Security Gap in Microservices: A Systematic Literature Review

Nurman Rasyid Panusunan Hutasuhut, Mochamad Gani Amri, Rizal Fathoni Aji
Faculty of Computer Science, Universitas Indonesia, Indonesia, Jakarta

***Abstract*—The growing importance of microservices architecture has raised concerns about its security despite a rise in publications addressing various aspects of microservices. Security issues are particularly critical in microservices due to their complex and distributed nature, which makes them vulnerable to various types of cyber-attacks. This study aims to fill the gap in systematic investigations into microservice security by reviewing current state-of-the-art solutions and models. A total of 487 papers were analyzed, with the final selection refined to 87 relevant articles using a snowball method. This approach ensures that the focus remains on security issues, particularly those identified post-2020. However, there is still a significant lack of dedicated security standards or comprehensive models specifically designed for microservices. Key findings highlight the vulnerabilities of container-based applications, the evolving nature of cyber-attacks, and the critical need for effective access control. Moreover, a substantial knowledge gap exists between academia and industry practitioners, which compounds the challenges of securing microservices. This study emphasizes the need for more focused research on security models and guidelines to address the unique vulnerabilities of microservices and facilitate their secure integration into critical applications across various domains.**

***Keywords*—Microservice security; cyber-attacks; container; security standards; access control**

I. Introduction

Security issues have been rising in many fields, especially in microservices. Even though publications on the topic of microservice are considered high, there is a lack of exploration of the security aspect of microservice [1] [2]. Furthermore, reported from the survey that security is the most ranked issue, followed by availability and scalability. Also, more cyber-attacks are indicated targeting microservices [3]. As indicated in many reports regarding security attacks, microservices have high vulnerabilities to many types of security attacks due to their complex and highly distributed nature.

The trend shows that the security topic in microservice still lacks exploration as opposed to the surge in literature discussing microservice in various topics such as architectural methods and practical application [4], [5]. This trend is supported by findings in grey literature stating that security is the biggest challenge in microservice systems. Moreover, a study reported that this trend is due to the security exploration in microservice is still in the early phase. This seems reasonable since microservice was first popularized by Netflix in 2015 [6].

It is concerning, given the importance of security in the landscape of software development, as microservices continue to gain traction and are adopted across industries. In study [7] reported that application security is the pressing issue in many aspects of microservice such as integration, scalability, API Gateway, etc. Moreover, security vulnerabilities and risks can have far-reaching consequences, making it imperative to address this aspect of microservice comprehensively.

The urgency of addressing security concerns in microservices cannot be overstated, given their increasing integration into mission-critical applications across various domains such as finance, healthcare, and e-commerce. As microservices continue to evolve [7], it is imperative that scholarly discourse on their security keeps pace, ensuring these modern software architectures remain resilient and trustworthy in an ever-changing technological landscape. It is crucial to identify and address the specific challenges inherent in microservice systems and explore how existing techniques can effectively contribute to their security. Despite the growing significance of microservices, there remains a notable gap in systematic investigations at the intersection of security and microservice architectures.

Particularly, many surveys and literature on practitioners that stated microservice is lack of security standard or model [8]. In [9] stated, moreover, more research is needed to deal with microservice complexity, handle security in microservices systems. However, securing MSA is a very challenging task since traditional security concepts cannot be directly applied to MSA [10].

Our findings reveal that more research is needed to (1) deal with microservices complexity at the design level, (2) handle security in microservices systems, and (3) address the monitoring and testing challenges through dedicated solutions.

A. Background

As microservice continues to emerge, paper [11] raised a concern regarding microservice security. This study conducted a systematic literature review on security topics within the microservice realm, by analyzing 290 publications from various sources. The research involved metadata analysis, vector-based markers, and a partitioned overview based on threat models, security, infrastructure, and development approaches. Additionally, recurring concepts like blockchain and service-mesh technologies were explored. The study identified open challenges in microservice security, including issues with data provenance, technology transfer, security-by-design adoption, dedicated attack trees, technological references, migration, global view/control, react and recover techniques, and DevSecOps integration. The lack of established venues for microservices security research was highlighted, emphasizing the need for dedicated platforms to facilitate knowledge

exchange and collaboration among researchers and practitioners. The article concludes by proposing future research directions, suggesting a focus on the grey literature and non-peer-reviewed sources to further enrich the understanding of microservices security.

