A Study about the Different Categories of IoT in Scientific Publications

Sebastian Fischer
Secure Systems Engineering
Fraunhofer AISEC
Berlin, Germany
email:
sebastian.fischer@aisec.fraunhofer.de

Katrin Neubauer
Dept. Computer Science and Mathematics
Ostbayerische Technische Hochschule
Regensburg, Germany
email:
katrin1.neubauer@oth-regensburg.de

Rudolf Hackenberg
Dept. Computer Science and Mathematics
Ostbayerische Technische Hochschule
Regensburg, Germany
email:
rudolf.hackenberg@oth-regensburg.de

***Abstract*—The Internet of Things (IoT) is widely used as a synonym for nearly every connected device. This makes it really difficult to find the right kind of scientific publication for the intended category of IoT. Conferences and other events for IoT are confusing about the target group (consumer, enterprise, industrial, etc.) and standardisation organisations suffer from the same problem. To demonstrate these problems, this paper shows the results of an analyses over IoT publications in different research libraries. The number of results for IoT, consumer, enterprise and industrial search queries were evaluated and a manual study about 100 publications was done. According to the research library or search engine, different results about the distribution of consumer-, enterprise- and industrial- IoT are visible. The comparison with the results of the manual evaluation shows that some search queries do not show all desired publications or that considerably more, unwanted results are returned. Most researchers do not use the keywords right and the exact category of IoT can only be accessed via the abstract. This shows major problems with the use of the term IoT and its minor limitations.**

Keywords–Internet of Things; IoT; publications; consumer; industrial; enterprise; categorization.

I. INTRODUCTION

The Internet of Things is defined in ISO/IEC 20924:2018 page 9 as "[...] infrastructure of interconnected entities, people, systems and information resources together with services, which processes and reacts to information from the physical world and virtual world." [1] This definition is very broad and includes all possible devices that are connected to other devices via a network (not necessarily the Internet), like smartphones, personal computers, connected vehicles, airplanes, smart grid components, smart home devices, connected environment sensors, eHealth hardware, wearables and many more. The ISO/IEC definition is not the only one using this range of devices, also researchers are using IoT to describe all kind of products and prototypes. This leads to difficult situations where conferences or other events focus on IoT and the attendees do not know if the presentations are in their field of interest.

Searching for IoT scientific publications can be difficult as well. With only IoT, a too wide range of topics are returned. Restrictions, such as "consumer" or "enterprise" can help, but a lot of researchers do not use it. For example, the publication "Smart Charger Based on IoT Concept" [2] is about a consumer product, but the title and the keywords (Smart Charger, Arduino, Phone Charger, Battery Charger) are only containing "IoT" and "Smart Charger". A search for "IoT" and "consumer" will not include the publication.

In this study, we want to show the different problems of IoT as a general term. We start with some related work in Section II and the first part of research (Section III) consists of the different numbers of IoT publications in selected research libraries. The second part (Section IV) shows the results of a manual review of 100 publications according to their IoT category. In Section V, the results were then compared and evaluated to show the problems with the term IoT in research. At the end, a short conclusion and our future work are given in Section VII.

II. RELATED WORK

There is no recent study about current research on IoT publications, which includes the different categories "consumer", "industrial" and "enterprise". Some publications, like a study from Mishra et.al. [3] are covering the years from 2000 to 2015 or another study about the IoT trends reaches from 1992 to 2015 [4].

Some newer bibliometric studies from 2019 and 2020 are restricted to Blockchain [5] or Industrial 4.0 [6]. They are both showing the increasing amount of IoT publications, but no current overview of the whole situation of the last two years.

This study was inspired by the approach of the publications mentioned above, although the focus is different. The used academic search libraries differ in many point. For example, the target group and the type of search are different. IEEE Xplore targets technical publications, while Google Scholar and Semantic Scholar are universal. A 2018 paper examined the sizes of different libraries and identified Google Scholar as the largest [7]. Semantic Scholar, on the other hand, uses an algorithm that is based on artificial intelligence and is therefore supposed to provide very precise results [8]. In the course of this paper, the differences with respect to IoT will become clear again.

III. IOT PUBLICATIONS IN RESEARCH LIBRARIES

The aim of this study is to find out whether it is possible to find publications on specific areas of IoT without getting too many results and limit the great diversity of IoT, but also

 ISBN: 978-1-61208-778-8

TABLE I. NUMBER OF RESULTS PER SEARCH QUERY

Search term:	**Springer Link**	**IEEE Xplore**	**ScienceDirect**	**ACM digital library**	**Google Scholar**	**Semantic Scholar**
iot	16,545	10,996	7,203	3,027	44,800	56,000
iiot	529	398	359	74	4,730	2,230
smart home iot	4,096	615	1,954	814	20,000	11,500
automotive iot	1,277	117	639	155	8,270	2,830

