Fraunhofer AISEC

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

A Study about the Different Categories of IoT in Scientific Publications

Sebastian Fischer (Fraunhofer AISEC)
Katrin Neubauer (OTH Regensburg)
Prof. Dr. Rudolf Hackenberg (OTH Regensburg)

CLOUD COMPUTING 2020 - October 25, 2020 to October 29, 2020 - Nice, France

Sebastian Fischer

2020	Chair and Coordinator of Special Track NCSIoT at IARIA CLOUD COMPUTING 2020
2018 - present	Fraunhofer AISEC
2015 - present	PhD candiate at FU Berlin
2015	M. Sc. Applied Research in Computer Science, OTH Regensburg
2013	B. Sc. Computer Science, OTH Regensburg

sebastian.fischer@aisec.fraunhofer.de

Research topics

- Internet of Things Security
  - Minimum Security Requirements
  - Device identification
  - …
- Cybersecurity with AI
- IT Security

Internet of Things (IoT)

- Very broad definition
- IoT 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]
- Not clear which products are included
- Consumer / Industrial / Enterprise products?
- Cars? Planes? …

Searching in Research Libraries

- Springer Link, IEEE Xplore, ScienceDirect, ACM digital library, Google Scholar, Semantic Scholar
- Started with “iot” and after analysing the results, added some terms to categorise IoT
- The three terms are the most common ones:
  - Industrial
  - Consumer
  - Enterprise

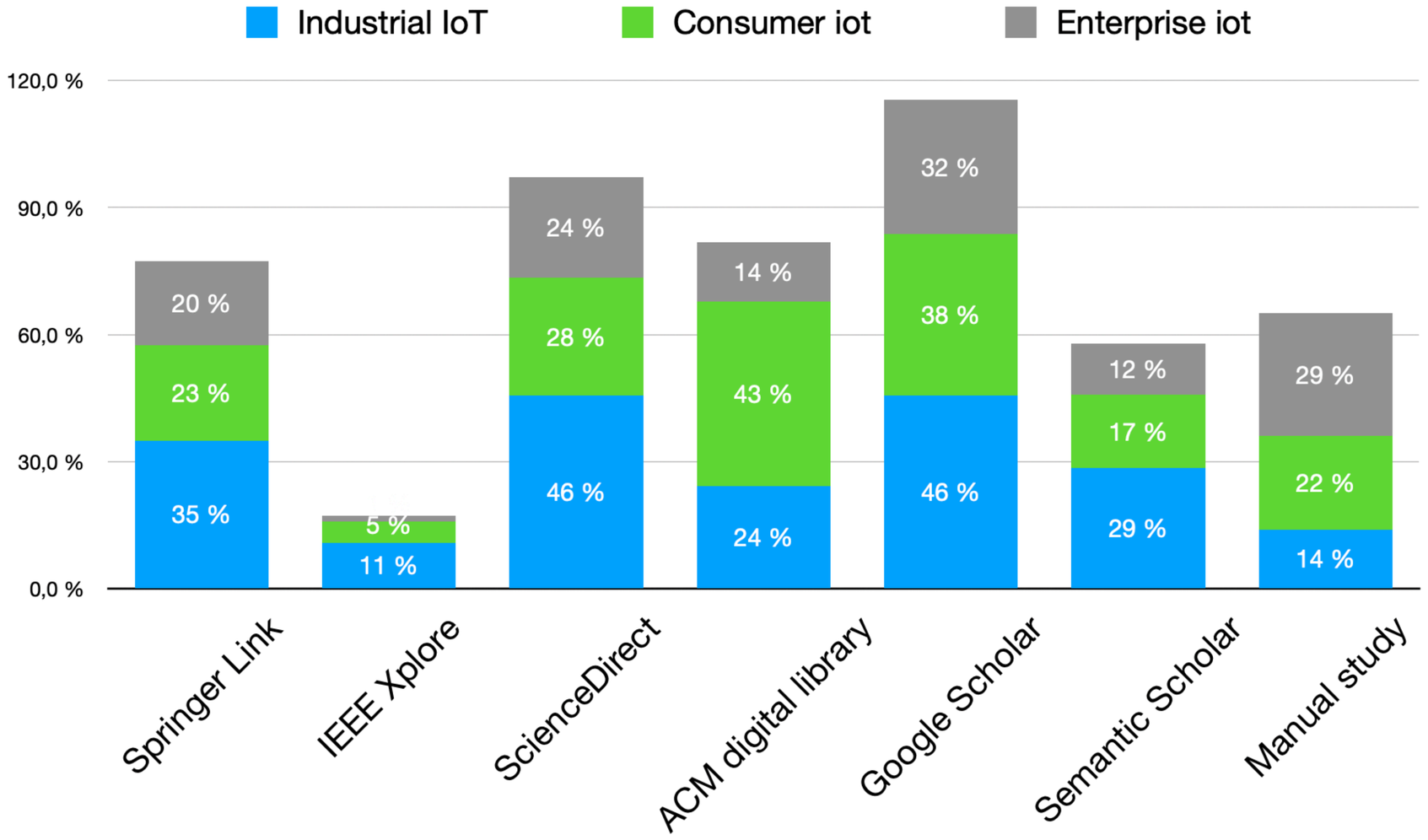
TABLE I. NUMBER OF RESULTS PER SEARCH QUERY