Microservices have gained popularity since being championed by Netflix in 2015, enabling scalable, modular, and resilient application architectures. Despite these advantages, their distributed nature introduces vulnerabilities, especially in inter-service communication and system integration. Studies highlight common protocols like OAuth 2.0, JWT, API Gateway, and OpenID Connect for managing authentication and authorization, yet challenges persist in implementing robust security across the architecture.

Prior systematic reviews (e.g., [5], [11], [12]) reveal that both academic and grey literature primarily propose mitigation strategies, with limited emphasis on proactive security models. Internal attacks, constituting 60% of all microservice-related breaches (IBM X-Force), remain underexplored compared to external threats, underscoring the need for more focused research.

This paper builds upon prior studies to investigate security challenges in microservices, with a specific focus on developing a comprehensive framework to address vulnerabilities, analyze threat models, and propose practical solutions for academia and industry.

This literature study shows that microservice architecture is well understood since many studies have been published since 2015, and yet there is still a gap that needs to be filled. For instance, it is reported that microservice is one the type of system that has vulnerabilities in security and yet there is no model or framework regarding security in microservice. Also, many studies regarding microservices are specific for a particular use case, and this can also be a challenge in creating a framework within the security realm in microservices. This issue is amplified by the skill gap between academia and industry, as shown by publications in grey and academic literature, where grey literature seems more applicable than academic literature.

Therefore, this study aims to continue the previous study [5] to identify and review the current state-of-the-art security solutions in microservices, specifically in the security models, in terms of developing secure applications. Also analyzed was the proposed study in academic literature. Furthermore, it is particularly important to understand the gap, identify which problems are especially relevant for microservice systems, and determine how existing techniques can contribute to addressing them.

II. Research Methods

To achieve the research goal, we performed a Systematic Literature Review (SLR) in accordance with the guidelines proposed in [14] and the structuring applied in [15]. According to the authors, an SLR is “a means of identifying, evaluating and interpreting all available research relevant to a specific research question, or topic area, or phenomenon of interest" [17]. In addition, this study used the online tool Rayyan [16] to support the screening and analysis of the identified studies.

Based on the literature study, Research Questions (RQ) is formulated and elaborated in the next section. During study, the bulk of papers is obtained from various sources and the RQ’s is used as tool for classifying as well as analyzing the papers.

A. Research Questions

Three research questions were formulated based on the literature study conducted, as explained in the previous section.

- RQ 1. What are the current threats in microservice?

Capturing the scene in terms of security threats as well as security attacks in microservice architecture through academic literature.

- RQ 2. Are there factors or features that are important in securing microservice?

Highlighting the main factors or features that are essential in ensuring security in microservices.

- RQ 3. Are there security standards or models regarding security in microservice architecture?

Based on threats or attacks documented in the literature, through this question is also capturing and characterize the solutions available.

B. Search Process

This study employed four major digital libraries ACM Digital Library, IEEE Xplore, and Scopus. To search in a structure manner, numerous string keywords and combinations are used based on [5], [17] as a query in each digital libraries.

- (“microservice” OR “security”) AND (“microservice”∗ OR "microservice"∗ OR “micro-service”∗) (“MICROSERVICE SECURITY” OR “MICROSERVICES SECURITY”) AND (“CHALLENGE*” OR “PROBLEM*” OR “ISSUE*” OR “SOLUTION*” OR “PROTOCOL*” OR “MECHANISM*” “STRATEGY*”.

