22. Nachwuchswissenschaftler*innenkonferenz (NWK)

https://doi.org/10.52825/ocp.v2i.149

Published: 15 Dec. 2022

Security and Configurable Storage Systems in Industry 4.0 Environments: A Systematic Literature Study

Richard May[1][https://orcid.org/0000-0001-7186-404X]*

[1] Hochschule Harz

* Korrespondenz; rmay@hs-harz.de

Abstract. An increasing amount of Industry 4.0 data storages is highly configurable. As each variant includes individual features and interactions, ensuring data security becomes increasingly challenging. However, we are missing an analysis of research on security and configurable storages in Industry 4.0, especially those based on product-line engineering. To address this gap, we conducted a literature study covering relevant state-of-the-art publications (2013–2022). Overall, security for configurable systems seems under-explored. We highlighted that security standards and concrete mitigations techniques are usually not considered. In addition, we are missing an analysis of configurable storage and software systems in concert to identify threats, risks, and vulnerabilities caused by variability.

1. Introduction

Due to the increasing number of interacting systems, the manufacturing industry generates a growing amount of data stored and processed in a variety of storages, such as databases embedded into cloud environments [1]. An increasing number of the storages used in Industry 4.0 is highly configurable, meaning they are based on variability to address specific customer needs, hardware constraints, industry standards, or regulatory requirements [2; 3; 4]. Since the attack surface of these systems is constantly growing due to their variant-based scaling up and networking, ensuring security becomes increasingly challenging [5].

In this study, we focus on configurable storages since they are one of the major targets of attacks and feature interactions can potentially reveal secrets [6; 7]. Unfortunately, there is a lack of an overview of the current research conducted on security and configurable storages as part of Industry 4.0 environments, e.g., cyber-physical systems. To address this gap, we conducted a systematic literature review [8] of 28 papers. We argue that our study can help researchers and practitioners in better understanding current shortcomings and concerns in the context of security for configurable systems, especially configurable storages.

2. Literature Study Methodology

Our study objective was to identify, classify, and discuss research in the intersection of configurable storages and security in Industry 4.0 environments by employing a systematic literature review [8]. We intentionally also considered potentially underlying configurable software systems that may be the actual focus of the analyzed papers. First, we defined the following search string, covering the most relevant thematic terms:

("software as a service" OR "SaaS" OR "service-based" OR "service-oriented" OR "on-demand") AND ("product line" OR "SPL" OR "product famil*" OR "variant*rich" OR "config*") AND ("robot*" OR "manufacturing" OR "industry 4.0" OR "cyber*physical*")

Using this string, we employed an automated search on the literature databases IEEE Xplore, ACM Digital Library, and Scopus. Second, we only included peer-reviewed conference papers or journal articles written in English, published between 2013 and 2022, and dealing with security and configurable storages in the context of Industry 4.0.

Third, we defined ten criteria to extract valuable data from the selected papers, namely the application area (e.g., robotics), the practice-orientation of the system (i.e., concept or implementation), the focus of the publication (i.e., software or storage), the underlying variability modeling technique (focusing on software product lines), the storage type (e.g., database or cloud), the variability focus of the publication (i.e., software or storage), the general mentioning of security as well as security threats (e.g., SQL injection attacks), goals (e.g., CIA triad), standards (e.g., ISO/IEC 27000 series), and mitigation techniques (e.g., encryption).

The search was conducted on February 01, 2022, resulting in a total of 199 papers. After a title/abstract selection and a duplication removal, we considered 57 papers for the full-text selection. Next, we had to remove 29 more papers in the full-text selection, since these dealt only superficially with configurability or security. Finally, we considered 28 papers as suitable for our data extraction.

3. Data Extraction Results

In this section, we provide an overview of the extracted data (see Table 1). The majority of the papers focus on general manufacturing applications (21) and address only two more areas, namely robotics (6) and mechatronics (1). This result implies that most approaches could provide a high transferability and applicability to a variety of industrial use cases. Interestingly, 18 publications present concrete implementations, indicating a certain practice-orientation of the approaches. Regarding the publications' focus, we found that no paper refers to the storage alone but to storage in combination with software (8). Surprisingly, the majority considers the software (20) and only mentions storage as part of the overall software system. A similar trend emerges regarding the variability focus, where often only the software system is actually configurable (18) or the storage in the context of the overall software (9). Once the focus is only on the variability of the storage.