TABLE II. NUMBER AND PERCENTAGE OF THE RELEVANT IOT CATEGORIES

Search term:	**Springer Link**	**IEEE Xplore**	**ScienceDirect**	**ACM digital library**	**Google Scholar**	**Semantic Scholar**
iot	16,545	10,996	7,203	3,027	44,800	56,000
industrial iot	5,780	1,197	3,281	735	20,400	16,000
consumer iot	3,738	545	2,010	1,316	17,100	9,620
enterprise iot	3,272	157	1,712	424	14,200	6,780
% of iot search:						
industrial iot	34.9 %	10.9 %	45.6 %	24.3 %	45.5 %	28.6 %
consumer iot	22.6 %	5.0 %	27.9 %	43.5 %	38.2 %	17.2 %
enterprise iot	19.8 %	1.4 %	23.8 %	14.0 %	31.7 %	12.1 %
Sum of %	77.3 %	17.3 %	97.2 %	81.8 %	115.4 %	57.9 %

without overlooking relevant publications. For this goal, we started with “IoT” as a search query in our manual study (Section IV) and after analysing the publications, we came up with three categories “industrial”, “consumer”, “enterprise”, as most of the devices can be classified into these (see Table III).

To find research about used encryption methods in consumer IoT devices, for example, the first search approach would be “consumer IoT encryption”. However, some researcher are not restrict their publications about encryption and just use the term IoT. The previous query will not find this work. If we just use “IoT encryption”, there are too many results (compared to the restricted). Research about encryption in vehicles, industrial environment, etc. are included as well.

To prove this statement we started with different research libraries and different queries and collected the numbers of results.

Overall, six libraries / search engines were used:

- Springer Link
- IEEE Xplore
- ScienceDirect
- ACM digital library
- Google Scholar
- Semantic Scholar

These libraries / search engines are the most common ones and widely used in computer science. Because of their different search algorithms (as seen in the results), data from all of them are shown. For example, IEEE Xplore finds a lot of results for “IoT” alone, but not much with “IoT” and other words combined. The words are all combined the same way over all search engines with the “AND” operator to find only publications with both words in it (e.g., “IoT AND consumer”).

The search was done with some word combinations to investigate the different areas of IoT. However, only a few words yielded many results. A precise search for a specific area is thus very well possible (e.g., automotive), as can be seen in Table I. However, the abbreviation IIoT for industrial IoT is not very common. All the results in this paper are only with new publications from the years 2019 and 2020, to show a current overview of the research in the field of IoT.

To get a better separation, for example of the whole 44,800 IoT results of Google Scholar, we used the three search terms in addition to “IoT”: “industrial”, “consumer” and “enterprise”. The results are shown in Table II. In our example from Google Scholar, we get about 45.5 % for “industrial”, 38.2 % for “consumer” and 31.7 % for “enterprise”. The sum is over 100 % because some of the publications can include more than one of them. This shows (in the case of Google Scholar) a good idea of how to find the right IoT category for a research (see Table II).

IV. IoT PUBLICATIONS STUDY

Because of the big differences in the search results and therefore in the search type, we made a manual study with 100 publications about their category of IoT. We want to know exactly, which publication belongs to industrial, consumer, enterprise or is not related to IoT at all. For this study, we needed 100 full publications most random as possible. Because we do not know the algorithms behind the different search engines, we decided to use Semantic Scholar with the option “has PDF”. This adds a bit randomness and makes it easier to get the full text. All the search parameters are:

- Keyword: iot
- Language: english
- Publication date: 2019 and 2020
- Option: ”has PDF”
- Sort by Relevance

This search leads to 11,800 results. We downloaded the first 100 publications [2], [9]–[107] and determined the categories. For a better evaluation of the results, it was also noted whether the category of the IoT devices in the publication can already be identified in the title, the abstract or only in the text. Additionally, it was evaluated whether the category can already be extracted from the keywords.

Table III shows the result of the manual review. First, the total number of publications. Not specified publications are

referring to IoT in general. For example, the publication about "Security on IoT Devices with Secure Elements" [30] can be applied to consumer, enterprise and industrial IoT devices. The category "consumer" consists of devices, which are meant to be used by consumers, not professional people. "Enterprise" describes the category for devices used by companies or installed / assembled by a professional service. The last category "industrial" are IoT devices for production. Overall, the different areas for each category were assigned as follows:

Consumer

- Smart Home devices
- Wearables
- Connected home automation and alarm systems

Enterprise

- Smart city devices
- Environment sensors (for big buildings or fields)
- Medical devices
- Vehicles (transportation)
- Sensors for bigger buildings
- Alarm systems (for business)

Industrial

- Machine sensors
- Machine control systems
- Industrial sensors
- Industrial devices with network connection

The lists above are not exhaustive. Medical and transportation devices can be used by consumer, but they have to be installed by a professional. Therefore, they are assigned to enterprise.