C. Snowballing Method

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either Times New Roman or the Symbol font (please, no other font). To create multilevel equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

The snowballing method [14] was implemented in our academic literature review to mitigate the risk of overlooking pertinent studies. This iterative process involved reviewing the references of each study within the initial paper set, incorporating them into the set, and repeating the procedure until no further additions were identified. Both backward and forward snowballing methods were employed. In the backward approach, we scrutinized the references of each selected study, while the forward method involved searching for citations of each selected study. Through this comprehensive snowballing process, additional primary studies were uncovered, resulting in the inclusion of 10 studies from academic literature and 15 from grey literature. Subsequently, the expanded list of articles underwent the application of inclusion/exclusion criteria,

leading to a final paper set comprising 36 primary studies from academic literature and 34 publications from grey literature.

Additionally, to safeguard against the omission of relevant studies, we implemented the snowballing process, following the approach outlined by study [20]. This involved verifying references related to the research object within each selected study. In essence, we actively sought out papers that cited the studies initially chosen. This meticulous approach aimed to ensure a comprehensive and thorough exploration of the existing literature, preventing the oversight of crucial contributions to the field equations should be placed at the center of the line and provided consecutively with equation numbers in parentheses flushed to the right margin, as in Eq. (1). The use of Microsoft Equation Editor or MathType is preferred.

D. Inclusion and Exclusion Criteria

Furthermore, the following are defined inclusion and exclusion criteria to filter relevant studies to be selected for the study.

Inclusion Criteria:

- Primarily from 2019, the latest
- Open access
- Studies related to microservice-based systems
- Studies focusing on security-scope
- Studies related to security scope in microservice
- Not limited to microservice, studies that provide solutions, methodologies, security reports, methodologies, security mechanisms, or other procedures to handle security scope

Exclusion Criteria:

- Studies published prior before 2019
- Short paper (less than three pages)

III. Result and Discussion

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit the use of hard returns to only one return at the end of a paragraph. Do not add any pagination anywhere in the paper. Do not number text heads- the template will do that for you. Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

A. Sources Paper Overview

There are 487 papers are obtained from various resources and using keyword as mentioned in the previous section. By removing duplicates and employed the criteria, there are 87 articles in the list that is relevant with this study. From those 87 articles, most of them are from Journal as much as 64 articles, conference 21 articles, and 1 book.

Furthermore, by employing the snowballing method, the list was refined to a total of 46 articles. This method involved a meticulous double-check of each article to ensure relevance and quality. Initially, a comprehensive list was compiled from various sources, but through the snowballing process, only the most pertinent studies were retained. This approach not only filtered out less relevant papers but also helped identify critical contributions and emerging trends in the field of microservice security.

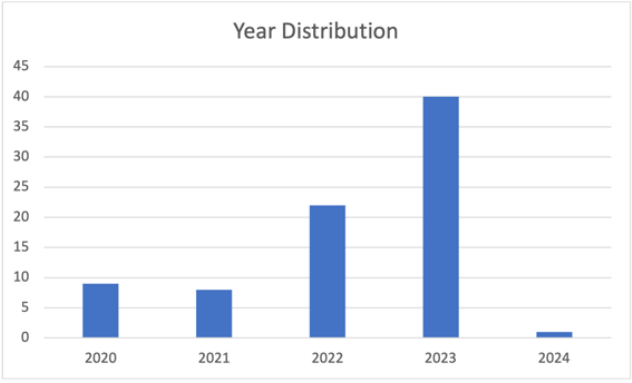

Fig. 1. Comparing publication year regarding microservice security using a certain keyword.

Fig. 1 shows the distribution of the publication year of microservice security publications using the keywords mentioned in the previous section. This study employed publication prior to 2020 at the latest. As shown in Fig. 1, most articles discuss security, particularly in microservices, in 2023. In which the trend gradually increased since 2020. In other words, more people or studies are raising concerns about security on this topic. Consequently, it indicates there are gaps or problems in microservice in terms of security.

In addition, this topic is still lack of exploration as indicates in the Fig. 1, this seems reasonable considering microservice is still quite young and still in an early phase since microservice is introduce in 2015 [18].

