Preliminary Systematic Literature Review on the Adoption of Security as a Service (SECaaS)

Mohammed Yahaya Tanko [1], Abu Bakar Md Sultan [2], Hazura Zulzalil [3], Mohd Hafeez Osman [4]

[1, 2, 3, 4] Department of Software Engineering and Information System,
Faculty of Computer Science and Information Technology, Universiti Putra Malaysia,
UPM Serdang, Selangor Malaysia.
Email: [1] tymohammed45@gmail.com, [2] abakar@upm.edu.my, [3] hazura@upm.edu.my,
[4] hafeez@upm.edu.my

Abstract

Security as a Service (SECaaS) involves delivering security applications and services via the cloud computing technology to consumers, known as subscribers. Inspired by software as a Service (SaaS), the SECaaS approach promises to provide a high level of security and resources saving. Recent studies revealed numerous benefits of SECaaS as an efficient security model for SaaS applications. However, there is little research about its current adoption and future development. This paper aims to present fill these gaps by conducting a Systematic Literature Review (SLR) that summarizes and analyzes current and past SECaaS development and adoption. The analysis involves classification according to an enhanced SECaaS taxonomy. The SLR began with searching all related literature from well-known online repositories published between January 2011 and October 2021. Furthermore, identified inclusion-exclusion criteria were applied to filter the relevant articles. The study has so far obtained a total of 19 papers from 663 papers that exactly met all the stated criteria. The analysis revealed five concerns by potential SaaS tenants about the adoption of SECaaS and five key factors that make SECaaS as a preferred security mechanism over traditional approaches. Apart from that, seven metrics was identified to evaluate SECaaS performances. Finally, the preliminary findings concluded that SECaaS is a promising solution and more thorough study is needed to further understand the benefits of SECaaS.

Keywords— SECaaS; Security as a Service, SaaS security, Software as a Service Security.

1. Introduction

SaaS is a software deployment model where applications are hosted remotely by a service provider. These applications are usually made available to users (known as customers) based on pay-as-you-go model, over the Internet [1]. A SaaS model is usually multi-tenant in nature, that is, tenants subscribe to and customize the SaaS via its own domain name while paying according to their requirement [2], [3]. SaaS has grown rapidly over the last decade to become the dominant delivery model for meeting the requirements of enterprise IT services. This is due to the significant advantages of a SaaS model, such as improved operational efficiency and lower costs [1].

The architecture of a Software as a Service (SaaS) system can be divided into three layers: the web application layer, the web services layer, and the database layer. Examples of web services used in SaaS include Representational State Transfer (REST) and Simple Object Access Protocol (SOAP). The web layer, which includes servers such as IIS and Apache, and the database layer, which includes servers like Azure SQL and AWS RDS, are part of the Platform as a Service (PaaS) of a SaaS system. These layers are typically installed on Virtual Machines (VMs), which form the Infrastructure as a Service (IaaS) level. To manage the data of multiple SaaS tenants, there are three models. There is a database for each tenant, a schema for each tenant, and shared tables for each tenant [2].

Unlike the other layers of the cloud such as PaaS and IaaS which are mostly accessible only to administrators and developers, the SaaS layer is closer to the end-users that can be malicious. This makes the layer the most vulnerable security-wise with 39% of attacks targeting it [1]. SaaS has become increasingly vulnerable to attacks such as SQL injection (SQLIA) and cross-site scripting (XSS) [2]. Many vendors have stated that adopting SaaS technology can provide many benefits to users, such as cost reduction, but some organizations are still hesitant to adopt SaaS due to trust concerns, such as data security [1].

Deploying security as a SaaS (using a service) model and outsourcing to a third party is known as Security as a Service (SECaaS). A SECaaS model is quite different from traditional security model, and they are considered the future of Managed Security Service. It is expected that demand for SECaaS will increase significantly, potentially reshaping existing IT security infrastructure landscapes. Despite the perceived numerous benefits of SECaaS by many recent studies as an efficient security model for SaaS applications, there is little research about the current adoption and future development of SECaaS [4][5].