The remaining columns in Table III are showing the difficulty of assigning the publications to the categories. If the category can be be determined by the title, the publication is added to column t. If it is only in part possible, it is added to column (t). For example, the title "IoT based home automation using Raspberry Pi" [23] is clearly for consumer, because home automation is one of the consumer parts. In this case the publications is added to column t. Another title "IoT-Enabled Door Lock System" [28] is not clear, because a door lock system can be for the smart home market or just for business buildings. In this case the publication is added to column (t) as the product is in the title, but the main category can only be recognized in the abstract. Therefore, the publication is added to column a as well. The procedure is the same for the columns a and (a). If it is not possible to recognize the category from the title or abstract at all, the publication is added to the text column. If the category is already determined by the title, it will not be counted to the abstract or text, but it can be added to the keywords.

There are only 9 publications in the keywords column, because only clear keywords like "industrial" count. If the keywords are not clearly about the category, like "door lock", they do not count.

TABLE III. RESULT OF THE MANUAL REVIEWED PUBLICATIONS

		title		abstract			
	total	**t**	**(t)**	**a**	**(a)**	**text**	**keywords**
not specific	30	2	6	17		6	
industrial	14	1	3	8		2	1
consumer	22	4	8	9	1	3	5
enterprise	33	10	15	5		4	3
not IoT	1						
sum	100	17	32	39	1	15	9

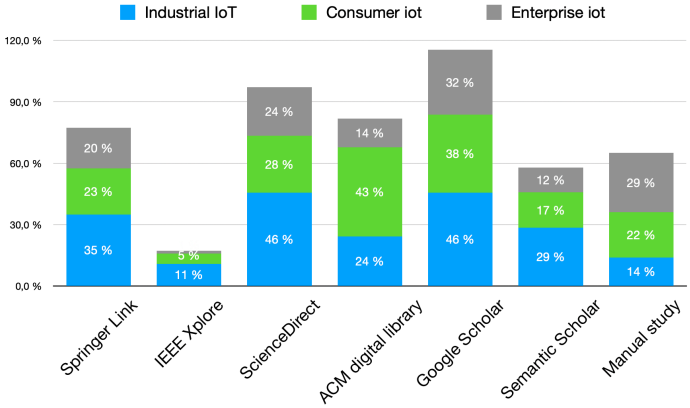

Figure 1. Result of the search in research libraries

There are 30 publications for IoT in general, 22 for consumer devices, 33 for enterprise, 14 for industrial and one publication, which is not related to IoT, but has some serial number with iot in the title. Most of the time, the publications for enterprise can be categorized with the title alone, 10 directly and 15 not clearly with related words. Overall, the most publications can be categorized without reading the whole text (but not without reading the abstract), in only 15 cases, further reading is needed. The keywords usage is not good, as only 9 are clearly categorizeable.

V. RESULTS

All results are from the previous research in early April 2020 as described in Sections III and IV. Figure 1 shows the percentage of the different categories according to the search results for only the term "IoT" in the different research libraries, compared with the manual study.

In the manual study, about 65 percent of all publications can be categorized. Semantic Scholar and Springer Link are near to this number with 58 and 77 percent. But with different weightings of the categories. This may be due to the limited number of samples in the manual study of 100.

IEEE Xplore shows a significantly lower number of results if the search term is expanded with the categories. This is due to the search method of IEEE Xplore, since only the metadata (title, abstract and keywords) are searched by default. This procedure has advantages and disadvantages, as will be shown in Section VI.

The other three libraries, ScienceDirect, ACM digital library and Google Scholar are over 82 percent (Google with

 ISBN: 978-1-61208-778-8

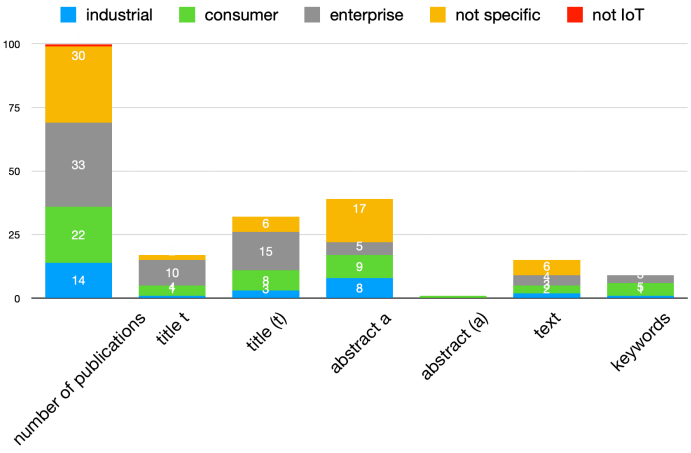

Figure 2. Result of the manual publications study

115 percent even over 100). This is the case, because some publications containing more than one of the three search words. This is useful, because general publications about IoT are still included in the restricted search queries, but for example, Google Scholar finds a lot of publications with “iot AND consumer” which are not consumer related. The high number of search results is because of the comprehensive search method. Even text inside the publication is found. For example, the two search results are in the first 100 results from google (search term: “iot AND consumer”): “A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements” [108] and “Beyond IoT Business” [109].