Besides the positive trend in terms of publications discussing security, however, as found in [11] reported that there is no event in conferences or journals that is security-oriented. Instead, the analyzed articles are found in publications covering a wide array of subjects, spanning from networking to cloud computing, and in open-access journals like IEEE Access and ACM Queue. Additionally, there isn't a single favored venue that stands out among others; instead, contributors are spread across numerous related platforms.

Fig. 2 shows the word cloud of topics discussed within the articles. Security is the main word followed by Cloud Computing, Computer Architecture, Internet of Things, and another word related security such as Authentication, Monitoring, Protocols, etc.

B. RQ1. Current Threads Towards Microservice

- Container apps brings threats: [18],[19],[21],[22]
- Cyber attacks are always evolving: [23],[22]
- The use of heterogeneity and unnecessary dependencies: [22][11]

Fig. 2. Wordcloud.

Overall, in terms of threats towards microservice, there are three main findings, namely, threats caused by containers, specifically by container third-party apps. Secondly, the approach to cyber-attacks is constantly evolving, making it harder to defend against such attacks. Lastly, it is related to containers, which use unnecessary dependencies.

Interestingly, during 2023 publication raising concern about security in container is increasing. Specifically, by using a third-party app. Beside container well-known advantages, many reports stated that container security has the highest vulnerability in microservice. As in study [24] reported the image in container also contains vulnerabilities. Consequently, employing in a large-scale bring threats and challenges. For instance, the system calls of a running container are a potential source of escalation and brute-force attacks [22].

In study [21] reported that container security issue have the highest vulnerability in microservice. At the same time, in report [22] also highlights that attacks towards container-based is the most attacks beside architectural attacks.

Yet, despite the raising concern in this issue, the most studied tools for defense in terms of container issue is still less studied. Therefore, it is crucial for more exploration in this issued to be done. Especially more study in creating lightweight container that can reduce the security vulnerabilities [22].

By its nature, the container is an isolated and restricted environment that typically looks like a Linux process anatomy. Besides their lightness, containers can be compromised by gaining unauthorized access or deriving vulnerabilities by using images from untrusted sources. Consequently, it is important to take more serious security measures at this level. As well as, more guidance should be explored in terms of containerization.

Furthermore, the use multilayer technology stacks also give a way towards system to be exploited [11], [22] in which still related to containerization. These include data leakage from interactions between the host and container, threats to encryption reliability from differing standards and data format conversions, and covert attacks through the hijacking of software libraries.

Therefore, more exploration throughout container issue is necessary. As many literatures reported that there is concerning vulnerability within container itself.

Microservice typically is hard to maintain. Therefore, many attacks reported are exposing data between each service. As reported in study [25] that the communication intercepted and altered by malicious insiders.

C. RQ2. Important Factors in Securing Microservice

- Access Control is critical in securing microservice: [26], [27]
- The use of third-party container apps: [19], [18]
- Knowledge Gap: [28], [29], [18], [22], [30], [31]
- Distributed nature: [18], [22], [31]
- Other: [13], [30], [31]

There are technical and non-technical factors that are important towards microservice security. Surprisingly, knowledge gap in securing microservice seems concerning. Both from academic and grey literature raising the same issue. Since, microservice is typically hard to maintain and always evolving by its nature [18]. Also, the gap also exists between practitioner and academia [22].

In terms of security, the microservice topic is still in an early phase, as indicated by the number of publications within this context [11]. This seems one of the factors that why there is a knowledge gap. There is still little empirical evidence available on security discussion in microservice [8]. This is due to the no dedicated fragment events on security issue especially architectural software topic [22]. Hence, it is crucial to have dedicated fragment that explore issue security especially in architectural software namely microservice.

As mentioned before, there is also a knowledge gap between practitioners and academia. This might be one of the reasons for the number of publications on this topic. Since, most publications are still discussion in theory of specific problem rather than security implementation. In contrast of in grey literature that more percentage of its publication are discussing security implementation. Moreover, there is also knowledge gap between the organizations and practitioner [18].