This paper aims to fill these gaps by conducting a systematic literature review of SECaaS. The main objective of the study is to comprehensively summarize and analyze current and past SECaaS implementations as well as classify them according to an enhanced existing SECaaS taxonomy. The result of the preliminary findings from this study are presented in this paper. The SLR began with searching all related literature from well-known online repositories published between January 2011 and October 2021. So far, a total of 19 papers from 663 papers that exactly met all the identified inclusion-exclusion criteria to filter the relevant articles have been identified and selected.

The rest of this paper is organized as follows: Related reviews are presented in section 2. Section 3 describes the details of the review method adopted in this study. This includes research questions (RQs), inclusion and exclusion criteria, the search strategies used, and the method for data extraction and analysis. In Section 4, results and findings of the review with respect to the RQs are discussed. Threats to the validity are then discussed in Section 5 and finally, section 6 concludes the paper.

2. Related Works

With the limited researches on its current adoption and future development of [4, 5], not many reviews have been conducted to analyze current and past researches on SECaaS. As of the time of conducting this SLR, and to the best of our knowledge, this is the first SLR to comprehensively summarize and analyze current and previous SECaaS researches in the manner that we have. Many of the existing reviews discussed an overview of SECaaS and attempted to provide some meaningful classification of a SECaaS. The studies by [4], [5], [6], [7], [8] provided a classification of SECaaS based on the categorization provided by Cloud Security Alliance (CSA) [9], a working group best known for its extensive research on cloud computing adoption and best practices guidelines for cloud environments. An acceptance model on the adoption of SECaaS by industries was developed by [4]. Their study provided an overview of SECaaS as well as perceived benefits and risks of its adoption. Data was collected from the industries via an online survey and the acceptance model developed was estimated by applying the Partial Least Squares technique to address the prediction-oriented nature of the study.

The study by [8] categorized existing SECaaS research according to their taxonomy which was also based on the one provided by CSA. However, a large number of the studies selected for this review were between 2010 and 2014. The study by [6] in addition to classification of SECaaS also provided gaps in SECaaS Web technologies. Challenges and opportunities were discussed by [5], [7], in addition to categorization of a SECaaS.

This SLR fills some of the gaps identified in the existing reviews and also covers most recent researches in SECaaS. We are confident that future researchers and practitioners will find it useful.

3. Review Method

The research method adopted in this study was inspired by Kitchenham's guidelines [24] for conducting Systematic Reviews in Software Engineering. The guideline proposed three stages in carrying out an SLR. They are planning, conducting and reporting. Each of these stages consists of a number of steps. Fig. 1 illustrates these stages and steps as applied in this SLR.

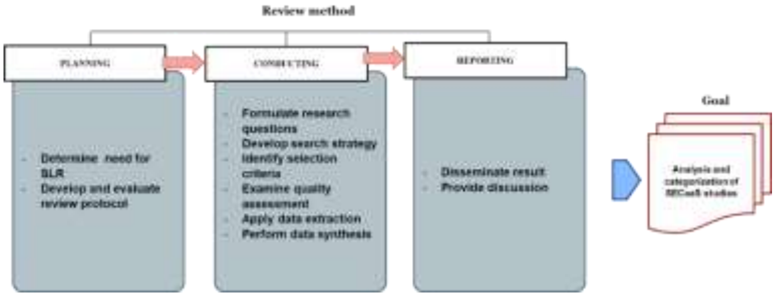
Review method
PLANNING
CONDUCTING
REPORTING
- Determine need for SLR
- Develop and evaluate review protocol
- Formulate research questions
- Develop search strategy
- Identify selection criteria
- Examine quality assessment
- Apply data extraction
- Perform data synthesis
- Disseminate result
- Provide discussion
Goal
Analysis and categorization of SECaaS studies

Figure 1. Review Method

A. Research Questions

The study aims to achieve the set objective by addressing the following research questions (RQs).

