in it. However, the data encryption process is not fast because it requires considerable capabilities or resources while IoT devices have limitations on these aspects.
5. The available policy services are still vague in dealing with issues of authorization and authentication.

3.3 Future Research Directions

Based on the findings in previous section, in this Sub-section we provided future research directions on IoT security based on our previous classification as follows:

1. Application domains. We found that some new application domains of IoT security e.g. radio access, industrial, big data, and approximate computing, have not been get enough researcher's attention and hence they can be the next research target to extent and expand the use of IoT in human life.
2. Vulnerabilities/attacks. There are several new types of vulnerabilities or attacks found in the literature such as social context, quantum computing, machine learning, and bad output, and these can be interesting to be scrutinized in the future.
3. Countermeasures. Due to the varied types of attacks, there are many countermeasures in IoT applications found in the literature and classification of them is necessary. Our classification of the countermeasures of IoT security attacks still seems to be wide category and some parts may overlap. Thus, a better classification will be a research challenge to provide and enhance understanding of IoT security awareness.
4. Platforms. Further investigation on the platforms used in IoT security and classification based on open or proprietary platform is necessary to provide a useful insight for other researchers especially for those who have difficulty in the use of proprietary platforms.
5. Protocols. There are many protocols in the IoT application, but the protocols most discussed or used for IoT security are CoAP, DTLS, and MQTT. Other protocols can be investigated to find ways to provide or improve IoT security.
6. Performance measurements. There is still a lack in performance measurement of IoT security. For example, in the reviewed literature, there is no measurement of the randomness level of cryptography algorithms. In addition, how to measure the performance of IoT security applications in the era of quantum computing is also a research challenge.
7. Others. Blockchain is a new paradigm of securing distributed implementation of IoT. The integration of blockchain to IoT implementation that can avoid the single point of failure occurring in centralized system become a research challenge to be investigated and realized by the researchers.

4. Conclusions

In this paper, a systematic review of IoT security during last three years (2015 - mid 2017) has been presented.

Classification of IoT security based application domains, vulnerabilities/attacks, countermeasures, platforms, protocols, and performance measurements has also been proposed. Based on the literature study, we highlighted some findings as follows: specific application domain that was widely discussed is healthcare; the most discussed vulnerability / attack is device attack; and the most discussed and proposed countermeasure is the use of encryption. We have also identified some research directions that can be explored in the future.

References

[1] A. M. Nia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," IEEE Transactions on Emerging Topics in Computing, vol. PP, pp. 1-1, 2017.

[2] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications, vol. 88, pp. 10-28, 2017.

[3] Aqeel-ur-Rehman, S. U. Rehman, I. U. Khan, M. Moiz, and S. Hasan, "Security and Privacy Issues in IoT," International Journal of Communication Networks and Information Security (IJCNIS) vol. Vol. 8, No. 3, December 2016, p. 11, 2016.

[4] A. u. Rehman, S. u. Rehman, I. U. Khan, M. Moiz, and S. Hasan, "Security and Privacy Issues in IoT," International Journal of Communication Networks and Information Security (IJCNIS), vol. 8, 2016.

[5] M. Jorgensen and M. Shepperd, "A Systematic Review of Software Development Cost Estimation Studies," IEEE Transactions on Software Engineering, vol. 33, pp. 33-53, 2007.

[6] P. H. Griffin, "Security for Ambient Assisted Living: Multi-factor Authentication in the Internet of Things," in 2015 IEEE Globecom Workshops (GC Wkshps), pp. 1-5, 2015.

[7] M. Gao, Q. Wang, M. T. Arafin, Y. Lyu, and G. Qu, "Approximate Computing for Low Power and Security in the Internet of Things," Computer, vol. 50, pp. 27-34, 2017.

[8] E. Ahmed, I. Yaqoob, I. A. T. Hashem, I. Khan, A. I. A. Ahmed, M. Imran, et al., "The role of big data analytics in Internet of Things," Computer Networks, 2017.

[9] S. F. Ochoa, G. Fortino, and G. Di Fatta, "Cyber-physical systems, internet of things and big data," Future Generation Computer Systems, vol. 75, pp. 82-84, 2017.

[10] C. González García, D. Meana-Llorián, B. C. Pelayo G-Bustelo, J. M. Cueva Lovelle, and N. Garcia-Fernandez, "Midgar: Detection of people through computer vision in the Internet of Things scenarios to improve the security in Smart Cities, Smart Towns, and Smart Homes," Future Generation Computer Systems, vol. 76, pp. 301-313, 2017.

[11] S. Raza, T. Helgason, P. Papadimitratos, and T. Voigt, "SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things," Future Generation Computer Systems, vol. 77, pp. 40-51, 2017.