Followed by its nature, the complexity of its system is linear with its diversity in security attacks. As experiment studies showed, the larger the architecture, the less likely bugs or errors can be localized, and the less likely the individual microservices can be independently developed and evolved [31]. Many publications reported security solutions with specific problems. The large spectrum of security issues is amplified by microservice in a neighboring area with cloud, edge, fog computing, and containerization, as explained in the previous section. Since microservice is typically implemented in those areas [31].

Due to its complex nature, many publications are problem specific. There is no general approach for security in

Microservice as will be explained further in the next section. As different environment requires different approach in system design including in terms of security. Therefore, the complex nature plays a big factor in security of microservice.

Moreover, in terms of attacks, architectural attacks are less addressed due to their complexity as opposed to software attacks [22][13]. As mentioned before, microservice architectures are always evolving. Consequently, it is required to provide low-level solutions related to hardware, nodes, and operating systems. Also, it is more challenging to provide more comprehensive solutions for microservices due to the granularity of their design [13]. Consequently, compromising a single service may affect the security of the whole system due to the complex configuration and communication between each service [13].

As a result, the configuration of communications between services is crucial for the security. As found through publications in this study, there is growing attention of this issue. Yet there is still lack of security solution implementation as well regarding this issue. In [30] reported that, composition and communication of each service in microservice should have much attention.

D. RQ3. Security Standard or Solutions

a) There are no generic standards: [8], [24], [30], [31]

b) Available solutions or security standards are for specific problems only: [20], [26], [27], [29], [32], [33], [34], [35], [36], [37], [38], [39], [40].

c) Security standards are a less studied topic: [8], [22], [31], [13], [21], [17]

As discussed in the previous sections, the main reason why microservice is hard to maintain is its nature. Microservice is always evolving. Consequently, the attack toward it is linear. Thus, it is hard to maintain such a system. In addition, there is also some knowledge on many levels of securing microservices.

As a result, it is hard to have or to establish a general guideline standard for microservice security, while at the same time, it is also crucial to have such a standard. As study in [8] reported, practitioners complain that there are no clear security standards in developing microservices. Despite many publications calling for such standards, it is still hard to find one. Fragments event that focuses on architectural security issues.

The term standard or model discussed in this section can be interpreted as threat, mitigation, monitoring models, or etc. Surprisingly, it is hard finding such publications regarding this context. This finding is correlated with finding explained in the previous section which this topic of study is still in an early phase. This might be understandable, since Microservice terms is popularized by Netflix in 2015.

Furthermore, the study also conjectures that this lack of usage of generic threat models since the majority of research done on microservice security comes from the software (engineering, languages) side of the field rather than from the side of security, which advocates for a security-by-design approach. This is correlated with findings in the previous section, which is there are no security event outlets available in conferences or journals that focus on this topic.

In terms of mitigation model, there is still lack of security approaches address applications across the full stack. Therefore, it is an opportunity to be explore more regarding this topic.

It is the same case in terms of threat models. There is still lack of model regarding this topic. Even though, with such model is proven useful in the identification of attack types and strategic counter measures. Not to mention the complexity of microservice nature, this guideline is crucial in tackling the multifaceted attack surface of microservices architectures.

There are several security standards or models discussed in the literature. Namely Trust Models and GDPR guidelines. The zero Trust model consists of several model types, such as socio-based, composition-based, control-based, and zero-trust-based, in which those models focus on how users, applications, devices, or packets establish trust with each other. On the other hand, the GDPR guideline is more focused on protecting the privacy of the users. In terms of GDPR guidelines, it is surprising that only one publication claimed to be a GDPR guideline to protect the privacy of users. Especially if the microservice is a cloud-based system.

Interestingly, one paper stated that the diversity of attacks is due to the adoption of zero-trust models. Since the model assumed to afford no default trust for entities within the system.