- RQ1: What are the current state of the art researches proposing a SECaaS security model for SaaS applications?
- RQ2: Are there concerns to the adoption SECaaS as a security model in SaaS by tenants?
- RQ3: What key factors make the adoption of SECaaS preferable over other security mechanisms in a SaaS?
- RQ4: What are the metrics used to evaluate a SECaaS framework?
- RQ5: Should we expect more researches in the adoption of SECaaS as a security model for SaaS applications?

B. Data Source and Search Strategy

The studies included in this SLR were searched for automatically from five of the largest digital repositories available for research today, namely ACM Digital Library (https://dl.acm.org), IEEExplore (https://ieeexplore.ieee.org), ScienceDirect (https://www.sciencedirect.com), SpringerLink (https://link.springer.com) and Scopus (https://www.sciencedirect.com). Search queries containing key words with respect to security as a service for SaaS applications were formed using the advanced search options of the repositories. The search strings were adjusted continuously in order to obtain the most relevant set of results. Any string made up of keywords related to security as a service, such as “secaas”, “security”, “service-based security”, and so on, were used in forming search strings. The advanced search functionalities of each of the repositories explored were utilized in composing search queries in order to obtain the best results. Wildcards were used to form some queries for the repositories that support its use.

C. Inclusion – exclusion criteria

The result from the search process yielded a large number of irrelevant studies. In order to eliminate many of the irrelevant studies, we define a set of inclusion – exclusion criteria as follows:

Inclusion Criteria

- Studies published between 2010 and October 2021
- Studies published in journals and conferences
- Studies in SECaaS that present a service model for security.
- Studies published in peer reviewed journals and conferences

Exclusion Criteria

- Studies published before 2010 or after October 2021
- Studies published outside journals and conference e.g book chapters, thesis, etc
- Studies that focus on IaaS, PaaS or any other platform different from SaaS
- Studies not published in peer reviewed journals or conferences

D. Study Quality Assessment

In addition to the inclusion – exclusion criteria, this research identified in this SLR were also subjected to quality assessment check. The goal of this check is to ensure that only studies that answer its research questions and ultimately achieve the goal of this study are selected. Kitchenham [24] proposed a defined quality assessment checklist. This study adopted this checklist in formulating eight quality assessment questions. Scoring of the quality assessment questions is as follows: A score of 1 indicates “yes”, a score of 0.5 indicates “partly” and a score of 0 indicates “no”.

E. Data Extraction

A total of nineteen articles have so far been reviewed in this SLR. For each of these articles, the following information was extracted. (i) problem addressed; (ii) objective(s) of the study (iii) category of security (according to taxonomy) (iv) merits and demerits of SECaaS (v) technique(s) used (vi) implementation environment (vii) evaluation metric(s) and validation method(s) (viii) publication type (ix) publisher (x) publication year. In addition, the title, author, year of publication, publication name and publication type were recorded were also recorded.

Table 1 shows the number of the articles that have been reviewed so far in each of the five repositories searched

Table 1. Number articles reviewed

Repository	Scopus	Springer Link	Science Direct	IEEE	ACM	Total
No. of articles	2	3	2	11	1	19

4. Results and Findings

A summary of the results obtained so far from the ongoing SLR with respected to the RQs is presented in this section

A. RQ1: What are the current state of the art researches proposing a SECcaaS security model for SaaS applications?

From this review so far, it is seen that researches into SECaaS started around the year 2010. All the researches that have been considered were conducted between the period of 2010 and 2021. No article that satisfactorily met all the defined selection criteria in this SLR conducted before this period was found. Out of the 19 selected primary studies, 14 of them, which represents about 74% of the total number of selected studies were conducted in the last 5 years. Fig. 2 gives the distribution of the studies by years.