Table 1: Overview of the extracted data based on the defined criteria

Reference	Application area	Practice-orienta-	Publication focus	Software product	Variability focus	Storage type	Storage configur-	Security mentio-	Security threats	Security goals	Security standards	Mitigation techni-
Gherardi 2014 [9]	R	I	S_1, S_2	●	S_2	C, D	●	○	○	○	○	○
Wang 2015a [10]	G	C	S_1	○	S_1	C	●	○	○	○	○	○
Fischer 2015 [11]	M	I	S_1	●	S_1	D	○	○	○	○	○	○
Garcia 2015 [12]	G	C	S_1	●	S_1	D	○	●	○	○	○	○
Wang 2015b [13]	R	I	S_2, S_1	○	S_1, S_2	C, D	●	●	●	○	○	○
Galindo 2015 [14]	G	C	S_1	●	S_1	D	○	●	●	○	○	●
Carlsson 2016 [15]	G	I	S_1	○	S_1	C	●	●	○	●	○	●
Arrieta 2016 [16]	G	I	S_1	●	S_1	D	○	○	○	○	○	○
Groher 2016 [17]	G	I	S_1	●	S_1	D	○	○	○	○	○	○
Metzger 2016 [18]	G	I	S_2, S_1	●	S_1, S_2	C	●	○	○	○	○	○
McGee 2016 [19]	G	C	S_1	●	S_1	C	●	●	●	○	○	○
Heikkilä 2016 [20]	R	C	S_1	●	S_1	C	●	●	●	○	○	○
Yu 2017 [21]	G	I	S_1, S_2	○	S_1, S_2	C	●	○	○	○	○	○
McGee 2017 [22]	G	I	S_1	●	S_1	D	○	●	●	○	○	○
Iglesias 2017 [23]	G	C	S_1	●	S_1	C	●	○	○	○	○	○
Wang 2018 [24]	R	I	S_1	○	S_1, S_2	C, D	●	●	○	○	○	○
Jalil 2017 [25]	G	I	S_2, S_1	●	S_1, S_2	C	●	●	○	○	○	●
Krieter 2018 [26]	G	C	S_2, S_1	●	S_1, S_2	C	●	●	●	●	○	●
Çapa 2018 [27]	G	I	S_1	○	S_1	C, D	●	●	●	●	○	●
Zhang 2018 [28]	G	I	S_2, S_1	●	S_1, S_2	C	●	●	○	○	○	○
Lazreg 2019 [29]	G	I	S_1	●	S_1, S_2	-	●	○	○	○	○	○
Shaaban 2019 [30]	G	I	S_1	●	S_1	C	●	●	●	●	●	●
Cañete 2019 [31]	G	C	S_1	●	S_1	C	●	●	○	○	○	○
Jamshidi 2019 [32]	R	I	S_1	○	S_1	C	●	○	○	○	○	○
Chumpitaz 2019 [33]	G	C	S_1, S_2	●	S_1, S_2	C	●	●	●	○	○	●
Fischer 2020 [34]	G	I	S_1	●	S_1	D	○	○	○	○	○	○
Cañete 2020 [35]	G	C	S_1	●	S_1	E	●	●	○	○	○	○
Schlingloff 2021 [36]	R	I	S_1	●	S_1	C	●	○	○	○	○	○

General: ● Fulfilled, ○ Not fulfilled

Domain: R: Robotics, M: Mechatronics, G: General manufacturing

Practice orientation: C: Concept, I: Implementation

Publication focus/Variability focus: S_1: Software, S_2: Storage

Storage type: C: Cloud, D: Database

Most storages (21) are actual configurable, mainly because these are usually cloud environments, which are configurable by definition. The majority presents software product line-based solutions (21); the remaining papers (7) also usually reference product-line techniques although they are not based on them. One time, an edge environment is described. However, we assume that the cloud and edge environments also integrate a database as storage medium, although they do not mention it. Unsurprisingly, security is usually not considered in detail by the selected publications (17); threats (9), goals (4), standards (1), or mitigation techniques (7) are only rarely given. However, we found out that communication (e.g., between software system and storage) and the system configurability are main threats. These are addressed by diverse, generally described mitigation techniques, such as encryption or certificates. In two cases, security goals of the CIA triad, namely confidentiality and integrity, are mentioned. Only one paper refers to concrete security standards (IEC 62443, IEEE 1686).

4. Directions for Future Research

Overall, we identified three relevant research directions **(RD)** that should be addressed in future research. The often software product line-based approaches are often implemented in a certain theoretical context, but usually not implemented or evaluated within a practice-oriented environment. We argue that *collaborations with practitioners would increase the value of this research* **(RD_1)**.

We identified a strong connection between storages and configurable software systems, as most papers focus on both. However, the actual configurability of the storage and its associated requirements is rarely addressed. In contrast, most papers focus more on the configurability of software systems storing variability-related data in their storages, e.g., variants. We state that *it is essential to investigate software and storage in Industry 4.0 together in an equivalent manner* **(RD_2)** to understand interactions in data exchange between software and configurable storage and to identify potential security risks caused by configurability.