IV. Conclusion

The exploration of microservice security reveals significant challenges and gaps in current understanding and practices, particularly highlighting the substantial security risks posed by containerization, evolving cyber-attacks, and unnecessary dependencies. Containers, despite their advantages, are prone to vulnerabilities such as unauthorized access and the use of untrusted images, necessitating stringent security measures to mitigate potential exploits and data breaches. Additionally, the distributed and evolving nature of microservices increases their complexity and the potential for security breaches, emphasizing the need for robust access control mechanisms and careful use of third-party container apps. The study also underscores a significant knowledge gap between academia and industry practitioners and the lack of comprehensive, adaptable security standards. This absence of cohesive security guidelines, coupled with the continuous evolution of microservices, presents substantial challenges in maintaining security.

As the study reported, Containerized applications have been getting traction lately in terms of security vulnerabilities. More exploration of this topic is crucial. Containers are becoming more popular because of their portability and efficiency in development and production. Moreover, increased collaboration and focused studies are essential to develop and disseminate effective security frameworks and standards, ensuring robust defenses against an ever-changing threat landscape.

REFERENCES

[1] P. Di Francesco, I. Malavolta, and P. Lago, "Research on Architecting Microservices: Trends, Focus, and Potential for Industrial Adoption," 2017 IEEE International Conference on Software Architecture (ICSA), pp. 21–30, May 2017, doi: 10.1109/ICSA.2017.24.

[2] M. T. Hinkley C, Snyder A, "Application Security Statistics Report. The evolution of the secure software lifecycle," 2018.

[3] N. Dragoni et al., "Microservices: Yesterday, today, and tomorrow," Present and Ulterior Software Engineering, pp. 195–216, Nov. 2017, doi: 10.1007/978-3-319-67425-4_12/COVER.

[4] A. Pereira-Vale, E. B. Fernandez, R. Monge, H. Astudillo, and G. Márquez, "Security in microservice-based systems: A Multivocal literature review," Computers and Security, vol. 103, p. 102200, 2021, doi: 10.1016/j.cose.2021.102200.

[5] C. Pahl and P. Jamshidi, "Microservices: A systematic mapping study," CLOSER 2016 - Proceedings of the 6th International Conference on Cloud Computing and Services Science, vol. 1, pp. 137–146, 2016, doi: 10.5220/0005785501370146.

[6] V. Bushong et al., "On Microservice Analysis and Architecture Evolution: A Systematic Mapping Study," Applied Sciences, vol. 11, no. 17, 2021, doi: 10.3390/app11177856.

[7] M. Waseem, P. Liang, M. Shahin, A. Di Salle, and G. Márquez, "Design, monitoring, and testing of microservices systems: The practitioners' perspective," Journal of Systems and Software, vol. 182, p. 111061, Dec. 2021, doi: 10.1016/J.JSS.2021.111061.

[8] M. Waseem, P. Liang, A. Ahmad, M. Shahin, A. A. Khan, and G. Márquez, "Decision models for selecting patterns and strategies in microservices systems and their evaluation by practitioners," pp. 135–144, May 2022, doi: 10.1145/3510457.3513079.

[9] P. Billawa, A. B. Tukaram, N. E. D. Ferreyra, J.-P. Steghöfer, R. Scandariato, and G. Simhandl, "SoK: Security of Microservice Applications: A Practitioners' Perspective on Challenges and Best Practices," ACM International Conference Proceeding Series, p. 10, Feb. 2022, doi: 10.1145/3538969.3538986.

[10] D. Berardi, S. Giallorenzo, A. Melis, M. Prandini, J. Mauro, and F. Montesi, "Microservice security: a systematic literature review," PeerJ Computer Science, vol. 7, pp. 1–66, 2022, doi: 10.7717/PEERJ-CS.779.

[11] M. G. de Almeida and E. D. Canedo, "Authentication and Authorization in Microservices Architecture: A Systematic Literature Review," Applied Sciences (Switzerland), vol. 12, no. 6, Mar. 2022, doi: 10.3390/APP12063023.

[12] A. Hannousse and S. Yahiouche, "Securing microservices and microservice architectures: A systematic mapping study," Computer Science Review, vol. 41, p. 100415, 2021, doi: https://doi.org/10.1016/j.cosrev.2021.100415.

[13] C. Wohlin, "Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering," in Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering, in EASE '14. New York, NY, USA: Association for Computing Machinery, 2014. doi: 10.1145/2601248.2601268.