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 %

Percentage of the terms



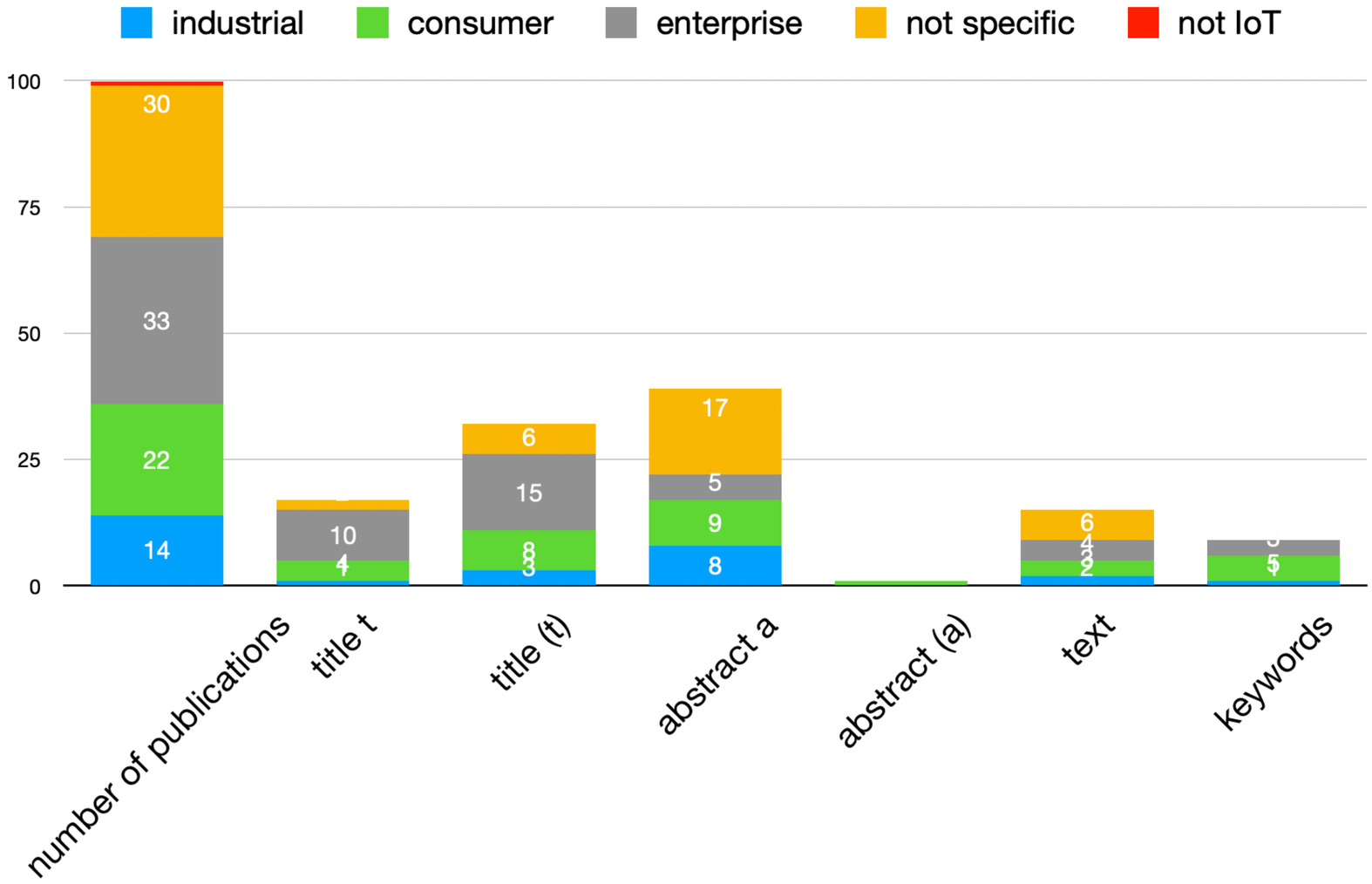
Results

- Different search strategies of the research libraries
  - e.g., Google finds the same publications for more than one category
  - IEEE Xplore does not include the whole publication text for searching
  - etc.
- You need to choose the right term and library for your research

Manual study of 100 publications

- Semantic Scholar with “iot”, Language: English, Publication date: 2019 and 2020, Option: ”has PDF”, Sort by Relevance
- First 100 publications are used to analyse (the full text)
- Manual categorisation to Industrial, Consumer and Enterprise
- Additional information, how much text is needed to find the right category (Category can be determined by the keywords, the title, in the abstract or only by reading the paper text)

Results


industrial
consumer
enterprise
not specific
not IoT
100
75
50
25
0
30
33
22
14
10
4
6
15
8
3
17
5
9
8
6
4
3
2
number of publications
title t
title (t)
abstract a
abstract (a)
text
keywords

Results

- Not easy to tell the category of IoT without reading the abstract
- Often, no useful keywords are given
- It's difficult, for example, to get all the research for consumer IoT products, because no category keywords are provided and you have to search for "wearable", "light bulb", "smart tv", etc.
- Not the same results as any of the search engines
- Some publications use more than one category in their text (this leads to wrong search results)

Summary

- IoT as term is too broad
- Limited study, but it shows the differences in searching in research libraries
- No clear usage of categorisations in nearly all publications (not in the keywords and even often not in the whole publication)
- Future work: we are trying to find suitable categories for IoT

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 en- forcement 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 interoper- ability 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," An- nals 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.

References

[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. Schla¨pfer and A. Ru¨st, “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 com- pression for cellular iot,” 2019.
[33] Ragula, “Waste management in iot-enabled smart cities,” 2019.