[12] R. Vilalta, R. Ciungu, A. Mayoral, R. Casellas, R. Martinez, D. Pubill, et al., "Improving Security in Internet of Things with Software Defined Networking," in 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1-6, 2016.

[13] T. Yang, B. Yu, H. Wang, J. Li, and Z. Lv, "Cryptanalysis and improvement of Panda - public auditing for shared data in cloud and internet of things," Multimedia Tools and Applications, vol. 76, pp. 19411-19428, 2017.

[14] G. Corbò, C. Foglietta, C. Palazzo, and S. Panzieri, "Smart Behavioural Filter for Industrial Internet of Things," Mobile Networks and Applications, 2017.

[15] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," IEEE Communications Magazine, vol. 55, pp. 26-33, 2017.

[16] J. H. Lee and H. Kim, "Security and Privacy Challenges in the Internet of Things [Security and Privacy Matters]," IEEE Consumer Electronics Magazine, vol. 6, pp. 134-136, 2017.

[17] I. Yaqoob, E. Ahmed, M. H. Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, et al., "The rise of ransomware and emerging security challenges in the Internet of Things," Computer Networks, 2017.

[18] M. Mohsin, Z. Anwar, G. Husari, E. Al-Shaer, and M. A. Rahman, "IoTSAT: A formal framework for security analysis of the internet of things (IoT)," in 2016 IEEE Conference on Communications and Network Security (CNS), pp. 180-188, 2016.

[19] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and Privacy Preservation Scheme of Face Identification and Resolution Framework Using Fog Computing in Internet of Things," IEEE Internet of Things Journal, vol. PP, pp. 1-1, 2017.

[20] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," IEEE Internet Computing, vol. 21, pp. 34-42, 2017.

[21] G. Sánchez-Arias, C. González García, and B. C. Pelayo G-Bustelo, "Midgar: Study of communications security among Smart Objects using a platform of heterogeneous devices for the Internet of Things," Future Generation Computer Systems, vol. 74, pp. 444-466, 2017.

[22] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, and A. Coen-Porisini, "A secure and quality-aware prototypical architecture for the Internet of Things," Information Systems, vol. 58, pp. 43-55, 2016.

[23] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," Journal of Network and Computer Applications, 2017.

[24] M. Taylor, D. Reilly, and B. Lempereur, "An access control management protocol for Internet of Things devices," Network Security, vol. 2017, pp. 11-17, 2017.

[25] M. Safkhani and N. Bagheri, "Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things," The Journal of Supercomputing, vol. 73, pp. 3579-3585, 2017.

[26] P. Porambage, A. Braeken, P. Kumar, A. Gurtov, and M. Ylianttila, "CHIP: Collaborative Host Identity Protocol with Efficient Key Establishment for Constrained Devices in Internet of Things," Wireless Personal Communications, vol. 96, pp. 421-440, 2017.

[27] N. Park and D. Lee, "Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment," Personal and Ubiquitous Computing, 2017.

[28] H. Lee;, O. Na;, Y. Kim;, and H. Chang, "A Study on Designing Public Safety Service for Internet of Things Environment," Wireless Personal Communication, vol. 93, pp. 447–459, 2017.

[29] H. Shen, J. Shen, M. K. Khan, and J.-H. Lee, "Efficient RFID Authentication Using Elliptic Curve Cryptography for the Internet of Things," Wireless Personal Communications, vol. 96, pp. 5253-5266, 2017.

[30] S. Hammoudi, Z. Aliouat, and S. Harous, "Challenges and research directions for Internet of Things," Telecommunication Systems, 2017.

[31] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K. R. Choo, et al., "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment," Journal of Network and Computer Applications, vol. 89, pp. 72-85, 2017.

[32] A. B. Lopez;, K. Vatanparvar;, A. P. D. Nath;, S. Yang;, S. Bhunia;, and M. A. A. Faruque, "A Security Perspective on Battery Systems of the Internet of Things," J Hardw Syst Secur, 2017.

