Towards a Systematic Survey of Industrial IoT Security Requirements: Research Method and Quantitative Analysis

Koen Tange, Michele De Donno, Xenofon Fafoutis
kpta@dtu.dk,mido@dtu.dk,xefa@dtu.dk
Technical University of Denmark

Nicola Dragoni
ndra@dtu.dk
Technical University of Denmark and
AASS, Örebro University

ABSTRACT

Industry 4.0 and, in particular, Industrial Internet of Things (IIoT) represent two of the major automation and data exchange trends of the 21^{st} century, driving a steady increase in the number of smart embedded devices used by industrial applications. However, IoT devices suffer from numerous security flaws, resulting in a number of large scale cyber-attacks. In this light, Fog computing, a relatively new paradigm born from the necessity of bridging the gap between Cloud computing and IoT, can be used as a security solution for the IIoT. To achieve this, the first step is to clearly identify the security requirements of the IIoT that can be subsequently used to design security solutions based on Fog computing. With this in mind, our paper represents a preliminary work towards a systematic literature review of IIoT security requirements. We focus on two key steps of the review: (1) the research method that will be used in the systematic work and (2) a quantitative analysis of the results produced by the study selection process. This lays the necessary foundations to enable the use of Fog computing as a security solution for the IIoT.

CCS CONCEPTS

• **Security and privacy**; • **Computer systems organization** → **Embedded and cyber-physical systems**; Real-time systems; Real-time system architecture; • **General and reference** → *Surveys and overviews*;

KEYWORDS

Industrial Internet of Things, IIoT, Industry 4.0, Security, Fog Computing, Systematic Literature Review

ACM Reference Format:
Koen Tange, Michele De Donno, Xenofon Fafoutis and Nicola Dragoni. 2019. Towards a Systematic Survey of Industrial IoT Security Requirements: Research Method and Quantitative Analysis. In *Workshop on Fog Computing and the IoT (IoT-Fog '19), April 15–18, 2019, Montreal, QC, Canada.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3313150.3313228

IoT-Fog '19, April 15–18, 2019, Montreal, QC, Canada

ACM ISBN 978-1-4503-6698-4/19/04…$15.00
https://doi.org/10.1145/3313150.3313228

1 INTRODUCTION

Today, we are living in the 4^{th} industrial revolution, also referred to as Industry 4.0. Due to the increasing availability, affordability, and proficiency of sensors, processors, and Wireless Sensor Network (WSN) technologies, the number of embedded devices used in industrial applications is steadily increasing. This leads to a growth in the interest for the Industrial Internet of Things (IIoT), a large network of devices, systems, and applications communicating and sharing intelligence with each other, the external environment, and with humans [30]. According to Accenture [30], the IIoT could be worth 7.1 trillion US dollars to the United States and more than 1.2 trillion to Europe by 2030.

In this wave of excitement, IoT security represents one of the biggest weak points holding back the adoption of the IIoT. As a matter of fact, IoT devices are often poorly secured [34] and thus easy targets for malware taking advantage of them to run devastating cyber attacks, such as Distributed Denial of Service (DDoS) [31] (e.g., Mirai [32]) or sabotage attacks (e.g., StuxNet [66], CrashOverride/Industroyer [68]).

In this scenario, a relatively new computing paradigm has attracted attention: Fog computing [18]. Fog computing is a system-level architecture born from the necessity of bridging the gap between IoT and Cloud computing, by distributing resources and services along the continuum from Cloud to IoT [96]. Among others, one of the promises of Fog computing is to present a possible solution to the IoT security problem.

The first step for improving security of the IIoT is to clearly define its main security requirements. To the best of our knowledge, the last surveys discussing security requirements of the IIoT date back to 2015 and 2016 [102, 103]. However, as we show later in this paper, the field has grown exponentially since then. Thus, we believe that a systematic and up-to-date survey on the security requirements of IIoT is becoming a necessity.

1.1 Contribution of the Paper

In this paper, we present a preliminary study towards a systematic literature review work that aims at identifying security requirements of the IIoT.

Systematic studies are meant to give an overview of a research area, following a structured methodology with respect to searching and study selection [98]. An essential part of a systematic literature review consists of defining the research method adopted to select relevant studies that are later used to extract qualitative results on the topic. In the paper, we focus on this methodological phase of the systematical literature review and we provide a quantitative analysis of the output produced by the research so far. Thus, the

paper can be considered as the first step towards a complete systematic literature review work, in which the selected papers will be used to extract qualitative results about security requirements in the IIoT. Once the requirements are delineated, it will be possible to focus on how Fog computing can meet them.

1.2 Outline of the Paper

The paper is organized as follows. Section 2 briefly mentions related work and motivates the need for a systematic review. Section 3 describes the research method used. Section 4 presents a quantitative analysis of the results obtained during the research phase. Section 5 concludes the paper.

2 RELATED WORK

To the best of our knowledge, the most recent work focused on reviewing IIoT security is [74], where the focus lies on threat characterization by looking at existing attacks. However, this work does not explicitly discuss security requirements, opting to leave them as implied by the described threats.

Another recent study [46] focuses on Industry 4.0 system architecture as a whole and observes that there is an increase in security-focused architectural proposals, but does not discuss security in depth.

Some older surveys dated back to 2015 and 2016 also mention IIoT security requirements [102, 103], but they refrain from discussing such requirements in-depth.

3 RESEARCH METHOD

In this section, we present the research method that will be used in the systematic literature review on security requirements for the IIoT that will extend this work.

We adopt the research method detailed by Petersen et al. [98], and utilize the suggested template for describing our approach. In the next subsections, we elaborate on research questions, search strategy, study selection, and validity concerns.

3.1 Research Questions

The main aim of this work is to identify security requirements for the IIoT. Our end goal is to investigate which ones can be solved by Fog computing. In addition, we want to provide an overview of the research activity in the field: how research activity has developed throughout the years, how this research was published, and what its geographical distribution is.

Thus, our research questions can be formulated as follows:

- **RQ1:** how are publications related to IIoT security spread throughout the years?
- **RQ2:** how is IIoT security research activity geographically distributed?
- **RQ3:** what are the most popular publication venues for IIoT security research?
- **RQ4:** what are the security requirements of the IIoT?
- **RQ5:** which of these security requirements can be solved by Fog computing?

Note that RQ4 and RQ5 are questions we aim to answer in our completed study, so they are not discussed in this preliminary work.

Answering these questions will aid in getting a better understanding of the current security landscape for the IIoT, while at the same time identifying various concrete research opportunities related to security for Fog computing. Each of these can then be traced back to concrete security requirements relevant to the Industry 4.0 paradigm.