[34] L. No´brega, 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 Con- trol, 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.
[46] W. Ejaz, M. A. Azam, S. Saadat, F. Iqbal, and A. Hanan, “Unmanned aerial vehicles enabled iot platform for disaster management,” Ener- gies, vol. 12, 2019, p. 2706.
[47] N. Kherraf, “Provisioning of edge computing resources for heteroge- neous iot workload,” 2019.
[48] A. Ma´rkus and J. Dombi, “Multi-cloud management strategies for simulating iot applications,” Acta Cybernetica, vol. 24, 2019, pp. 83– 103.
[49] I. Sitto´ n-Candanedo, R. S. Alonso, O.
[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, Switzer- land), vol. 19, 2019.

References

[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 collab- orative 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 classifi- cation for supporting intelligent iot applications,” Electronics, vol. 8, 2019, p. 164.
[62] H. M. A. Islam, D. Lagutin, A. Yla¨-Ja¨a¨ski, 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. Soe- wito, “Iot system for sleep quality monitoring using ballistocardiogra- phy 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-Gonza´lez, “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 distil- lation 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, “Man- agement 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.

References

[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 position- ing 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 communica- tions 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 Telecommunica- tion Computing Electronics and Control, vol. 17, 2019, pp. 2378–2388.
[91] H. Alaiz-Moreto´n et al., “Multiclass classification procedure for de- tecting 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.
Garc´ıa, L.
S. Rodr´ıguez, “Edge computing, iot and social computing in smart
energy scenarios,” Sensors (Basel, Switzerland), vol. 19, 2019.
[94] B. Mataloto, J. Ferreira, and N. Cruz, “Lobemsiot for building and energy management systems,” Electronics, vol. 8, 2019, pp. 1–27.
[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 med- ical image communication in healthcare iot: Watermark for authenti- cation,” 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.

References

[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, Switzer- land), 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.