[14] C. Wohlin, "Second-Generation Systematic Literature Studies using Snowballing", doi: 10.1145/2915970.2916006.

[15] M. Ouzzani, H. Hammady, Z. Fedorowicz, and A. Elmagarmid, "Rayyan-\--a web and mobile app for systematic reviews," Systematic Reviews, vol. 5, no. 1, p. 210, 2016, doi: 10.1186/s13643-016-0384-4.

[16] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic Mapping Studies in Software Engineering," in International Conference on Evaluation \& Assessment in Software Engineering, 2008.

[17] A. Rezaei Nasab, M. Shahin, S. A. Hoseyni Raviz, P. Liang, A. Mashmool, and V. Lenarduzzi, "An empirical study of security practices for microservices systems," Journal of Systems and Software, vol. 198, p. 111563, Apr. 2023, doi: 10.1016/j.jss.2022.111563.

[18] S. Sultan, I. Ahmad, and T. Dimitriou, "Container Security: Issues, Challenges, and the Road Ahead," IEEE Access, vol. 7, pp. 52976–52996, 2019, doi: 10.1109/ACCESS.2019.2911732.

[19] H. Jin, Z. Li, D. Zou, and B. Yuan, "DSEOM: A Framework for Dynamic Security Evaluation and Optimization of MTD in Container-based Cloud," IEEE Trans. Dependable and Secure Comput., pp. 1–1, 2019, doi: 10.1109/TDSC.2019.2916666.

[20] A. J. Cabrera-Gutiérrez, E. Castillo, A. Escobar-Molero, J. Cruz-Cozar, D. P. Morales, and L. Parrilla, "Blockchain-Based Services Implemented in a Microservices Architecture Using a Trusted Platform Module Applied to Electric Vehicle Charging Stations," Energies, vol. 16, no. 11, p. 4285, May 2023, doi: 10.3390/en16114285.

[21] M. S. Rahaman, A. Islam, T. Cerny, and S. Hutton, "Static-Analysis-Based Solutions to Security Challenges in Cloud-Native Systems: Systematic Mapping Study," Sensors, vol. 23, no. 4, p. 1755, Feb. 2023, doi: 10.3390/s23041755.

[22] Z. Li, H. Jin, D. Zou, and B. Yuan, "Exploring New Opportunities to Defeat Low-Rate DDoS Attack in Container-Based Cloud Environment," IEEE Trans. Parallel Distrib. Syst., vol. 31, no. 3, pp. 695–706, Mar. 2020, doi: 10.1109/TPDS.2019.2942591.

[23] F. Ying, S. Zhao, and H. Deng, "Microservice Security Framework for IoT by Mimic Defense Mechanism," Sensors, vol. 22, no. 6, p. 2418, Mar. 2022, doi: 10.3390/s22062418.

[24] C. Zhong, H. Zhang, C. Li, H. Huang, and D. Feitosa, "On measuring coupling between microservices," Journal of Systems and Software, vol. 200, p. 111670, Jun. 2023, doi: 10.1016/J.JSS.2023.111670.

[25] S. Xu et al., "Log2Policy: An Approach to Generate Fine-Grained Access Control Rules for Microservices from Scratch," in Annual Computer Security Applications Conference, Austin TX USA: ACM, Dec. 2023, pp. 229–240. doi: 10.1145/3627106.3627137.

[26] Z. Zaheer, H. Chang, S. Mukherjee, and J. Van der Merwe, "eZTrust: Network-Independent Zero-Trust Perimeterization for Microservices," in Proceedings of the 2019 ACM Symposium on SDN Research, in SOSR '19. New York, NY, USA: Association for Computing Machinery, Apr. 2019, pp. 49–61. doi: 10.1145/3314148.3314349.

[27] T. Cerny et al., "On Code Analysis Opportunities and Challenges for Enterprise Systems and Microservices," IEEE Access, vol. 8, pp. 159449–159470, 2020, doi: 10.1109/ACCESS.2020.3019985.