A big difference in all libraries are the weights between the categories. For example, the technical library IEEE Xplore has more industrial publications as a percentage than all the others. This should be considered by a search for only one category.

The results of the manual study from Section IV are shown in Figure 2. This figure shows the difficulty by categorizing IoT research. Only 17 publications can clearly be assigned with the title and 15 of them only via the text. The keywords are often not used and only useful in 9 cases. The different search approach from IEEE Xplore can only find results from column t and a, but most of the time, there is not a clear “consumer” or “industrial” in the title or the abstract and the library can not include the publication. Some assignments can only be done if, for example, it is possible to relate smart home to consumer.

Only with the results from Figure 1, it seems that IoT can be clearly delimited to the three categories (Google Scholar with over 100 percent together in all 3 categories). However, the manual study shows that there is research in IoT that is suitable for all areas (“not specific” in figure 2). But it is not easy to find the research that is relevant for your own field. Depending on the research library, different numbers of results are found and the weighting of the categories also varies greatly. The search for publications in the field of IoT is therefore associated with many problems, which will be described in more detail in Section VI.

VI. Problems

Since IoT is a comprehensive term, some problems arise when searching for scientific publications. Some of them are described in more detail in this section on the basis of the previous study.

We use the same example from Section III: searching for an encryption method for consumer IoT devices, like a smart home sensor. If we use “IoT AND consumer AND encryption”, we get a lower number of search results, but missing general IoT solutions for encryption, which do not include “consumer” in their text. If we change the search term to “IoT AND encryption AND NOT enterprise AND NOT industrial” we might miss some general research, too, but not as much as before. But also publications about production line encryption will be included, because they often miss the term “industrial IoT” or IIoT. Therefore, all unwanted terms must be excluded.

It takes less effort, to search for more specific term like “smart home” instead of IoT to get fewer results. However, by doing that, one misses a lot of publications or has to search for a lot of specific words. A Keyword search would be the best solution, but only a small subset would be returned. A restriction to categories is almost impossible, regardless of the fact that the keywords exists exactly for this purpose.

One of the biggest problems, with the large amount of search results is the difficulty to determine, if the publication is relevant. The results of the manual publications study shows, most of the time the abstract is necessary to get the information. This should be easier if the title or the keywords are better.

Another problem are the different ways in which the search engines work. Depending on the library, a restriction of IoT is useful or not (fewer results from IEEE Xplore with the category).

As a last issue, it is not clear how many publications in total from one category have been published in 2019 and 2020 because every search engine differs in the number of results and some are showing publications in more than one category. Therefore, this research question cannot be answered by this study.

VII. Conclusion and Future Work

IoT is a too broad term. Nearly every device can be counted as an Internet of Things devices. Therefore, a scientific search about IoT returns thousand of results. No categorization or other distinction is used by many researchers. In this study we only presented results about the big three categories “consumer”, “enterprise” and “industrial”. The more detailed results are not necessary for the biggest problems with IoT and not shown in this paper.

Some weak points about this study are the limitation of 100 papers from only one research library and no further research about the quality of the publications. Nevertheless, the study shows the need of clear categories and a strict use of them. The best way is to include them into the keywords and avoid using words from other categories in the whole publication, as the most search engines including the whole text. In some publications, the term IoT is not necessary at all (e.g., smart home or smart vehicles).

 ISBN: 978-1-61208-778-8

As future work, we are trying to find suitable categories and additional characteristics to build a categorization for every IoT device. Because not only researchers are struggling with the term IoT, standardisation organisations have the same problem, too. They have to decide, which product should be included in a new standard and which restrictions can be applied to all the included ones. They use very broad definitions like in ETSI EN 303 645, consumer devices are defined to be used typical in the home or as wearables, but they can be included in enterprise IoT environments as well: "Consumer IoT devices are commonly also used in business contexts. These devices remain classified as consumer IoT devices." [110]

REFERENCES

[1] "Information technology Internet of Things (IoT) Vocabulary," International Organization for Standardization, Geneva, CH, Standard, Dec. 2018.

[2] M. H. bin Husin, "Smart charger based on iot concept," International Journal of Education, Science, Technology and Engineering, vol. 2, 2019, pp. 39–44.

[3] D. Mishra et al., "Vision, applications and future challenges of internet of things: A bibliometric study of the recent literature," Ind. Manag. Data Syst., vol. 116, 2016, pp. 1331–1355.

[4] H.-H. Tsai, "A case study of research trends of internet of things." ICEB, 2015.