Mostly, security is either not considered at all or only described superficially. Threats (e.g., system configurability) are mentioned, but the associated issues and challenges are not addressed. Thus, we argue that security in the context of configurable storages in Industry 4.0 environments seems under-explored. *Research on configurable storages should be connected to concrete security standards (i.e., at least ISO/IEC 27000 series) and measures to address industry-specific artifacts, tasks, processes, and concrete security vulnerabilities* **(RD_3)**.

5. Conclusion

In this paper, we presented a literature study to provide an overview understanding of security in the context of configurable data storages in Industry 4.0 environments. Overall, we found several valuable insights and highlighted three directions for future research. Although there is extensive research on the security of (configurable) systems and established standards and norms, these are not usually referenced by configurable data storages, especially those based on software product lines. Consequently, we state the security in the context of configurable storages in Industry 4.0 environments seems under-explored despite the fact that these systems provide a growing attack surface due to their increasing complexity. We strongly recommend to connect configurable storages to concrete security approaches and international standards, e.g., by considering security not as a system's quality attribute or non-functional requirement, but as a concrete system feature with particular requirements.

Data availability statement

The analysis file generated during the study is available as an open access replication package: https://doi.org/10.5281/zenodo.7050709.

Competing interests

The author declares that he has no conflicts of interest or competing interests.

References

1. Gabel, Matthias, and Jeremias Mechler (2017): "Secure database outsourcing to the cloud: Side-channels, counter-measures and trusted execution". CBMS, pp. 799–804. doi: https://doi.org/10.1109/CBMS.2017.141.
2. Pohl, Klaus, Günter Böckle, and Frank Van Der Linden (2005): "Software product line engineering: foundations, principles, and techniques". Heidelberg, Springer.
3. Apel, Sven et al. (2016): "Feature-oriented software product lines". Berlin, Springer.
4. Krüger, Jacob et al. (2017): "Beyond software product lines: Variability modeling in cyber-physical systems". SPLC, pp. 237–241. doi: https://doi.org/10.1145/3106195.3106217.
5. Kenner, Andy et al. (2021): "Safety, security, and configurable software systems: a systematic mapping study". SPLC, pp. 148–159. doi: https://doi.org/10.1145/3461001.3471147.
6. Bamrara, Atul. (2015): "Evaluating database security and cyber attacks: A relational approach". The Journal of Internet Banking and Commerce 20/2: pp. 1–17.
7. Gamundani, Attlee M., and Lucas M. Nekare (2018): "A review of new trends in cyber attacks: A zoom into distributed database systems". IST-Africa, pp. 1–17.
8. Kitchenham, Barbara Ann, David Budgen, and Pearl Brereton (2015): "Evidence-based software engineering and systematic reviews". Boca Raton, CRC press.
9. Gherardi, Luca, Dominique Hunziker, and Gajamohan Mohanarajah (2014): "A software product line approach for configuring cloud robotics applications". CLOUD, pp. 745–75. doi: https://doi.org/10.1109/CLOUD.2014.104.
10. Wang, Yunxia, Jun Wei, and Chengchong Gao (2015a): "Customization design of cloud manufacturing resources based on polychromatic sets theory". IHMSC, pp. 518-521. doi: https://doi.org/10.1109/IHMSC.2015.255.
11. Fischer, Stefan et al. (2015): "Bridging the gap between software variability and system variant management: experiences from an industrial machinery product line". SEAA, pp. 402–409. doi: https://doi.org/10.1109/SEAA.2015.57.
12. Garcia, Cleiton et al. (2015): "A software process line for service-oriented applications". SAC, pp. 1680–1687. doi: https://doi.org/10.1145/2695664.2695743.
13. Wang, Xi Vincent, Abdullah Mohammed, and Lihui Wang (2015b): "Cloud-based robotic system: architecture framework and deployment models". FAIM, pp. 1–8.
14. Galindo, José A. et al. (2015): "Supporting distributed product configuration by integrating heterogeneous variability modeling approaches". Information and Software Technology 62/1: pp. 78–100. doi: https://doi.org/10.1016/j.infsof.2015.02.002.
15. Carlsson, Oscar et al. (2016): "Configuration service in cloud based automation systems". IECON, pp. 5238–5245. Doi: https://doi.org/10.1109/IECON.2016.7793489.
16. Arrieta, Aitor et al. (2016): "Test case prioritization of configurable cyber-physical systems with weight-based search algorithms". GECCO, pp. 1053–1060. doi: https://doi.org/10.1145/2908812.2908871.
17. Groher, Iris et al. (2016): "Reusable architecture variants for customer-specific automation solutions". SPLC, pp. 242–251. doi: https://doi.org/10.1145/2934466.2934492.
18. Metzger, Andreas et al. (2016): "Coordinated run-time adaptation of variability-intensive systems: an application in cloud computing". VACE, pp. 5–11. doi: https://doi.org/10.1109/VACE.2016.010.
19. McGee, Ethan T., and John D. McGregor (2016): "Using dynamic adaptive systems in safety-critical domains". SEAMS, pp. 115–121. doi: https://doi.org/10.1145/2897053.2897062.