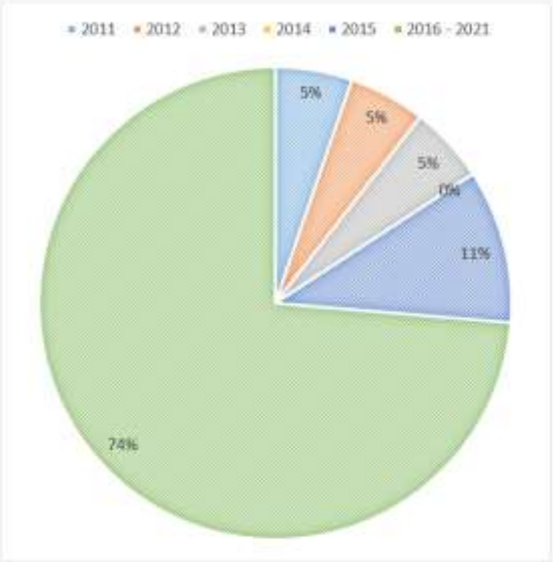

Figure 2. Distribution of selected primary studies over the period 2010 – 2021

B. RQ2: Are there concerns to the adoption SECaaS as a security model in SaaS by tenants?

In this research, we have so far come across four factors that tenants are concerned about when it comes to using a SECaaS. These factors are trust, confidentiality, privacy and Authentication and Authorization. Trust is the foundation of secure interaction between entities. With respect to confidentiality, service provides need to guarantee the accuracy of users' data and any analyses on these data when they in transit or when being stored. Considering that data is stored and communicated via the cloud and even across borders, cloud computing introduces new forms of information leakage and user categorized data security and privacy issues. When an entity attempts to access a protected resource, its identity is validated through authentication. On the other hand, authorization management in the cloud ensures that clients have the necessary permissions to access cloud-protected resources [28]

C. RQ3: What key factors make the adoption of SECaaS preferable over other security mechanisms in a SaaS?

This review has identified five key factors that make the adoption of a SECaaS preferable over the traditional approach to security management so far. The factors are Loss of Control, Tenant Security Requirement, Cost, Scalability and Flexibility, and availability.

D. RQ4: What are the metrics used to evaluate a SECaaS framework?

This research was able to obtain some of the metrics used to evaluate a SECaaS framework. These metrics were largely dependent on the particular security threat addressed by the framework. These valuation metrics are Detection Accuracy, Scalability, Flexibility, Overhead, Response time, Cost and Transfer time

Other evaluation metrics with respect to the security mechanism used are Scanner time, Encryption time and decryption time

E. RQ5: Should we expect more researches in the adoption of SECaaS as a security model for SaaS applications?

There is sufficient evidence from the findings of this SLR so far to indicate that more researches on SECaaS should be expected. According to a recent studies conducted by [31] on the security as a service market for Small and Medium Enterprises (SMEs), some of the benefits that attracts SMEs to cloud services include:

- Small businesses typically do not possess the necessary expertise to maintain and operate an IT infrastructure. Therefore, they often rely on cloud services to fulfill their needs as they provide easy access to applications, resources, and services that can be dynamically scaled according to their requirements.
- An environment characterized by rising security concerns necessitates more resource investment to combat these challenges.
- It is difficult to overlook the possibility to conduct IT operations more cost-effectively in the cloud than in-house, in addition to classic cloud benefits like scalability, elasticity, and ubiquitous access. According to the findings of [31], there are significantly more positive implications for SECaaS (Security as a Service) providers as small and medium-sized enterprise (SME) cloud consumers readily recognize the importance of SECaaS services in all circumstances. Although some SMEs may choose to accept the risks associated with not using expensive security services, the market for SECaaS services continues to grow overall.

Putting all these together, interested parties would want the most cost-effective security solution that adequately caters for their needs. This is bound to result in a healthy competition as providers will try to win more users than their rivals. This in turn should drive more researches in SECaaS. This assertion is further strengthened by this SLR as about 74% of all selected primary studies were conducted in the last five years as previously highlighted in section 3.1.