3.2 Search Strategy

We utilize the adjusted PICOC criteria for software engineering [60] in order to identify relevant keywords. In particular:

- **Population:** we consider the IIoT as the application area in which our research is conducted. However, this is a very broad population, therefore, we take into account only studies addressing IIoT security.
- **Intervention:** this criterion does not apply to our research questions, as we are interested in *any* work in the IIoT domain that describes security requirements.
- **Comparison:** we compare the security requirements identified by different studies by taking into account such factors as the number of studies that mention them, related threats, and proposed solutions.
- **Outcomes:** we present the identified security requirements as well as the properties of their mitigation, allowing us to discuss which requirements call for further research.
- **Context:** As we do not empirically compare the available works, this criterion does not apply to our study.

With these criteria in mind, we have formulated the following keywords: *IIoT, Industrial Internet of Things, Industry 4.0,* and *security*.

We considered as sources the following databases: ACM Digital Library, IEEE Xplore, Elsevier/ScienceDirect. In this domain, we believe that the combination of these three sources provides an accurate representation of the research that has been conducted globally.

We divided the search into two stages. First, we queried the databases for articles related to IIoT/Industry 4.0 in general, based on their titles. This provided an overview of the amount of research conducted in this field. After that, we narrowed down our search to only include works related to security, by excluding articles not containing the word "security" in their abstract. The queries are summarized in Table 1. The search results for both queries are listed in Table 2.

3.3 Study Selection

The study selection process was done in multiple phases. Firstly, the JabRef [1] reference management software was used to identify and delete duplicates. Two duplicates were found, leaving the number of considered papers for the subsequent phases at 173.

In the second phase, we independently reviewed titles and abstracts of each article in order to reduce selection bias. Each article

[1] https://www.jabref.org

Table 1: Queries used for our search, expressed in pseudo-code

Query	Description
Q1	*in title:* IIoT OR "Industrial Internet of Things" OR "Industry 4.0"
Q2	(*in title:* IIoT OR "Industrial Internet of Things" OR "Industry 4.0") AND *in abstract:* security

Table 2: Number of papers returned from our queries

Source	Q1	Q2
ACM	36	6
IEEE Xplore	1462	160
Scopus	219	9
Total	1717	175

was marked as being relevant, not relevant, or of doubtful relevance. Articles were voted for inclusion when the work covers cyber-security challenges and/or solutions for Industry 4.0, and it was published before 2019, since that is the year in which this study is conducted. Articles were voted for exclusion when the work was not related to Industry 4.0 security, a duplicate, or was not presented in legible English.

The following rules were used for filtering out articles based on title and abstract review (this has been done jointly by two authors of the paper):

- when both authors considered an article relevant, the article was included for the next phase;
- when one author expressed doubt and the other author considered an article relevant, the article was included for the next phase;
- when both authors expressed doubt, a joint review was done considering also other sections of the article (e.g. introduction, outline, conclusion) in order to determine its relevance. If this review did not clear up doubts for either of the authors, the article was given the benefit of the doubt and included for the next phase;
- when one author considered an article relevant, while the other considered it to not be relevant, the article was marked for joint review as described in the previous rule;
- when one author considered an article not relevant, while the other considered it to be doubtful, the article was marked for joint review as with the previous rules;
- when both authors considered an article not relevant, the article was excluded.

After the individual title and abstract reviews, 35 articles were excluded and 41 were marked as doubtful entries requiring a joint review. These were then jointly reviewed, leading to an additional 18 exclusions. The remaining 120 papers ([1–9, 11–17, 19–29, 33, 35–53, 55–59, 61–65, 67, 69–73, 75–95, 97, 99–102, 104–134]) were considered for full-text reading, overall reducing the number of papers to analyse by 93% compared to results of Q1 and 30% compared to Q2.

The next phase, consisting of reading the full text of each selected paper, is currently in progress. It is already clear that some articles are not relevant and will be excluded but, at present, we are unable to provide relevant numbers on this. During the full-text reading phase, we extract information relevant to the stated research questions, and use this to create a comprehensive picture of the security challenges and corresponding requirements for the IIoT.

3.4 Validity Evaluation

Every study that is subject to manual selection is vulnerable to researcher bias in the filtering process. In order to reduce this issue, we performed the filtering process twice: two authors of this paper selected studies independently, and the results of the filtering process were based on a systematic approach combining the selections of both authors, and in some cases a joint review.

Furthermore, we have described our research process in detail, and have taken care to list the criteria by which we have filtered studies. This is done to increase the repeatability of this work.

Finally, it is worth mentioning that our approach does not suffer from the Matthew's effect, as opposed to querying databases that rank papers based on citation count [10].

4 RESULTS

In this section, we provide a quantitative analysis of the set of studies resulting from the presented research method.

4.1 Spread of publications throughout the years (RQ1)

Figure 1 shows the number of publications between 2013 and 2018. Security research for the IIoT starts first appearing around 2013, growing slowly over the next 3 years. In 2017, a drastic increase in activity can be seen. One possible reason is that 2016 saw several serious IoT related security incidents (such as Mirai [32] and Crashoverride/Industroyer [68]), which served to illustrate the importance of security on these devices. In 2018, the growth in activity

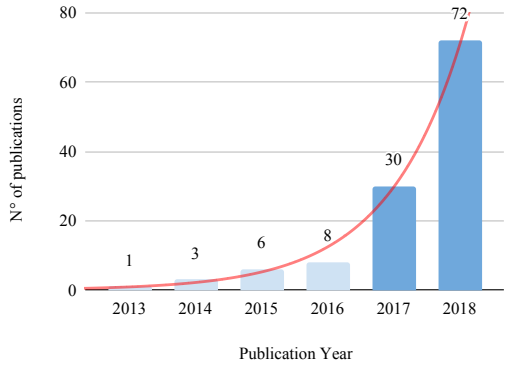

Figure 1: Number of publications per year

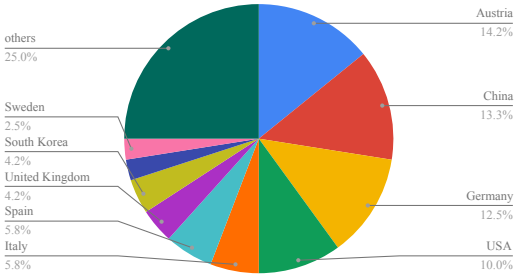

Figure 2: Demographic: geographical distribution of research activity based on first author country of affiliation