20. Heikkilä, Tapio, Tadeusz Dobrowiecki, and Lars Dalgaard (2016): "Dealing with configurability in robot systems". MESA, pp. 1–7. doi: https://doi.org/10.1109/MESA.2016.7587120.
21. Yu, Shiqiang et al. (2017): "Product-Service Family Enabled Product Configuration System for Cloud Manufacturing". MSEC, pp. 1–9. doi: https://doi.org/10.1115/MSEC2017-2987.
22. McGee, Ethan T. et al. (2017): "Designing for reuse in an industrial internet of things monitoring application." WASHES, pp. 19–25. doi: https://doi.org/10.1145/3098322.3098323.
23. Iglesias, Aitziber et al. (2017): "Product line engineering of monitoring functionality in industrial cyber-physical systems: a domain analysis". SPLC. 2017, pp. 195–204. doi: https://doi.org/10.1145/3106195.3106223.
24. Wang, Lihui, and Xi Vincent Wang (2018): "Cloud robotics towards a CPS assembly system". Cloud-Based Cyber-Physical Systems in Manufacturing, pp. 243–259. doi: https://doi.org/10.1007/978-3-319-67693-7_10.
25. Jalil, Dzulkafli, and Muhamad Shahbani Abu Bakar (2017): "Adapting Software Factory Approach into Cloud ERP Production Model". International Journal of Computer Science and Information Security 15/1: pp. 1–9.
26. Krieter, Sebastian et al. (2018): "Towards secure dynamic product lines in the cloud". ICSE-NIER, pp. 5–8. doi: https://doi.org/10.1145/3183399.3183425.
27. Çapa, Birol et al. (2018): "Rapid PLC-to-Cloud Prototype for Smart Industrial Automation". ISCSIC, pp. 1–5. doi: https://doi.org/10.1145/3284557.3284710.
28. Zhang, Zhenjie et al. (2018): "CMfgIA: a cloud manufacturing application mode for industry alliance". The International Journal of Advanced Manufacturing Technology 98/9: pp. 2967–2985. doi: https://doi.org/10.1007/s00170-018-2476-x.
29. Lazreg, Sami et al. (2019): "Multifaceted automated analyses for variability-intensive embedded systems". ICSE, pp. 854–865. doi: https://doi.org/10.1109/ICSE.2019.00092.
30. Shaaban, Abdelkader Magdy, Thomas Gruber, and Christoph Schmittner (2019): "Ontology-based security tool for critical cyber-physical systems". SPLC, pp. 207–210. doi: https://doi.org/10.1145/3307630.3342397.
31. Cañete, Angel, Mercedes Amor, and Lidia Fuentes (2020): "Supporting the evolution of applications deployed on edge-based infrastructures using multi-layer feature models". SPLC, pp. 79–87. doi: https://doi.org/10.1145/3382026.3425772.
32. Jamshidi, Pooyan et al. (2019): "Machine learning meets quantitative planning: Enabling self-adaptation in autonomous robots". SEAMS, pp. 39–50. doi: https://doi.org/10.1109/SEAMS.2019.00015.
33. Chumpitaz, Luis, Andrei Furda, and Seng W. Loke (2019): "Evolving Variability Requirements of IoT Systems". Software Engineering for Variability Intensive Systems, Auerbach Pubs, pp. 321–334.
34. Fischer, Juliane et al. (2020): "VarApp: Variant management app for IEC 61131-3 compliant legacy software". ICPS, pp. 269–276. doi: 1 https://doi.org/0.1109/ICPS48405.2020.9274774.
35. Cañete, Angel (2019): "Energy efficient assignment and deployment of tasks in structurally variable infrastructures". SPLC, pp. 222–229. doi: https://doi.org/10.1145/3307630.3342704.
36. Schlingloff, Bernd-Holger, and Niels Hoppe (2021): "A Framework for Cloud-based Testing of Multi-variant Cyber-physical Systems". MECO, pp. 1–4. doi: 10.1109/MECO52532.2021.9460159.