5. Conclusion

The paper introduces a preliminary systematic literature review on the adoption of Security as a Service (SECaaS). The review was conducted using the standard guideline for performing a systematic literature review in Software Engineering, which was proposed by [24].

The SLR began with searching all related literature from well-known online repositories published between January 2011 and October 2021. Furthermore, identified inclusion-exclusion criteria were applied to filter the relevant articles. The study has so far obtained a total of 19 papers from 663 papers that exactly met all the stated criteria.

The analysis revealed five concerns by potential SaaS tenants about the adoption of SECaaS and five key factors that make SECaaS as a preferred security mechanism over traditional approaches. Apart from that, seven metrics was identified to evaluate SECaaS performances. Finally, the preliminary findings concluded that SECaaS is a promising solution and more thorough study is needed to further understand the benefits of SECaaS.

6. Acknowledgement

This research was supported by the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia.

References

[1] A. A. Soofi, M. I. Khan, R. Talib, and U. Sarwar, "Security Issues in SaaS Delivery Model of Cloud Computing," vol. 3, no. 3, pp. 15–21, 2014.

[2] M. Yassin, H. Ould-slimane, C. Talhi, and H. Boucheneb, "Multi-tenant intrusion detection framework as a service for SaaS," vol. 1374, no. c, pp. 1–14, 2021, doi: 10.1109/TSC.2021.3077852.

[3] C. Kurian, "SaaS CLOUD COMPUTING A STUDY on SECURITY ISSUES in SaaS CLOUD COMPUTING," doi: 10.47760/ijcsmc.2021.v10i03.008.

[4] C. Senk, "Adoption of security as a service," *J. Internet Serv. Appl.*, vol. 4, no. 1, pp. 1–16, 2013, doi: 10.1186/1869-0238-4-11.

[5] W. Wang and S. Yongchareon, "Security-as-a-service: a literature review," *Int. J. Web Inf. Syst.*, vol. 16, no. 5, pp. 493–517, 2020, doi: 10.1108/IJWIS-06-2020-0031.

[6] B. Delamore and R. K. L. Ko, *Security as a service (SecaaS)—An overview*. Elsevier Inc., 2015.

[7] W. Wang and S. Yongchareon, "A survey on security as a service," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10570 LNCS, pp. 303–310, 2017, doi: 10.1007/978-3-319-68786-5_24.

[8] M. Elsayed and M. Zulkernine, "A taxonomy of security as a service," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11230 LNCS, pp. 305–312, 2018, doi: 10.1007/978-3-030-02671-4_19.

[9] "Cloud Security Alliance," 2020. https://cloudsecurityalliance.org/research/working-groups/security-as-a-service/ (accessed Oct. 22, 2021).

[10] W. W. Wu, "Developing an explorative model for SaaS adoption," *Expert Syst. Appl.*, vol. 38, no. 12, pp. 15057–15064, 2011, doi: 10.1016/j.eswa.2011.05.039.

[11] "Cloud Security Alliance: The Treacherous 12 - Cloud Computing Top Threats in 2016," 2016.

[12] A. Furfaro, A. Garro, and A. Tundis, "Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2014-Octob, no. October, 2014, doi: 10.1109/CCST.2014.6986995.

[13] L. F. Pla, N. Shashidhar, and C. Varol, "On-Premises Versus SECaaS Security Models," *8th Int. Symp. Digit. Forensics Secur. ISDFS 2020*, 2020, doi: 10.1109/ISDFS49300.2020.9116453.

[14] CSA, "SecaaS Category 1 Identity and Access Management Implementation Guidance," *Secaas Implement. Guid.*, no. September, pp. 1–43, 2012, [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf.

[15] CSA, "SecaaS Category 2 Data Loss Prevention Implementation Guidance," *Secaas Implement. Guid.*, no. September, 2012.

[16] CSA, "SecaaS Category 3 Web Security Implementation Guidance," *Secaas Implement. Guid.*, no. September, 2012.