[5] M. Kamran, H. U. Khan, M. W. Nisar, M. Farooq, and S.-U. Rehman, "Blockchain and internet of things: A bibliometric study," Comput. Electr. Eng., vol. 81, 2020, p. 106525.

[6] A. Ahmi, H. Elbardan, and R. H. R. M. Ali, "Bibliometric analysis of published literature on industry 4.0," 2019 International Conference on Electronics, Information, and Communication (ICEIC), 2019, pp. 1–6.

[7] M. Gusenbauer, "Google scholar to overshadow them all? comparing the sizes of 12 academic search engines and bibliographic databases," Scientometrics, vol. 118, 2018, pp. 177–214.

[8] S. N. Fricke, "Semantic scholar," Journal of the Medical Library Association : JMLA, vol. 106, 2018, pp. 145 – 147.

[9] Z. B. Celik, G. Tan, and P. D. McDaniel, "Iotguard: Dynamic enforcement of security and safety policy in commodity iot," in NDSS Symposium, 2019.

[10] M. E. SUtIOT, "Exiopol-development and illustrative analyses of a detailed global mr ee sut / iot," 2019.

[11] J. Koo, S.-R. Oh, and Y.-G. Kim, "Device identification interoperability in heterogeneous iot platforms ," Sensors (Basel, Switzerland), vol. 19, 2019.

[12] I. Arpithashankar, "Iot based industrial pollution monitoring system," International Journal of Innovative Research in Technology, vol. 6, 2019, pp. 327–332.

[13] J. S. R. Dr and V. A. J. Ms, "Automation using iot in greenhouse environment," Journal of Information Technology and Digital World, vol. 1, 2019, pp. 38–47.

[14] M. Alhaisoni, "Iot energy efficiency through centrality metrics," Annals of Emerging Technol. in Com., vol. 3, no. 2, 2019, pp. 14–21.

[15] C. Nguyen and D. B. Hoang, "S-manage protocol for provisioning iot applications on demand." JTDE, Vol 7, No 3, Article 185, 2019.

[16] P. Radanliev et al., "Cyber risk in iot systems." Preprints, 2019.

[17] P. Manjunathmin and P. G. Shah, "Machine to machine metamorphosis to the iot," 2019.

[18] D. Johnson and M. Ketel, "Iot: Application protocols and security," I.J. Computer Network and Information Security, 4, 2019, pp. 1–8.

[19] D. Bilgeri, H. Gebauer, E. Fleisch, and F. Wortmann, "Driving process innovation with iot field data," MIS Q. Executive, vol. 18, 2019, p. 5.

[20] D. Sethuramalingam, N. V. Brindha, and S. Balamurugan, "Security for smart vehicle in iot," The IoT and the Next Revolutions Automating the World, 2019, pp. 289–296.

[21] E. Borelli et al., "Habitat: An iot solution for independent elderly," Sensors (Basel, Switzerland), vol. 19, 2019.

[22] A. Mavrogiorgou, A. Kiourtis, K. Perakis, S. Pitsios, and D. Kyriazis, "Iot in healthcare: Achieving interoperability of high-quality data acquired by iot medical devices," Sensors (Basel, Switzerland), vol. 19, 2019.

[23] A. Sinha and R. Tatikonda, "Iot based home automation using raspberry pi," International Journal of Advance Research, Ideas and Innovations in Technology, vol. 5, 2019, pp. 558–560.

[24] N. Walee et al., "An iot based smart parking system," 2019.

[25] L. C. Booth and M. Mayrany, "Iot penetration testing: Hacking an electric scooter," 2019.

[26] R. Pierdicca, M. Marques-Pita, M. Paolanti, and E. S. Malinverni, "Iot and engagement in the ubiquitous museum," Sensors (Basel, Switzerland), vol. 19, 2019.

[27] K. Ma, A. B. Bagula, C. N. Nyirenda, and O. Ajayi, "An iot-based fog computing model," Sensors (Basel, Switzerland), vol. 19, 2019.

[28] T. Adiono, S. Fuada, S. F. Anindya, I. G. Purwanda, and M. Y. Fathany, "Iot-enabled door lock system," International Journal of Advanced Computer Science and Applications, vol. 10, 2019.

[29] A. Singh, U. Sinha, and D. Sharma, "Cloud-based iot architecture in green buildings," Green Building Management and Smart Automation, 2020, pp. 164–183.

[30] T. Schläpfer and A. Rüst, "Security on iot devices with secure elements," 2019.

[31] S. Giordano et al., "Uprise-iot: User-centric privacy & security in the iot," 2019.

[32] M. Ansgariusson and A. Wihlborg-Rasmusen, "Robust header compression for cellular iot," 2019.

[33] Ragula, "Waste management in iot-enabled smart cities," 2019.