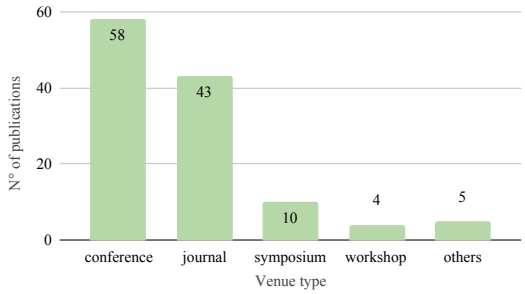

Figure 3: Popularity of different venue types

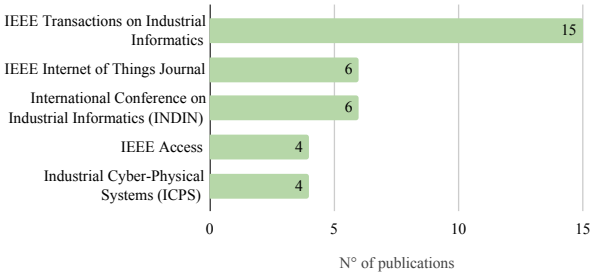

Figure 4: Popularity of different specific publication venues

continued, showing that the research community deems IIoT security to be of high importance.

4.2 Geographical Distribution of IIoT Security Research (RQ2)

The geographical distribution of research activity is shown in Figure 2. Data was obtained by extracting the country of affiliation of the first author of the considered studies.

German-speaking countries are strongly represented, making for a total of 26.7% of contributions. One possible explanation is that one of our search terms, *Industry 4.0*, was originally coined by the German government [54], thus, it might have seen higher adoption in German-speaking countries.

This raises the question of whether our search terms were successful in providing a good global sample of studies in this field. We believe they were, since the field we are considering is very narrow; we specifically searched for *Industrial* challenges in order to be able to extract security requirements unique to this field. However, we acknowledge that this might be a threat to the theoretical validity of our contribution that should be further investigated. We plan to address this issue in our future work, as stated in Section 5.

China and United States of America are the two other major contributors. This can possibly be attributed to the size of their industries and thus the relevance of research in this area. However, interestingly, 62.5% of the studies originate from Europe, showing that this topic is also regarded as highly relevant in countries with smaller industries.

The 'others' group consists of the 30 countries that have 2 or fewer publications in this field: France, Portugal, Czech Republic, Brazil, Australia, Greece, Belgium, Singapore, Ireland, Pakistan, Japan, Qatar, Turkey, Malaysia, Ukraine, Taiwan, Netherlands, Canada, Hungary, New Zealand, and Iran.

4.3 Venue Types for Publication (RQ3)

We have grouped the studies based on the venue type of their publication, which is shown in Figure 3. As can be seen, conference proceedings are the most popular dissemination method, followed by journals. The 'others' category consists of venue types in which 2 or fewer publications were published: congresses, summits, and forums.

Looking at the specific venues of publication (Figure 4), it can be seen that the IEEE Transactions on Industrial Informatics journal is by far the most popular venue, with 15 publications. One noteworthy observation here is that, out of all considered studies, only 5 were published in venues that were focused on security. The vast majority of IIoT security-related work appears to be published in venues targeting industrial systems or IoT instead.

5 CONCLUSION

In this preliminary study, we have described a systematic search and filtering of IIoT security studies, and laid the groundwork for extracting security requirements and putting them in a Fog computing perspective (RQ4 and RQ5). We also answered a number of questions about the IIoT security research domain itself, adding perspective to developments in this field. Of course, as in any mapping study, it is challenging to take all studies of the field into account, but it is more important to have a good representation of studies rather than a high number of studies [98].

Future work will be based on two phases. First, we will further improve the study selection by means of reverse snowball sampling. This will ensure that we end up with a good sample of relevant studies, mitigating bias that might have been introduced by the search terms. Second, we plan to address the remaining research questions, and provide a content review of the selected studies. We will use the extracted research requirements to discuss what research opportunities might exist within this field, as well as discussing the role that can be played by Fog computing as a security solution for the IIoT.

ACKNOWLEDGMENTS

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 764785, FORA – Fog computing for Robotics and Industrial Automation.

REFERENCES

[1] M. Aazam, S. Zeadally, and K. A. Harras. 2018. Deploying Fog Computing in Industrial Internet of Things and Industry 4.0. *IEEE Transactions on Industrial Informatics* 14, 10 (2018), 4674–4682. https://doi.org/10.1109/TII.2018.2855198

[2] D. Airehrour, J. Gutierrez, and S. K. Ray. 2016. Securing RPL routing protocol from blackhole attacks using a trust-based mechanism. In *2016 26th International Telecommunication Networks and Applications Conference (ITNAC)*. IEEE, 115–120. https://doi.org/10.1109/ATNAC.2016.7878793

[3] R. Al-Ali, R. Heinrich, P. Hnetynka, A. Juan-Verdejo, S. Seifermann, and M. Walter. 2018. Modeling of Dynamic Trust Contracts for Industry 4.0 Systems. In *Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings (ECSA '18)*. ACM, Article 45, 4 pages. https://doi.org/10.1145/3241403.3241450

[4] F. Al-Turjman and S. Alturjman. 2018. Context-Sensitive Access in Industrial Internet of Things (IIoT) Healthcare Applications. *IEEE Transactions on Industrial Informatics* 14, 6 (2018), 2736–2744. https://doi.org/10.1109/TII.2018.2808190

[5] P. Autenrieth, C. Lörcher, C. Pfeiffer, T. Winkens, and L. Martin. 2018. Current Significance of IT-Infrastructure Enabling Industry 4.0 in Large Companies. In *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. IEEE, 1–8. https://doi.org/10.1109/ICE.2018.8436244

[6] Z. Bakhshi, A. Balador, and J. Mustafa. 2018. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 173–178. https://doi.org/10.1109/WCNCW.2018.8368997

[7] N.C. Batista, R. Melício, and V.M.F. Mendes. 2017. Services enabler architecture for smart grid and smart living services providers under industry 4.0. *Energy and Buildings* 141 (2017), 16–27. https://doi.org/10.1016/j.enbuild.2017.02.039

[8] E. Bauer, O. Schluga, S. Maksuti, A. Bicaku, D. Hofbauer, I. Ivkic, M. G. Tauber, and A. Wöhrer. 2017. Towards a security baseline for IaaS-cloud back-ends in Industry 4.0. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 427–432. https://doi.org/10.23919/ICITST.2017.8356438

[9] A. Bécue, Y. Fourastier, I. Praça, A. Savarit, C. Baron, B. Gradussofs, E. Pouille, and C. Thomas. 2018. CyberFactory#1 — Securing the industry 4.0 with cyber-ranges and digital twins. In *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*. IEEE, 1–4. https://doi.org/10.1109/WFCS.2018.8402377

[10] J. Beel and B. Gipp. 2009. Google Scholar's Ranking Algorithm: An Introductory Overview. In *Proceedings of the 12th International Conference on Scientometrics and Informetrics (ISSIâĂŹ09*. Springer, 439–446.