[17] CSA, "SecaaS Category 4 Email Security Implementation Guidance," *Secaas Implement. Guid.*, no. September, 2012.

[18] CSA, "SecaaS Category 5 Security Assessments Implementation Guidance," *Secaas Implement. Guid.*, no. September, 2012.

[19] CSA, "SecaaS Category 6 Intrusion Management Implementation Guidance," *Secaas Implement. Guid.*, no. September, 2012.

[20] CSA, "SecaaS Category 7 Security Information and Event Management Implementation Guidance," *Secaas Implement. Guid.*, no. October, 2012.

[21] Cloud Security Alliance, "SecaaS Implementation Guidance Category 8 // Encryption," *Secaas Implement. Guid.*, no. September, pp. 1–28, 2012, [Online]. Available: http://now.dstv.com/livetv/play/0866e73b-6ece-42c9-8b87-68ad31db5847?acc_pg_sec=livetv channel list.

[22] Cloud Security Alliance, "Category 9 Business Continuity / Disaster Recovery," *Secaas Implement. Guid.*, no. September, 2012, [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_9_BCDR_Implementation_Guidance.pdf.

[23] CSA, "SecaaS Category 10 Network Security Implementation Guidance," *Secaas Implement. Guid.*, no. September, 2012.

[24] Barbara Kitchenham and S. Charters, "Методи за автоматично управление на подемни устройства при Jack-up системите," 2007, doi: 10.1145/1134285.1134500.

[25] T. Zhang, L. Yan, and Y. Yang, "Trust evaluation method for clustered wireless sensor networks based on cloud model," *Wirel. Networks*, vol. 24, no. 3, pp. 777–797, 2018, doi: 10.1007/s11276-016-1368-y.

[26] T. Ngo-ye and J. Choi, "Trust in Security As a Service: a Theoretical Model," *Issues Inf. Syst.*, no. October, 2020, doi: 10.48009/2_iis_2020_64-74.

[27] H. Abbas, O. Maennel, and S. Assar, "Security and privacy issues in cloud computing," *Ann. des Telecommun. Telecommun.*, vol. 72, no. 5–6, pp. 233–235, 2017, doi: 10.1007/s12243-017-0578-3.

[28] D. H. Sharma, C. A. Dhote, and M. M. Potey, "Identity and Access Management as Security-as-a-Service from Clouds," *Procedia Comput. Sci.*, vol. 79, pp. 170–174, 2016, doi: 10.1016/j.procs.2016.03.117.

[29] M. Hawedi, C. Talhi, and H. Boucheneb, "Security as a Service for Public Cloud Tenants(SaaS)," *Procedia Comput. Sci.*, vol. 130, pp. 1025–1030, 2018, doi: 10.1016/j.procs.2018.04.143.

[30] D. H. Sharma, C. A. Dhote, and M. M. Potey, “Implementing Intrusion Management as Security-as-a-service from cloud,” *2016 Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solut. CSITSS 2016*, pp. 363–366, 2016, doi: 10.1109/CSITSS.2016.7779387.

[31] D. L. Nazareth, J. Choi, and T. L. Ngo-Ye, “The Security-as-a-Service Market for Small and Medium Enterprises,” *J. Comput. Inf. Syst.*, vol. 00, no. 00, pp. 1–11, 2021, doi: 10.1080/08874417.2021.1954563.

[32] K. Takahashi, T. Matsuzaki, and T. Mine, “Security as a Service for User Customized Data,” pp. 298–309.

[33] T. Alharkan and P. Martin, “IDSaaS: Intrusion detection system as a service in public clouds,” *Proc. - 12th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. CCGrid 2012*, pp. 686–687, 2012, doi: 10.1109/CCGrid.2012.81.