[28] I. Araujo, N. Antunes, and M. Vieira, "Evaluation of Machine Learning for Intrusion Detection in Microservice Applications," in 12th Latin-American Symposium on Dependable and Secure Computing, La Paz Bolivia: ACM, Oct. 2023, pp. 126–135. doi: 10.1145/3615366.3615375.

[29] Z. Lu, D. T. Delaney, and D. Lillis, "A Survey on Microservices Trust Models for Open Systems," IEEE Access, vol. 11, pp. 28840–28855, 2023, doi: 10.1109/ACCESS.2023.3260147.

[30] D. Berardi, S. Giallorenzo, J. Mauro, A. Melis, F. Montesi, and M. Prandini, "Microservice security: a systematic literature review," PeerJ Computer Science, vol. 7, p. e779, Jan. 2022, doi: 10.7717/peerj-cs.779.

[31] C. Meadows, S. Hounsinou, T. Wood, and G. Bloom, "Sidecar-based Path-aware Security for Microservices," in Proceedings of the 28th ACM Symposium on Access Control Models and Technologies, Trento Italy: ACM, May 2023, pp. 157–162. doi: 10.1145/3589608.3594742.

[32] A. Bambhore Tukaram, S. Schneider, N. E. Díaz Ferreyra, G. Simhandl, U. Zdun, and R. Scandariato, "Towards a Security Benchmark for the Architectural Design of Microservice Applications," in Proceedings of the 17th International Conference on Availability, Reliability and Security, in ARES '22. New York, NY, USA: Association for Computing Machinery, Aug. 2022, pp. 1–7. doi: 10.1145/3538969.3543807.

[33] I. Araujo, N. Antunes, and M. Vieira, "Intrusion Detection and Tolerance for Microservice Applications," in Proceedings of the 12th Latin-American Symposium on Dependable and Secure Computing, in LADC '23. New York, NY, USA: Association for Computing Machinery, Oct. 2023, pp. 176–181. doi: 10.1145/3615366.3622794.

[34] A. Chatterjee, M. W. Gerdes, P. Khatiwada, and A. Prinz, "SFTSDH: Applying Spring Security Framework With TSD-Based OAuth2 to Protect Microservice Architecture APIs," IEEE Access, vol. 10, pp. 41914–41934, 2022, doi: 10.1109/ACCESS.2022.3165548.

[35] W. Wang, A. Benea, and F. Ivancic, "Zero-Config Fuzzing for Microservices," in 2023 38th IEEE/ACM International Conference on Automated Software Engineering (ASE), Luxembourg, Luxembourg: IEEE, Sep. 2023, pp. 1840–1845. doi: 10.1109/ASE56229.2023.00036.

[36] B. G. Kim, Y.-S. Cho, S.-H. Kim, H. Kim, and S. S. Woo, "A Security Analysis of Blockchain-Based Did Services," IEEE Access, vol. 9, pp. 22894–22913, 2021, doi: 10.1109/ACCESS.2021.3054887.

[37] S. Tang, Z. Wang, J. Dong, and Y. Ma, "Blockchain-Enabled Social Security Services Using Smart Contracts," IEEE Access, vol. 10, pp. 73857–73870, 2022, doi: 10.1109/ACCESS.2022.3190963.

[38] M. Jin et al., "An Anomaly Detection Algorithm for Microservice Architecture Based on Robust Principal Component Analysis," IEEE Access, vol. 8, pp. 226397–226408, 2020, doi: 10.1109/ACCESS.2020.3044610.

[39] M. Anisetti, C. A. Ardagna, and N. Bena, "Multi-Dimensional Certification of Modern Distributed Systems," IEEE Trans. Serv. Comput., pp. 1–14, 2022, doi: 10.1109/TSC.2022.3195071.

[40] A. Hannousse and S. Yahiouche, "Securing microservices and microservice architectures: A systematic mapping study," Computer Science Review, vol. 41, p. 100415, Aug. 2021, doi: 10.1016/j.cosrev.2021.100415.