[33] F. Li, J. Hong, and A. A. Omala, "Efficient certificateless access control for industrial Internet of Things," Future Generation Computer Systems, vol. 76, pp. 285-292, 2017.
[34] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," Telecommunication Systems, 2017.
[35] H. Tschofenig, "Fixing User Authentication for the Internet of Things (IoT)," Datenschutz und Datensicherheit - DuD, vol. 40, pp. 222-224, 2016.
[36] F. Li;, D. Zhong;, and T. Takagi, "Efficient Deniably Authenticated Encryption and Its Application to E-Mail," IEEE Transactions on Information Forensics and Security, vol. 11, pp. 2477 - 2486, 2016.
[37] M. Kang, O. Na, and H. Chang, "Security experts' capability design for future internet of things platform," Supercomput, vol. 72, pp. 103-119, 2016.
[38] A. A. Alamr, F. Kausar, J. Kim, and C. Seo, "A secure ECC-based RFID mutual authentication protocol for internet of things," The Journal of Supercomputing, 2016.
[39] S. Jang;, D. Lim;, J. Kang;, and I. Joe, "An Efficient Device Authentication Protocol Without Certification Authority for Internet of Things," Wireless Pers Commun, vol. 91, pp. 1681–1695, 2016.
[40] M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim, "A framework for automating security analysis of the internet of things," Journal of Network and Computer Applications, vol. 83, pp. 12-27, 2017.
[41] S. Sahraoui and A. Bilami, "Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things," Computer Networks, vol. 91, pp. 26-45, 2015.
[42] N. Wang, T. Jiang, W. Li, and S. Lv, "Physical-layer security in Internet of Things based on compressed sensing and frequency selection," IET Communications, vol. 11, pp. 1431-1437, 2017.
[43] T. Maphats'oe and M. Masinde, "A security algorithm for wireless sensor networks in the Internet of Things paradigm," in 2016 IST-Africa Week Conference, pp. 1-10, 2016.
[44] E. Ferrera, R. Rossini, D. Conzon, S. Tassone, and C. Pastrone, "Adaptive Security Framework for Resource-Constrained Internet-of-Things Platforms," in 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1-5, 2016.
[45] T. El-Maliki and J. M. Seigne, "Efficient Security Adaptation Framework for Internet of Things," in 2016 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 206-211, 2016
[46] M. E. S. Saeed, Q. Liu, G. Tian, B. Gao, and F. Li, "HOOSC: heterogeneous online/offline signcryption for the Internet of Things," Wireless Networks, 2017.
[47] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, "On perspective of security and privacy-preserving solutions in the internet of things," Computer Networks, vol. 102, pp. 83-95, 2016.
[48] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, et al., "End-to-end security scheme for mobility enabled healthcare Internet of Things," Future Generation Computer Systems, vol. 64, pp. 108-124, 2016.
[49] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, et al., "Session Resumption-Based End-to-End Security for Healthcare Internet-of-Things," in 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 581-588, 2015.
[50] O. Arias, J. Wurm, K. Hoang, and Y. Jin, "Privacy and Security in Internet of Things and Wearable Devices," IEEE Transactions on Multi-Scale Computing Systems, vol. 1, pp. 99-109, 2015.
[51] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," in 2016 3rd International Conference on Electronic Design (ICED), pp. 321-326, 2016.
[52] H. Sándor and G. Sebestyén-Pál, "Optimal security design in the Internet of Things," in 2017 5th International Symposium on Digital Forensic and Security (ISDFS), pp. 1-6, 2017.
[53] T. Ivaşcu, M. Frîncu, and V. Negru, "Considerations towards security and privacy in Internet of Things based eHealth applications," in 2016 IEEE 14th International Symposium on Intelligent Systems and Informatics (SISY), pp. 275-280, 2016.
[54] S. Siboni, A. Shabtai, N. O. Tippenhauer, J. Lee, and Y. Elovici, "Advanced Security Testbed Framework for Wearable IoT Devices," ACM Trans. Internet Technol., vol. 16, pp. 1-25, 2016.
[55] P. A. H. Williams and V. McCauley, "Always connected: The security challenges of the healthcare Internet of Things," in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), pp. 30-35, 2016.
[56] K. Lotfy and M. L. Hale, "Assessing Pairing and Data Exchange Mechanism Security in the Wearable Internet of Things," in 2016 IEEE International Conference on Mobile Services (MS), pp. 25-32, 2016.
[57] R. Mieronkoski, I. Azimi, A. M. Rahmani, R. Aantaa, V. Terävä, P. Liljeberg, et al., "The Internet of Things for basic nursing care—A scoping review," International Journal of Nursing Studies, vol. 69, pp. 78-90, 2017.
[58] F. Chen, Y. Luo, J. Zhang, J. Zhu, Z. Zhang, C. Zhao, et al., "An infrastructure framework for privacy protection of community medical internet of things," World Wide Web, 2017.
[59] B. C. Chifor, I. Bica, and V. V. Patriciu, "A Participatory Verification security scheme for the Internet of Things," in 2016 International Conference on Communications (COMM), pp. 267-270, 2016.
[60] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini, "SecKit: A Model-based Security Toolkit for the Internet of Things," Computers & Security, vol. 54, pp. 60-76, 2015.
[61] A. Kamble, V. S. Malemath, and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey," in 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), pp. 33-39, 2017.
[62] K. Yang, D. Forte, and M. M. Tehranipoor, "CDTA: A Comprehensive Solution for Counterfeit Detection, Traceability, and Authentication in the IoT Supply Chain," ACM Trans. Des. Autom. Electron. Syst., vol. 22, pp. 1-31, 2017.
[63] T. H. Szymanski, "Strengthening security and privacy in an ultra-dense green 5G Radio Access Network for the industrial and tactile Internet of Things," in 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 415-422, 2017.
[64] D. Mukhopadhyay, "PUFs as Promising Tools for Security in Internet of Things," IEEE Design & Test, vol. 33, pp. 103-115, 2016.
[65] H. G. C. Ferreira and R. T. de Sousa Junior, "Security analysis of a proposed internet of things middleware," Cluster Computing, vol. 20, pp. 651-660, 2017.
[66] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," Journal of Information Security and Applications, vol. 34, pp. 255-270, 2017.
[67] M. Lavanya and V. Natarajan, "Lightweight key agreement protocol for IoT based on IKEv2," Computers & Electrical Engineering, 2017.
[68] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities," Future Generation Computer Systems, 2017.