[11] M. Beltrán, M. Calvo, and S. González. 2017. Federated system-to-service authentication and authorization combining PUFs and tokens. In *2017 12th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC)*. IEEE, 1–8. https://doi.org/10.1109/ReCoSoC.2017.8016157

[12] N. Benias and A. P. Markopoulos. 2017. A review on the readiness level and cyber-security challenges in Industry 4.0. In *2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*. IEEE, 1–5. https://doi.org/10.23919/SEEDA-CECNSM.2017.8088234

[13] A. Bicaku, S. Maksuti, S. Palkovits-Rauter, M. Tauber, R. Matischek, C. Schmittner, G. Mantas, M. Thron, and J. Delsing. 2017. Towards trustworthy end-to-end communication in industry 4.0. In *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*. IEEE, 889–896. https://doi.org/10.1109/INDIN.2017.8104889

[14] A. Bicaku, C. Schmittner, M. Tauber, and J. Delsing. 2018. Monitoring Industry 4.0 applications for security and safety standard compliance. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 749–754. https://doi.org/10.1109/ICPHYS.2018.8390801

[15] S. Blanch-Torné, F. Cores, and R. M. Chiral. 2015. Agent-based PKI for Distributed Control System. In *2015 World Congress on Industrial Control Systems Security (WCICSS)*. IEEE, 28–35. https://doi.org/10.1109/WCICSS.2015.7420319

[16] G. Bloom, B. Alsulami, E. Nwafor, and I. C. Bertolotti. 2018. Design patterns for the industrial Internet of Things. In *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*. IEEE, 1–10. https://doi.org/10.1109/WFCS.2018.8402353

[17] A. Bluschke, W. Bueschel, M. Hohmuth, F. Jehring, R. Kaminski, K. Klamka, S. Koepsell, A. Lackorzynski, T. Lackorzynski, M. Matthews, P. Rietzsch, A. Senier, P. Sieber, V. Ulrich, R. Wiggers, and J. Wolter. 2018. fastvpn - Secure and Flexible Networking for Industry 4.0. In *Broadband Coverage in Germany; 12th ITG-Symposium*. VDE, 1–8. https://imld.de/en/research/research-projects/fastvpn/

[18] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli. 2012. Fog Computing and Its Role in the Internet of Things. In *Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing (MCC '12)*. ACM, 13–16. https://doi.org/10.1145/2342509.2342513

[19] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson. 2018. The industrial internet of things (IIoT): An analysis framework. *Computers in Industry* 101 (2018), 1–12. https://doi.org/10.1016/j.compind.2018.04.015

[20] R. Chaturvedi. 2017. UL testing standards to mitigate cybersecurity risk ~ UL's approach with complement to the other standards for SICE 2017. In *2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*. IEEE, 728–730. https://doi.org/10.23919/SICE.2017.8105618

[21] M. Cheminod, L. Durante, L. Seno, F. Valenza, A. Valenzano, and C. Zunino. 2017. Leveraging SDN to improve security in industrial networks. In *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*. IEEE, 1–7. https://doi.org/10.1109/WFCS.2017.7991960

[22] G. Chen and W. S. Ng. 2017. An efficient authorization framework for securing industrial Internet of Things. In *TENCON 2017 - 2017 IEEE Region 10 Conference*. IEEE, 1219–1224. https://doi.org/10.1109/TENCON.2017.8228043

[23] M. Chen, Y. Miao, Y. Hao, and K. Hwang. 2017. Narrow Band Internet of Things. *IEEE Access* 5 (2017), 20557–20577. https://doi.org/10.1109/ACCESS.2017.2751586

[24] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. A. Faruque. 2017. Security Trends and Advances in Manufacturing Systems in the Era of Industry 4.0. In *Proceedings of the 36th International Conference on Computer-Aided Design (ICCAD '17)*. IEEE Press, 1039–1046. https://doi.org/10.1109/ICCAD.2017.8203896

[25] K. R. Choo, S. Gritzalis, and J. H. Park. 2018. Cryptographic Solutions for Industrial Internet-of-Things: Research Challenges and Opportunities. *IEEE Transactions on Industrial Informatics* 14, 8 (2018), 3567–3569. https://doi.org/10.1109/TII.2018.2841049

[26] M. W. Condry and C. B. Nelson. 2016. Using Smart Edge IoT Devices for Safer, Rapid Response With Industry IoT Control Operations. *Proc. IEEE* 104, 5 (2016), 938–946. https://doi.org/10.1109/JPROC.2015.2513672

[27] H. Cui, R. H. Deng, J. K. Liu, X. Yi, and Y. Li. 2018. Server-Aided Attribute-Based Signature With Revocation for Resource-Constrained Industrial-Internet-of-Things Devices. *IEEE Transactions on Industrial Informatics* 14, 8 (2018), 3724–3732. https://doi.org/10.1109/TII.2018.2813304

[28] B. Czybik, S. Hausmann, S. Heiss, and J. Jasperneite. 2013. Performance evaluation of MAC algorithms for real-time Ethernet communication systems. In *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*. IEEE, 676–681. https://doi.org/10.1109/INDIN.2013.6622965

[29] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues. 2018. Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment. *IEEE Internet of Things Journal* 5, 6 (2018), 4900–4913. https://doi.org/10.1109/JIOT.2018.2877690

[30] P. Daugherty and B. Berthon. 2015. *Winning with the Industrial Internet of Things: How to Accelerate the Journey to Productivity and Growth*. Technical Report. Dublín: Accenture.

[31] Michele De Donno, Nicola Dragoni, Alberto Giaretta, and Angelo Spognardi. 2017. Analysis of DDoS-Sapable IoT Malwares. In *Federated Conference on Computer Science and Information Systems (FedCSIS)*. IEEE, 807–816.

[32] Michele De Donno, Nicola Dragoni, Alberto Giaretta, and Angelo Spognardi. 2018. DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. *Security and Communication Networks* 2018 (2018).

[33] J. Delsing. 2017. Local Cloud Internet of Things Automation: Technology and Business Model Features of Distributed Internet of Things Automation Solutions. *IEEE Industrial Electronics Magazine* 11, 4 (2017), 8–21. https://doi.org/10.1109/MIE.2017.2759342

[34] Nicola Dragoni, Alberto Giaretta, and Manuel Mazzara. 2017. The Internet of Hackable Things. In *Proceedings of 5th International Conference in Software Engineering for Defence Applications*, Paolo Ciancarini, Stanislav Litvinov, Angelo Messina, Alberto Sillitti, and Giancarlo Succi (Eds.). Springer, 129–140.