[34] L. Nóbrega, P. Gonalves, P. Pedreiras, and J. Pereira, "An iot-based solution for intelligent farming ," Sensors (Basel, Switzerland), vol. 19, 2019.

[35] H. A. Abdul-Ghani and D. Konstantas, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: An iot perspective," J. Sensor and Actuator Networks, vol. 8, 2019, p. 22.

[36] D. Minoli and B. Occhiogrosso, "Practical aspects for the integration of 5g networks and iot applications in smart cities environments," Wireless Communications and Mobile Computing, vol. 2019, 2019, pp. 5 710 834:1–5 710 834:30.

[37] Y. B. Zikria, S. W. Kim, O. Hahm, M. K. Afzal, and M. Y. Aalsalem, "Internet of things (iot) operating systems management: Opportunities, challenges, and solution," Sensors (Basel, Switzerland), vol. 19, 2019.

[38] E. C. Reilly, M. Maloney, M. Siegel, and G. Falco, "A smart city iot integrity-first communication protocol via an ethereum blockchain light client," 2019.

[39] R. H. Putra, F. T. Kusuma, T. N. Damayanti, and D. N. Ramadan, "Iot: smart garbage monitoring using android and real time database," TELKOMNIKA Telecommunication Computing Electronics and Control, vol. 17, 2019, pp. 1483–1491.

[40] D. Krcmarik, M. Petru, and R. Moezzi, "Innovative iot sensing and communication unit in agriculture," European Journal of Electrical Engineering, vol. 21, 2019, pp. 273–278.

[41] T. Alam and B. Rababah, "Convergence of manet in communication among smart devices in iot," International Journal of Wireless and Microwave Technologies, vol. 9, 2019, pp. 1–10.

[42] G. Yoon, D. Choi, J. Lee, and H. Choi, "Management of iot sensor data using a fog computing node," J. Sensors, vol. 2019, 2019, pp. 5 107 457:1–5 107 457:9.

[43] S. K. Lo, C. S. Liew, K. S. Tey, and S. Mekhilef, "An interoperable component-based architecture for data-driven iot system," Sensors (Basel, Switzerland), vol. 19, 2019.

[44] I. Bica, B.-C. Chifor, tefan Ciprian Arseni, and I. Matei, "Multi-layer iot security framework for ambient intelligence environments," Sensors (Basel, Switzerland), vol. 19, 2019.

[45] S. Rathore, Y. Pan, and J. H. Park, "Blockdeepnet: A blockchain-based secure deep learning for iot network," Sustainability, vol. 11, 2019, p. 3974.

 ISBN: 978-1-61208-778-8

[46] W. Ejaz, M. A. Azam, S. Saadat, F. Iqbal, and A. Hanan, "Unmanned aerial vehicles enabled iot platform for disaster management," Energies, vol. 12, 2019, p. 2706.

[47] N. Kherraf, "Provisioning of edge computing resources for heterogeneous iot workload," 2019.

[48] A. Márkus and J. Dombi, "Multi-cloud management strategies for simulating iot applications," Acta Cybernetica, vol. 24, 2019, pp. 83–103.

[49] I. Sittón-Candanedo, R. S. Alonso, Ó. García, L. Muñoz, and S. Rodríguez, "Edge computing, iot and social computing in smart energy scenarios," Sensors (Basel, Switzerland), vol. 19, 2019.

[50] A. M. Zarca et al., "Enabling virtual aaa management in sdn-based iot networks ," Sensors (Basel, Switzerland), vol. 19, 2019.

[51] M. Marchese, A. Moheddine, and F. Patrone, "Iot and uav integration in 5g hybrid terrestrial-satellite networks," Sensors (Basel, Switzerland), vol. 19, 2019.

[52] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore, Y. Sung, and J. H. Park, "Blockchain-based secure storage management with edge computing for iot," Electronics, vol. 8, 2019, p. 828.

[53] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (iot) authentication schemes ," Sensors (Basel, Switzerland), vol. 19, 2019.

[54] L. Jiang, X. Lou, R. Tan, and J. Zhao, "Differentially private collaborative learning for the iot edge," in EWSN, 2019.

[55] E. N. Ganesh, "Implementation of digital notice board using raspberry pi and iot," Oriental journal of computer science and technology, vol. 12, 2019, pp. 14–20.

[56] H. Miyajima and N. Shiratori, "Proposal of fast and secure clustering methods for iot," 2019.

[57] A. Brezulianu et al., "Iot based heart activity monitoring using inductive sensors," Sensors (Basel, Switzerland), vol. 19, 2019.

[58] S.-R. Oh, Y.-G. Kim, and S. Cho, "An interoperable access control framework for diverse iot platforms based on oauth and role ," Sensors (Basel, Switzerland), vol. 19, 2019.

[59] H. Muccini, C. Arbib, P. Davidsson, and M. T. Moghaddam, "An iot software architecture for an evacuable building architecture," in HICSS, 2019.