[69] A. P. Johnson, S. Patranabis, R. S. Chakraborty, and D. Mukhopadhyay, "Remote dynamic partial reconfiguration: A threat to Internet-of-Things and embedded security applications," Microprocessors and Microsystems, vol. 52, pp. 131-144, 2017.
[70] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System," IEEE Internet of Things Journal, vol. PP, pp. 1-1, 2017.
[71] H. Zhang, "How to disinfect and secure the Internet of Things," Network Security, vol. 2016, pp. 18-20, 2016.
[72] G. S. Rose, "Security meets nanoelectronics for Internet of things applications," in 2016 International Great Lakes Symposium on VLSI (GLSVLSI), pp. 181-183, 2016.
[73] S. N. Premnath and Z. J. Haas, "Security and Privacy in the Internet of Things Under Time-and-Budget-Limited Adversary Model," IEEE Wireless Communications Letters, vol. 4, pp. 277-280, 2015.
[74] Y. Yang, X. Zheng, and C. Tang, "Lightweight distributed secure data management system for health internet of things," Journal of Network and Computer Applications, vol. 89, pp. 26-37, 2017.
[75] E. Bertino and N. Islam, "Botnets and Internet of Things Security," Computer, vol. 50, pp. 76-79, 2017.
[76] R. H. Weber and E. Studer, "Cybersecurity in the Internet of Things: Legal aspects," Computer Law & Security Review, vol. 32, pp. 715-728, 2016.
[77] D. Pishva, "Internet of Things: Security and privacy issues and possible solution," in 2017 19th International Conference on Advanced Communication Technology (ICACT), pp. 797-808, 2017.
[78] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," Future Generation Computer Systems, vol. 76, pp. 540-549, 2017.
[79] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy: From sensors to the Internet of Things," Future Generation Computer Systems, vol. 75, pp. 46-57, 2017.
[80] M. Murphy, "The Internet of Things and the threat it poses to DNS," Network Security, vol. 2017, pp. 17-19, 2017.
[81] G. Rontidis, E. Panaousis, A. Laszka, T. Dagiuklas, P. Malacaria, and T. Alpcan, "A game-theoretic approach for minimizing security risks in the Internet-of-Things," in 2015 IEEE International Conference on Communication Workshop (ICCW), pp. 2639-2644, 2015.
[82] M. Vučinić, B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "OSCAR: Object security architecture for the Internet of Things," Ad Hoc Networks, vol. 32, pp. 3-16, 2015.
[83] G. Baldini, A. Skarmeta, E. Fourneret, R. Neisse, B. Legeard, and F. L. Gall, "Security certification and labelling in Internet of Things," in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), pp. 627-632, 2016.
[84] B.-C. Chifor, I. Bica, V.-V. Patriciu, and F. Pop, "A security authorization scheme for smart home Internet of Things devices," Future Generation Computer Systems, 2017.
[85] R. D. Chamberlain, M. Chambers, D. Greenwalt, B. Steinbrueck, and T. Steinbrueck, "Layered Security and Ease of Installation for Devices on the Internet of Things," in 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 297-300, 2016.
[86] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF-Based Secure Communication Protocol for IoT," ACM Trans. Embed. Comput. Syst., vol. 16, pp. 1-25, 2017.
[87] Y. Chahid, M. Benabdellah, and A. Azizi, "Internet of things security," in 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), pp. 1-6, 2017.
[88] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, "Learning Internet-of-Things Security Hands-On," IEEE Security & Privacy, vol. 14, pp. 37-46, 2016.
[89] S. Tomasin, S. Zulian, and L. Vangelista, "Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks," in 2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 1-6, 2017.
[90] H. Ko, J. Jin, and S. L. Keoh, "Secure Service Virtualization in IoT by Dynamic Service Dependency Verification," IEEE Internet of Things Journal, vol. 3, pp. 1006-1014, 2016.
[91] M. Tiloca, K. Nikitin, and S. Raza, "Axiom: DTLS-Based Secure IoT Group Communication," ACM Trans. Embed. Comput. Syst., vol. 16, pp. 1-29, 2017.
[92] S. Raza, L. Seitz, D. Sitenkov, and G. Selander, "S3K: Scalable Security With Symmetric Keys—DTLS Key Establishment for the Internet of Things," IEEE Transactions on Automation Science and Engineering, vol. 13, pp. 1270-1280, 2016.
[93] S. M. Hashemi, H. Jingsha, and A. E. Basabi, "Security for the Internet of Things with Intelligent Automata," in 2016 2nd IEEE International Conference on Computer and Communications (ICCC), pp. 1047-1051, 2016.
[94] Z. Zhong, J. Peng, and K. Huang, "Analysis on Physical-Layer Security for Internet of Things in Ultra Dense Heterogeneous Networks," in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 39-43, 2016.
[95] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a Quantum World," IEEE Communications Magazine, vol. 55, pp. 116-120, 2017.
[96] R. Behrens and A. Ahmed, "Internet of Things: An end-to-end security layer," in 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), pp. 146-149. 2017.
[97] L. González-Manzano, J. M. d. Fuentes, S. Pastrana, P. Peris-Lopez, and L. Hernández-Encinas, "PAgIoT – Privacy-preserving Aggregation protocol for Internet of Things," Journal of Network and Computer Applications, vol. 71, pp. 59-71, 2016.
[98] A. Tewari and B. B. Gupta, "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags," The Journal of Supercomputing, vol. 73, pp. 1085-1102, 2017.
[99] B. Halak, M. Zwolinski, and M. S. Mispan, "Overview of PUF-based hardware security solutions for the internet of things," in 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 1-4, 2016
[100] P. Schaumont, "Security in the Internet of Things: A challenge of scale," in Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 674-679, 2017.
[101] V. Mai and I. Khalil, "Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography," Future Generation Computer Systems, vol. 72, pp. 327-338, 2017.
[102] A. Mathur, T. Newe, W. Elgenaidi, M. Rao, G. Dooly, and D. Toal, "A secure end-to-end IoT solution," Sensors and Actuators A: Physical, vol. 263, pp. 291-299, 2017.
[103] J. Wu, M. Dong, K. Ota, L. Liang, and Z. Zhou, "Securing distributed storage for Social Internet of Things using regenerating code and Blom key agreement," Peer-to-Peer Networking and Applications, vol. 8, pp. 1133-1142, 2015.
[104] D. Shin, V. Sharma, J. Kim, S. Kwon, and I. You, "Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks," IEEE Access, vol. 5, pp. 11100-11117, 2017.