[35] M. H. Eldefrawy, N. Pereira, and M. Gidlund. 2018. Key Distribution Protocol for Industrial Internet of Things without Implicit Certificates. *IEEE Internet of Things Journal* (2018). https://doi.org/10.1109/JIOT.2018.2865212 (early access).

[36] C. Esposito, A. Castiglione, F. Palmieri, and A. D. Santis. 2018. Integrity for an Event Notification Within the Industrial Internet of Things by Using Group Signatures. *IEEE Transactions on Industrial Informatics* 14, 8 (2018), 3669–3678. https://doi.org/10.1109/TII.2018.2791956

[37] G. Falco, C. Caldera, and H. Shrobe. 2018. IIoT Cybersecurity Risk Modeling for SCADA Systems. *IEEE Internet of Things Journal* 5, 6 (2018), 4486–4495. https://doi.org/10.1109/JIOT.2018.2822842

[38] X. Feng, J. Wu, J. Li, and S. Wang. 2018. Efficient Secure Access to IEEE 21451 Based Wireless IIoT Using Optimized TEDS and MIB. In *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 5221–5227. https://doi.org/10.1109/IECON.2018.8591182

[39] H. Flatt, S. Schriegel, J. Jasperneite, H. Trsek, and H. Adamczyk. 2016. Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements. In *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 1–4. https://doi.org/10.1109/ETFA.2016.7733634

[40] J. L. Flores and I. Mugarza. 2018. Runtime Vulnerability Discovery as a Service on Industrial Internet of Things (IIoT) Systems. In *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, Vol. 1. IEEE, 948–955. https://doi.org/10.1109/ETFA.2018.8502660

[41] F. Fraile, T. Tagawa, R. Poler, and A. Ortiz. 2018. Trustworthy Industrial IoT Gateways for Interoperability Platforms and Ecosystems. *IEEE Internet of Things Journal* 5, 6 (2018), 4506–4514. https://doi.org/10.1109/JIOT.2018.2832041

[42] J. Fu, Y. Liu, H. Chao, B. K. Bhargava, and Z. Zhang. 2018. Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing. *IEEE Transactions on Industrial Informatics* 14, 10 (2018), 4519–4528. https://doi.org/10.1109/TII.2018.2793350

[43] G. George and S. M. Thampi. 2018. A Graph-Based Security Framework for Securing Industrial IoT Networks From Vulnerability Exploitations. *IEEE Access* 6 (2018), 43586–43601. https://doi.org/10.1109/ACCESS.2018.2863244

[44] A. Hassanzadeh, S. Modi, and S. Mulchandani. 2015. Towards effective security control assignment in the Industrial Internet of Things. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, 795–800. https://doi.org/10.1109/WF-IoT.2015.7389155

[45] A. Hoeller and R. Toegl. 2018. Trusted Platform Modules in Cyber-Physical Systems: On the Interference Between Security and Dependability. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. IEEE, 136–144. https://doi.org/10.1109/EuroSPW.2018.00026

[46] F. Hofer. 2018. Architecture, Technologies and Challenges for Cyber-physical Systems in Industry 4.0: A Systematic Mapping Study. In *Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM '18)*. ACM, Article 1, 10 pages. https://doi.org/10.1145/3239235.3239242

[47] F. Hofer. 2018. Enhancing Security and Reliability for Smart- Systems' Architectures. In *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*. IEEE, 150–153. https://doi.org/10.1109/ISSREW.2018.000-8

[48] P. Hu. 2015. A System Architecture for Software-Defined Industrial Internet of Things. In *2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*. IEEE, 1–5. https://doi.org/10.1109/ICUWB.2015.7324414

[49] Y. Huang and W. Sun. 2018. An AHP-Based Risk Assessment for an Industrial IoT Cloud. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE, 637–638. https://doi.org/10.1109/QRS-C.2018.00112

[50] F. Januário, C. Carvalho, A. Cardoso, and P. Gil. 2016. Security challenges in SCADA systems over Wireless Sensor and Actuator Networks. In *2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. IEEE, 363–368. https://doi.org/10.1109/ICUMT.2016.7765386

[51] N. Jazdi. 2014. Cyber physical systems in the context of Industry 4.0. In *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*. IEEE, 1–4. https://doi.org/10.1109/AQTR.2014.6857843

[52] S. Jeong, W. Na, J. Kim, and S. Cho. 2018. Internet of Things for Smart Manufacturing System: Trust Issues in Resource Allocation. *IEEE Internet of Things Journal* 5, 6 (2018), 4418–4427. https://doi.org/10.1109/JIOT.2018.2814063

[53] P. Kadera and P. Novák. 2017. Performance Modeling Extension of Directory Facilitator for Enhancing Communication in FIPA-Compliant Multiagent Systems. *IEEE Transactions on Industrial Informatics* 13, 2 (2017), 688–695. https://doi.org/10.1109/TII.2016.2601918

[54] H. Kagermann, W. Wahlster, and J. Helbig. 2013. *Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0 – Securing the Future of German Manufacturing Industry*. Final Report of the Industrie 4.0 Working Group. acatech – National Academy of Science and Engineering, München. http://forschungsunion.de/pdf/industrie_4_0_final_report.pdf

[55] E. Kail, A. Banati, E. Lászlo, and M. Kozlovszky. 2018. Security Survey of Dedicated IoT Networks in the Unlicensed ISM Bands. In *2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. IEEE, 000449–000454. https://doi.org/10.1109/SACI.2018.8440945

[56] A. Karati, S. H. Islam, and M. Karuppiah. 2018. Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environments. *IEEE Transactions on Industrial Informatics* 14, 8 (2018), 3701–3711. https://doi.org/10.1109/TII.2018.2794991

[57] S. Katsikeas, K. Fysarakis, A. Miaoudakis, A. Van Bemten, I. Askoxylakis, I. Papaefstathiou, and A. Plemenos. 2017. Lightweight amp; secure industrial IoT communications via the MQ telemetry transport protocol. In *2017 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 1193–1200. https://doi.org/10.1109/ISCC.2017.8024687

[58] B. Kim and Y. Kang. 2018. Abnormal Traffic Detection Mechanism for Protecting IIoT Environments. In *2018 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 943–945. https://doi.org/10.1109/ICTC.2018.8539533

[59] Y. Kim, Y. Lee, and J. Kim. 2018. RIPPLE: Adaptive fine-grained access control in multi-hop LLNs. In *2018 International Conference on Information Networking (ICOIN)*. IEEE, 863–868. https://doi.org/10.1109/ICOIN.2018.8343245

[60] Barbara Kitchenham and Stuart Charters. 2007. *Guidelines for performing Systematic Literature Reviews in Software Engineering*. Technical Report EBSE-2007-01. EBSE Technical Report.