[60] N. T. Kamatham, "Quality and energy aware services selection for iot," International Journal of Scientific Research in Science and Technology, 2020, pp. 93–98.

[61] Y.-S. Seo and J.-H. Huh, "Automatic emotion-based music classification for supporting intelligent iot applications," Electronics, vol. 8, 2019, p. 164.

[62] H. M. A. Islam, D. Lagutin, A. Ylä-Jääski, N. Fotiou, and A. V. Gurtov, "Transparent coap services to iot endpoints through icn operator networks ," Sensors (Basel, Switzerland), vol. 19, 2019.

[63] S. Taj, U. Asad, M. Azhar, and S. Kausar, "Interoperability in iot based smart home: A review," 2019.

[64] N. Surantha, C. Adiwiputra, O. Kurniawan, S. Muhamad, and B. Soewito, "Iot system for sleep quality monitoring using ballistocardiography sensor," International Journal of Advanced Computer Science and Applications, vol. 11, 2020.

[65] A. Pravin, P. Jacob, and G. Nagarajan, "A comprehensive survey on edge computing for the iot," 2019.

[66] S. Awadallah, A. D. Moure, and P. Torres-González, "An internet of things (iot) application on volcano monitoring," Sensors (Basel, Switzerland), vol. 19, 2019.

[67] D. A. F. Saraiva et al., "Prisec: Comparison of symmetric key algorithms for iot devices," Sensors (Basel, Switzerland), vol. 19, 2019.

[68] J. M. Waworundeng, N. C. Suseno, and R. R. Y. Manaha, "Automatic watering system for plants with iot monitoring and notification," 2019.

[69] G. Cerutti, R. Prasad, A. Brutti, and E. Farella, "Neural network distillation on iot platforms for sound event detection," in INTERSPEECH 2019, 2019.

[70] J. M. Ceron, K. Steding-Jessen, C. Hoepers, L. Z. Granville, and C. B. Margi, "Improving iot botnet investigation using an adaptive network layer," Sensors (Basel, Switzerland), vol. 19, 2019.

[71] E. Odat, "Traffic monitoring and mac-layer design for future iot systems," 2019.

[72] K. Kost'al, P. Helebrandt, M. Bellus, M. Ries, and I. Kotuliak, "Management and monitoring of iot devices using blockchain ," Sensors (Basel, Switzerland), vol. 19, 2019.

[73] N. Kumar, S. N. Panda, P. Pradhan, and R. K. Kaushal, "Iot based hybrid system for patient monitoring and medication," EAI Endorsed Trans. Pervasive Health Technol., vol. 5, 2019, p. e1.

[74] F. Zantalis, G. E. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and iot in smart transportation," Future Internet, vol. 11, 2019, p. 94.

[75] T. R. Mauldin, A. H. H. Ngu, V. Metsis, M. E. Canby, and J. Tesic, "Experimentation and analysis of ensemble deep learning in iot applications," OJIOT, vol. 5, 2019, pp. 133–149.

[76] A. L. Golande, P. Sorte, V. A. Suryawanshi, U. Yermalkar, and S. Satpute, "Smart hospital for heart disease prediction using iot," 2019.

[77] C. Kamienski et al., "Smart water management platform: Iot-based precision irrigation for agriculture ," Sensors (Basel, Switzerland), vol. 19, 2019.

[78] X. Yuan and M. Elhoseny, "Intelligent data aggregation inspired paradigm and approaches in iot applications," Journal of Intelligent and Fuzzy Systems, vol. 37, 2019, pp. 3–7.

[79] E. Jovanov, "Wearables meet iot: Synergistic personal area networks (spans)," Sensors (Basel, Switzerland), vol. 19, 2019.

[80] C. Robberts and J. Toft, "Finding vulnerabilities in iot devices : Ethical hacking of electronic locks," 2019.

[81] J. Lee, S. Yu, K. Park, Y. Park, and Y. Park, "Secure three-factor authentication protocol for multi-gateway iot environments," Sensors (Basel, Switzerland), vol. 19, 2019.

[82] S. Ghosh, R. Misoczki, and M. R. Sastry, "Lightweight post-quantum-secure digital signature approach for iot motes," IACR Cryptology ePrint Archive, vol. 2019, 2019, p. 122.

[83] M. U. Ali, S. Hur, and Y. Park, "Wi-fi-based effortless indoor positioning system using iot sensors," Sensors (Basel, Switzerland), vol. 19, 2019.

[84] D. Stiawan et al., "Investigating brute force attack patterns in iot network," J. Electrical and Computer Engineering, vol. 2019, 2019, pp. 4 568 368:1–4 568 368:13.

[85] S. Sidhu, B. J. Mohd, and T. Hayajneh, "Hardware security in iot devices with emphasis on hardware trojans," J. Sensor and Actuator Networks, vol. 8, 2019, p. 42.