[105] W. Shi;, N. Kumar;, P. Gong;, N. Chilamkurti;, and H. Chang, "On the security of a certificateless online/offline signcryption for Internet of Things," Peer-to-Peer Netw. Appl. , vol. 8, pp. 881–885, 2015.

[106] Z. Zieliński, J. Chudzikiewicz, J. Furtak, and P. Głębocki, "Integrating some security and fault tolerant techniques for military applications of Internet of Things," in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), pp. 117-122, 2016.

[107] F. A. Teixeira, F. M. Q. Pereira, H.-C. Wong, J. M. S. Nogueira, and L. B. Oliveira, "SIoT: Securing Internet of Things through distributed systems analysis," Future Generation Computer Systems, 2017.

[108] E. Bertino, K.-K. R. Choo, D. Georgakopolous, and S. Nepal, "Internet of Things (IoT): Smart and Secure Service Delivery," ACM Trans. Internet Technol., vol. 16, pp. 1-7, 2016.

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

[110] R. A. Gheorghiu and V. Iordache, "Analysis of the Possibility to Implement ZigBee Communications in Road Junctions," Procedia Engineering, vol. 181, pp. 489-495, 2017.

[111] W. Mardini, M. Ebrahim, and M. Al-Rudaini, "Comprehensive Performance Analysis of RPL Objective Functions in IoT Networks," International Journal of Communication Networks and Information Security (IJCNIS), vol. 9, 2017.