[61] T. Kobzan, S. Schriegel, S. Althoff, A. Boschmann, J. Otto, and J. Jasperneite. 2018. Secure and Time-sensitive Communication for Remote Process Control and Monitoring. In *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, Vol. 1. IEEE, 1105–1108. https://doi.org/10.1109/ETFA.2018.8502539

[62] K. K. Kolluru, C. Paniagua, J. van Deventer, J. Eliasson, J. Delsing, and R. J. DeLong. 2018. An AAA solution for securing industrial IoT devices using next generation access control. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 737–742. https://doi.org/10.1109/ICPHYS.2018.8390799

[63] F. Kurtz, C. Bektas, N. Dorsch, and C. Wietfeld. 2018. Network Slicing for Critical Communications in Shared 5G Infrastructures - An Empirical Evaluation. In *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*. IEEE, 393–399. https://doi.org/10.1109/NETSOFT.2018.8460110

[64] E. Laarouchi, D. Cancila, and H. Chaouchi. 2017. Safety and degraded mode in civilian applications of unmanned aerial systems. In *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*. IEEE, 1–7. https://doi.org/10.1109/DASC.2017.8102040

[65] M. Langfinger, M. Schneider, D. Stricker, and H. D. Schotten. 2017. Addressing security challenges in industrial augmented reality systems. In *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*. IEEE, 299–304. https://doi.org/10.1109/INDIN.2017.8104789

[66] R. Langner. 2011. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy* 9, 3 (2011), 49–51.

[67] A. Laszka, W. Abbas, Y. Vorobeychik, and X. Koutsoukos. 2018. Synergistic Security for the Industrial Internet of Things: Integrating Redundancy, Diversity, and Hardening. In *2018 IEEE International Conference on Industrial Internet (ICII)*. IEEE, 153–158. https://doi.org/10.1109/ICII.2018.00025

[68] R Lee. 2017. *CRASHOVERRIDE: Analysis of the threat to electric grid operations*. Technical Report. Dragos Inc.

[69] C. Lesjak, H. Bock, D. Hein, and M. Maritsch. 2016. Hardware-secured and transparent multi-stakeholder data exchange for industrial IoT. In *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*. IEEE, 706–713. https://doi.org/10.1109/INDIN.2016.7819251

[70] C. Lesjak, D. Hein, M. Hofmann, M. Maritsch, A. Aldrian, P. Priller, T. Ebner, T. Ruprechter, and G. Pregartner. 2015. Securing smart maintenance services: Hardware-security and TLS for MQTT. In *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*. IEEE, 1243–1250. https://doi.org/10.1109/INDIN.2015.7281913

[71] C. Lesjak, D. Hein, and J. Winter. 2015. Hardware-security technologies for industrial IoT: TrustZone and security controller. In *IECON 2015 - 41st Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 002589–002595. https://doi.org/10.1109/IECON.2015.7392493

[72] C. Lesjak, T. Ruprechter, H. Bock, J. Haid, and E. Brenner. 2014. ESTADO — Enabling smart services for industrial equipment through a secured, transparent and ad-hoc data transmission online. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*. IEEE, 171–177. https://doi.org/10.1109/ICITST.2014.7038800

[73] C. Lesjak, T. Ruprechter, J. Haid, H. Bock, and E. Brenner. 2014. A secure hardware module and system concept for local and remote industrial embedded system identification. In *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*. IEEE, 1–7. https://doi.org/10.1109/ETFA.2014.7005086

[74] Marianna Lezzi, Mariangela Lazoi, and Angelo Corallo. 2018. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry* 103 (2018), 97 – 110. https://doi.org/10.1016/j.compind.2018.09.004

[75] F. Li, J. Hong, and A. A. Omala. 2017. Efficient certificateless access control for industrial Internet of Things. *Future Generation Computer Systems* 76 (2017), 285–292. https://doi.org/10.1016/j.future.2016.12.036

[76] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari. 2018. A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics* 14, 8 (2018), 3599–3609. https://doi.org/10.1109/TII.2017.2773666

[77] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K. R. Choo. 2018. A Robust and Energy Efficient Authentication Protocol for Industrial Internet of Things. *IEEE Internet of Things Journal* 5, 3 (2018), 1606–1615. https://doi.org/10.1109/JIOT.2017.

2787800

[78] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang. 2018. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics* 14, 8 (2018), 3690–3700. https://doi.org/10.1109/TII.2017.2786307

[79] L. Liang, Y. Liu, Y. Yao, T. Yang, Y. Hu, and C. Ling. 2017. Security challenges and risk evaluation framework for industrial wireless sensor networks. In *2017 4th International Conference on Control, Decision and Information Technologies (CoDIT)*. IEEE, 0904–0907. https://doi.org/10.1109/CoDIT.2017.8102711

[80] C. Lin, D. He, X. Huang, K. R. Choo, and A. V. Vasilakos. 2018. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *Journal of Network and Computer Applications* 116 (2018), 42–52. https://doi.org/10.1016/j.jnca.2018.05.005

[81] M. Ma, D. He, N. Kumar, K. R. Choo, and J. Chen. 2018. Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics* 14, 2 (2018), 759–767. https://doi.org/10.1109/TII.2017.2703922

[82] Z. Ma, A. Hudic, A. Shaaban, and S. Plosz. 2017. Security Viewpoint in a Reference Architecture Model for Cyber-Physical Production Systems. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. IEEE, 153–159. https://doi.org/10.1109/EuroSPW.2017.65

[83] S. Maksuti, A. Bicaku, M. Tauber, S. Palkovits-Rauter, S. Haas, and J. Delsing. 2017. Towards flexible and secure end-to-end communication in industry 4.0. In *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*. IEEE, 883–888. https://doi.org/10.1109/INDIN.2017.8104888

[84] G. Marchetto, R. Sisto, J. Yusupov, and A. Ksentinit. 2018. Formally verified latency-aware VNF placement in industrial Internet of things. In *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*. IEEE, 1–9. https://doi.org/10.1109/WFCS.2018.8402355

[85] S. Marksteiner. 2018. Reasoning on Adopting OPC UA for an IoT-Enhanced Smart Energy System from a Security Perspective. In *2018 IEEE 20th Conference on Business Informatics (CBI)*, Vol. 02. IEEE, 140–143. https://doi.org/10.1109/CBI.2018.10060