[86] F. Chiti, R. Fantacci, and L. Pierucci, "Energy efficient communications for reliable iot multicast 5g/satellite services," Future Internet, vol. 11, 2019, p. 164.

[87] Y. Pu et al., "Two secure privacy-preserving data aggregation schemes for iot," Wireless Communications and Mobile Computing, vol. 2019, 2019, pp. 3 985 232:1–3 985 232:11.

[88] D. Dinculeana and X. Cheng, "Vulnerabilities and limitations of mqtt protocol used between iot devices," Applied Sciences, vol. 9, 2019, p. 848.

[89] N. Mora et al., "Iot-based home monitoring: Supporting practitioners assessment by behavioral analysis," Sensors (Basel, Switzerland), vol. 19, 2019.

[90] F. Kamaruddin et al., "Iot-based intelligent irrigation management and monitoring system using arduino," TELKOMNIKA Telecommunication Computing Electronics and Control, vol. 17, 2019, pp. 2378–2388.

[91] H. Alaiz-Moretón et al., "Multiclass classification procedure for detecting attacks on mqtt-iot protocol," Complexity, vol. 2019, 2019, pp. 6 516 253:1–6 516 253:11.

[92] M. Khapne and N. A. Chavhan, "Secured and reliable urban area applications based on iot," International Journal of Scientific Research in Science and Technology, vol. 6, 2019, pp. 701–703.

[93] K. Jung, J. Gascon-Samson, and K. Pattabiraman, "Oneos: Iot platform based on posix and actors," in HotEdge, 2019.

[94] B. Mataloto, J. Ferreira, and N. Cruz, "Lobemsiot for building and energy management systems," Electronics, vol. 8, 2019, pp. 1–27.

 ISBN: 978-1-61208-778-8

[95] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," Sensors (Basel, Switzerland), vol. 19, 2019.

[96] M. P. Doan, V. T. Tran, H. H. Huynh, and H. X. Huynh, "A scalable iot video data analytics for smart cities," EAI Endorsed Trans. Context-aware Syst. and Appl., vol. 6, 2019, p. e3.

[97] S. Janakiraman, S. Rajagopalan, and R. Amirtharajan, "Reliable medical image communication in healthcare iot: Watermark for authentication," 2019.

[98] H. He, Y. Zhang, and S. Wang, "Design of intelligent meter reading technology based on nb-iot," 2019.

[99] A. F. Santamaria, P. Raimondo, M. Tropea, F. D. Rango, and C. Aiello, "An iot surveillance system based on a decentralised architecture," Sensors (Basel, Switzerland), vol. 19, 2019.

[100] M. Chanson, A. Bogner, D. Bilgeri, E. Fleisch, and F. Wortmann, "Blockchain for the iot: Privacy-preserving protection of sensor data," J. AIS, vol. 20, 2019, p. 10.

[101] C. Akasiadis, V. Pitsilis, and C. D. Spyropoulos, "A multi-protocol iot platform based on open-source frameworks," Sensors (Basel, Switzerland), vol. 19, 2019.

[102] J. Rubio-Aparicio, F. Cerdan-Cartagena, J. S. Muro, and J. Ybarra-Moreno, "Design and implementation of a mixed iot lpwan network architecture," Sensors (Basel, Switzerland), vol. 19, 2019.

[103] Y. Kortesniemi, D. Lagutin, T. Elo, and N. Fotiou, "Improving the privacy of iot with decentralised identifiers (dids)," Journal Comp. Netw. and Communic., vol. 2019, 2019, pp. 8 706 760:1–8 706 760:10.

[104] C. Arbib, D. Arcelli, J. Dugdale, M. T. Moghaddam, and H. Muccini, "Real-time emergency response through performant iot architectures," in ISCRAM, 2019.

[105] Y. Wang et al., "Modeling and building iot data platforms with actor-oriented databases," in EDBT, 2019.

[106] M. Nekrasov, R. Allen, I. Artamonova, and E. M. Belding-Royer, "Optimizing 802.15.4 outdoor iot sensor networks for aerial data collection," Sensors (Basel, Switzerland), vol. 19, 2019.

[107] J.-N. Luo and M.-H. Yang, "An improved single packet traceback scheme for iot devices," Journal of Internet Technology, vol. 20, 2019, pp. 887–901.

[108] E. Manavalan and K. Jayakrishna, "A review of internet of things (iot) embedded sustainable supply chain for industry 4.0 requirements," Computers & Industrial Engineering, vol. 127, 2019, pp. 925–953.

[109] H. Kortelainen et al., "Beyond iot business," 2019.

[110] CYBER, "EN 303 645 - V2.1.1 - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements," European Telecommunications Standards Institute, Jun. 2020, p. 10.

 ISBN: 978-1-61208-778-8