[34] Y. Meng, W. Li, L. F. Kwok, and Y. Xiang, “Towards designing privacy-preserving signature-based IDS as a service: A study and practice,” *Proc. - 5th Int. Conf. Intell. Netw. Collab. Syst. INCoS 2013*, pp. 181–188, 2013, doi: 10.1109/INCoS.2013.35.

[35] V. Varadharajan, S. Member, and U. Tupakula, “Security as a Service Model for Cloud Environment,” vol. 11, no. 1, pp. 60–75, 2014.

[36] Y. Ghazi, R. Masood, A. Rauf, M. A. Shibli, and O. Hassan, “DB-SECaaS : a cloud-based protection system for document-oriented NoSQL databases,” *EURASIP J. Inf. Secur.*, 2016, doi: 10.1186/s13635-016-0040-5.

[37] J. K. K. Mahalakshimi, “‘Security-as-a-Service’ for Files in Cloud Computing - A Novel Application Model,” *2016 10th Int. Conf. Intell. Syst. Control*, pp. 1–5, 2016.

[38] M. Elsayed and M. Zulkernine, “IFCaaS : Information Flow Control as a Service for Cloud Security,” pp. 211–216, 2016, doi: 10.1109/ARES.2016.27.

[39] K. A. Torkura, M. I. H. Sukmana, F. Cheng, and C. Meinel, “Leveraging Cloud Native Design Patterns for Security-as-a-Service Applications,” 2017, doi: 10.1109/SmartCloud.2017.21.

[40] M. Yassin, H. Ould-Slimane, C. Talhi, and H. Boucheneb, “SQLIIDaaS: A SQL Injection Intrusion Detection Framework as a Service for SaaS Providers,” *Proc. - 4th IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2017 3rd IEEE Int. Conf. Scalable Smart Cloud, SSC 2017*, pp. 163–170, 2017, doi: 10.1109/CSCloud.2017.27.

[41] M. Elsayed and M. Zulkernine, “Offering security diagnosis as a service for cloud SaaS applications,” *J. Inf. Secur. Appl.*, vol. 44, pp. 32–48, 2019, doi: 10.1016/j.jisa.2018.11.006.

[42] O. Mjihil, H. Taramit, A. Haqiq, and D. Huang, *Optimized security as a service platforms via stochastic modeling and dynamic programming*, vol. 735. Springer International Publishing, 2018.

[43] Y. Birman, S. Hindi, G. Katz, and A. Shabtai, “Cost-Effective Malware Detection as a Service over Serverless Cloud Using Deep Reinforcement Learning,” *Proc. - 20th IEEE/ACM Int. Symp. Clust. Cloud Internet Comput. CCGRID 2020*, pp. 420–429, 2020, doi: 10.1109/CCGrid49817.2020.00-51.

[44] S. Fehis, O. Nouali, and T. Kechadi, “Secure encryption key management as a SecaaS based on Chinese wall security policy,” *J. Inf. Secur. Appl.*, vol. 63, no. October, p. 102975, 2021, doi: 10.1016/j.jisa.2021.102975.

[45] P. Empl and G. Pernul, *A Flexible Security Analytics Service for the Industrial IoT*, vol. 1, no. 1. Association for Computing Machinery, 2021.

[46] Z. J. Estrada *et al.*, “Using OS design patterns to provide reliability and security as-a-service for VM-based clouds,” *VEE 2017 - Proc. 2017 ACM SIGPLAN/SIGOPS Int. Conf. Virtual Exec. Environ.*, pp. 157–170, 2017, doi: 10.1145/3050748.3050759.

[47] M. Hawedi, C. Talhi, and H. Boucheneb, *Multi-tenant intrusion detection system for public cloud (MTIDS)*, vol. 74, no. 10. Springer US, 2018.

[48] R. L. Paikrao and V. H. Patil, “Security as a Service Model for Virtualization Vulnerabilities in Cloud Computing,” *2018 Int. Conf. Adv. Commun. Comput. Technol. ICACCT 2018*, pp. 559–562, 2018, doi: 10.1109/ICACCT.2018.8529573.