[86] D. W. McKee, S. J. Clement, J. Almutairi, and J. Xu. 2017. Massive-Scale Automation in Cyber-Physical Systems: Vision amp;amp; Challenges. In *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*. IEEE, 5–11. https://doi.org/10.1109/ISADS.2017.56

[87] D. W. McKee, S. J. Clement, J. Almutairi, and J. Xu. 2018. Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems. *CAAI Transactions on Intelligence Technology* 3, 2 (2018), 75–82. https://doi.org/10.1049/trit.2018.0010

[88] A. Melis, D. Berardi, C. Contoli, F. Callegati, F. Esposito, and M. Prandini. 2018. A Policy Checker Approach for Secure Industrial SDN. In *2018 2nd Cyber Security in Networking Conference (CSNet)*. IEEE, 1–7. https://doi.org/10.1109/CSNET.2018.8602927

[89] H. Mouratidis and V. Diamantopoulou. 2018. A Security Analysis Method for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics* 14, 9 (2018), 4093–4100. https://doi.org/10.1109/TII.2018.2832853

[90] N. Moustafa, E. Adi, B. Turnbull, and J. Hu. 2018. A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems. *IEEE Access* 6 (2018), 32910–32924. https://doi.org/10.1109/ACCESS.2018.2844794

[91] J. Moyne, S. Mashiro, and D. Gross. 2018. Determining a security roadmap for the microelectronics industry. In *2018 29th Annual SEMI Advanced Semiconductor Manufacturing Conference (ASMC)*. IEEE, 291–294. https://doi.org/10.1109/ASMC.2018.8373213

[92] I. Mugarza, J. Parra, and E. Jacob. 2018. Cetratus: Towards a live patching supported runtime for mixed-criticality safe and secure systems. In *2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES)*. IEEE, 1–8. https://doi.org/10.1109/SIES.2018.8442088

[93] E. T. Nakamura and S. L. Ribeiro. 2018. A Privacy, Security, Safety, Resilience and Reliability Focused Risk Assessment Methodology for IIoT Systems Steps to Build and Use Secure IIoT Systems. In *2018 Global Internet of Things Summit (GIoTS)*. IEEE, 1–6. https://doi.org/10.1109/GIOTS.2018.8534521

[94] M. Niedermaier, F. Fischer, and A. von Bodisco. 2017. PropFuzz — An IT-security fuzzing framework for proprietary ICS protocols. In *2017 International Conference on Applied Electronics (AE)*. IEEE, 1–4. https://doi.org/10.23919/AE.2017.8053600

[95] P. O'Donovan, C. Gallagher, K. Bruton, and D. T.J. O'Sullivan. 2018. A fog computing industrial cyber-physical system for embedded low-latency machine learning Industry 4.0 applications. *Manufacturing Letters* 15 (2018), 139–142. https://doi.org/10.1016/j.mfglet.2018.01.005 Industry 4.0 and Smart Manufacturing.

[96] OpenFog Consortium Architecture Working Group and others. 2017. *OpenFog Reference architecture for Fog Computing*. Technical Report. OpenFog Consortium. https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf

[97] T. Pereira, L. Barreto, and A. Amaral. 2017. Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing* 13 (2017), 1253–1260. https://doi.org/10.1016/j.promfg.2017.09.047 Manufacturing Engineering Society International Conference 2017, MESIC 2017, 28-30 June 2017, Vigo (Pontevedra), Spain.

[98] K. Petersen, S. Vakkalanka, and L. Kuzniarz. 2015. Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology* 64 (2015), 1–18.

[99] D. Preuveneers, W. Joosen, and E. Ilie-Zudor. 2016. Data Protection Compliance Regulations and Implications for Smart Factories of the Future. In *2016 12th International Conference on Intelligent Environments (IE)*. IEEE, 40–47. https://doi.org/10.1109/IE.2016.15

[100] D. Preuveneers, W. Joosen, and E. Ilie-Zudor. 2017. Identity Management for Cyber-physical Production Workflows and Individualized Manufacturing in Industry 4.0. In *Proceedings of the Symposium on Applied Computing (SAC '17)*. ACM, 1452–1455. https://doi.org/10.1145/3019612.3019861

[101] P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu, and M. Huth. 2018. Economic impact of IoT cyber risk - Analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. In *Living in the Internet of Things: Cybersecurity of the IoT - 2018*. IET, 1–9. https://doi.org/10.1049/cp.2018.0003

[102] A. Sadeghi, C. Wachsmann, and M. Waidner. 2015. Security and Privacy Challenges in Industrial Internet of Things. In *Proceedings of the 52Nd Annual Design Automation Conference (DAC '15)*. ACM, Article 54, 6 pages. https://doi.org/10.1145/2744769.2747942

[103] A. Sajid, H. Abbas, and K. Saleem. 2016. Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges. *IEEE Access* 4 (2016), 1375–1384. https://doi.org/10.1109/ACCESS.2016.2549047

[104] C. Sandberg and B. Hunter. 2017. Cyber security primer for legacy process plant operation. In *2017 Petroleum and Chemical Industry Technical Conference (PCIC)*. IEEE, 97–102. https://doi.org/10.1109/PCICON.2017.8188728

[105] J. Schuette and G. S. Brost. 2018. LUCON: Data Flow Control for Message-Based IoT Systems. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 289–299. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00052

[106] A. Seitz, D. Henze, D. Miehle, B. Bruegge, J. Nickles, and M. Sauer. 2018. Fog Computing as Enabler for Blockchain-Based IIoT App Marketplaces - A Case Study. In *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*. IEEE, 182–188. https://doi.org/10.1109/IoTSMS.2018.8554484

[107] G. Settanni, F. Skopik, A. Karaj, M. Wurzenberger, and R. Fiedler. 2018. Protecting cyber physical production systems using anomaly detection to enable self-adaptation. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 173–180. https://doi.org/10.1109/ICPHYS.2018.8387655

[108] G. Shaabany and R. Anderl. 2018. Security by Design as an Approach to Design a Secure Industry 4.0-Capable Machine Enabling Online-Trading of Technology Data. In *2018 International Conference on System Science and Engineering (ICSSE)*. IEEE, 1–5. https://doi.org/10.1109/ICSSE.2018.8520195

[109] V. Sharma, G. Choudhary, Y. Ko, and I. You. 2018. Behavior and Vulnerability Assessment of Drones-Enabled Industrial Internet of Things (IIoT). *IEEE Access* 6 (2018), 43368–43383. https://doi.org/10.1109/ACCESS.2018.2856368

[110] L. Shu, M. Mukherjee, M. Pecht, N. Crespi, and S. N. Han. 2018. Challenges and Research Issues of Data Management in IoT for Large-Scale Petrochemical Plants. *IEEE Systems Journal* 12, 3 (2018), 2509–2523. https://doi.org/10.1109/JSYST.2017.2700268

[111] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund. 2018. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Transactions on Industrial Informatics* 14, 11 (2018), 4724–4734. https://doi.org/10.1109/TII.2018.2852491

[112] V. Sklyar and V. Kharchenko. 2017. Challenges in assurance case application for industrial IoT. In *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Vol. 2. IEEE, 736–739. https://doi.org/10.1109/IDAACS.2017.8095187

[113] Z. A. Solangi, Y. A. Solangi, S. Chandio, M. bt. S. Abd. Aziz, M. S. bin Hamzah, and A. Shah. 2018. The future of data privacy and security concerns in Internet of Things. In *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*. IEEE, 1–4. https://doi.org/10.1109/ICIRD.2018.8376320

[114] T. K. Sung. 2018. Industry 4.0: A Korea perspective. *Technological Forecasting and Social Change* 132 (2018), 40–45. https://doi.org/10.1016/j.techfore.2017.11.005

[115] M. Traub, H. Vögel, E. Sax, T. Streichert, and J. Härri. 2018. Digitalization in automotive and industrial systems. In *2018 Design, Automation Test in Europe Conference Exhibition (DATE)*. IEEE, 1203–1204. https://doi.org/10.23919/DATE.2018.8342198

[116] M. H. u. Rehman, E. Ahmed, I. Yaqoob, I. A. T. Hashem, M. Imran, and S. Ahmad. 2018. Big Data Analytics in Industrial IoT Using a Concentric Computing Model. *IEEE Communications Magazine* 56, 2 (2018), 37–43. https://doi.org/10.1109/

MCOM.2018.1700632

[117] T. Ulz, T. Pieber, C. Steger, S. Haas, H. Bock, and R. Matischek. 2017. Bring your own key for the industrial Internet of Things. In *2017 IEEE International Conference on Industrial Technology (ICIT)*. IEEE, 1430–1435. https://doi.org/10.1109/ICIT.2017.7915575

[118] T. Ulz, T. Pieber, C. Steger, S. Haas, and R. Matischek. 2018. Secured remote configuration approach for industrial cyber-physical systems. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 812–817. https://doi.org/10.1109/ICPHYS.2018.8390811

[119] B. van Lier. 2017. The industrial internet of things and cyber security: An ecological and systemic perspective on security in digital industrial ecosystems. In *2017 21st International Conference on System Theory, Control and Computing (ICSTCC)*. IEEE, 641–647. https://doi.org/10.1109/ICSTCC.2017.8107108

[120] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee. 2018. Access Control Policy Enforcement for Zero-Trust-Networking. In *2018 29th Irish Signals and Systems Conference (ISSC)*. IEEE, 1–6. https://doi.org/10.1109/ISSC.2018.8585365

[121] K. Wallis, F. Kemmer, E. Jastremskoj, and C. Reich. 2017. Adaption of a Privilege Management Infrastructure (PMI) Approach to Industry 4.0. In *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*. IEEE, 101–107. https://doi.org/10.1109/FiCloudW.2017.71

[122] K. Matthias Weber, Niklas Gudowsky, and Georg Aichholzer. 2018. Foresight and technology assessment for the Austrian parliament — Finding new ways of debating the future of industry 4.0. *Futures* (2018). https://doi.org/10.1016/j.futures.2018.06.018

[123] E. Weippl and P. Kieseberg. 2017. Security in cyber-physical production systems: A roadmap to improving IT-security in the production system lifecycle. In *2017 AEIT International Annual Conference*. IEEE, 1–6. https://doi.org/10.23919/AEIT.2017.8240552

[124] F. Xiao, L. Sha, Z. Yuan, and R. Wang. 2018. VulHunter: A Discovery for unknown Bugs based on Analysis for known patches in Industry Internet of Things. *IEEE Transactions on Emerging Topics in Computing* (2018). https://doi.org/10.1109/TETC.2017.2754103 (early access).

[125] P. Xu, S. He, W. Wang, W. Susilo, and H. Jin. 2018. Lightweight Searchable Public-Key Encryption for Cloud-Assisted Wireless Sensor Networks. *IEEE Transactions on Industrial Informatics* 14, 8 (2018), 3712–3723. https://doi.org/10.1109/TII.2017.2784395

[126] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu. 2018. A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things. *IEEE Communications Magazine* 56, 2 (2018), 30–36. https://doi.org/10.1109/MCOM.2018.1700621

[127] C. Yin, J. Xi, R. Sun, and J. Wang. 2018. Location Privacy Protection Based on Differential Privacy Strategy for Big Data in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics* 14, 8 (2018), 3628–3636. https://doi.org/10.1109/TII.2017.2773646

[128] M. Yousif. 2016. Manufacturing and the Cloud. *IEEE Cloud Computing* 3, 4 (2016), 4–5. https://doi.org/10.1109/MCC.2016.77

[129] M. Yu, M. Zhu, G. Chen, J. Li, and Z. Zhou. 2016. A cyber-physical architecture for industry 4.0-based power equipments detection system. In *2016 International Conference on Condition Monitoring and Diagnosis (CMD)*. IEEE, 782–785. https://doi.org/10.1109/CMD.2016.7757942

[130] S. Zanero. 2017. Cyber-Physical Systems. *Computer* 50, 4 (2017), 14–16. https://doi.org/10.1109/MC.2017.105

[131] L. Zhou and H. Guo. 2018. Anomaly Detection Methods for IIoT Networks. In *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*. IEEE, 214–219. https://doi.org/10.1109/SOLI.2018.8476769

[132] L. Zhou, K. Yeh, G. Hancke, Z. Liu, and C. Su. 2018. Security and Privacy for the Industrial Internet of Things: An Overview of Approaches to Safeguarding Endpoints. *IEEE Signal Processing Magazine* 35, 5 (2018), 76–87. https://doi.org/10.1109/MSP.2018.2846297

[133] M. Zolanvari, M. A. Teixeira, and R. Jain. 2018. Effect of Imbalanced Datasets on Security of Industrial IoT Using Machine Learning. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 112–117. https://doi.org/10.1109/ISI.2018.8587389

[134] E. Zugasti, M. Iturbe, I. Garitano, and U. Zurutuza. 2018. Null is Not Always Empty: Monitoring the Null Space for Field-Level Anomaly Detection in Industrial IoT Environments. In *2018 Global Internet of Things Summit (GIoTS)*. IEEE, 1–6. https://doi.org/10.1109/GIOTS.2018.8534574