



Review

# Software-as-a-Service Security Challenges and Best Practices: A Multivocal Literature Review

Mamoona Humayun <sup>1,\*</sup>, Mahmood Niazi <sup>2,3,\*</sup>, Maram Fahhad Almufareh <sup>1</sup>, N. Z. Jhanjhi <sup>4</sup>,  
Sajjad Mahmood <sup>2,3</sup> and Mohammad Alshayeb <sup>2,3</sup>

- <sup>1</sup> Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakakah 72311, Saudi Arabia; mfalmufareh@ju.edu.sa
- <sup>2</sup> Department of Information and Computer Science, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia; smahmood@kfupm.edu.sa (S.M.); alshayeb@kfupm.edu.sa (M.A.)
- <sup>3</sup> Interdisciplinary Research Centre for Intelligent Secure Systems, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
- <sup>4</sup> School of Computer Science and Engineering (SCE), Taylor's University, Subang Jaya 47500, Malaysia; noorzaman.jhanjhi@taylors.edu.my
- \* Correspondence: mahumayun@ju.edu.sa (M.H.); mkniazi@kfupm.edu.sa (M.N.)

**Abstract:** Cloud computing (CC) is the delivery of computing services on demand and is charged using a “pay per you use” policy. Of the multiple services offered by CC, SaaS is the most popular and widely adapted service platform and is used by billions of organizations due to its wide range of benefits. However, security is a key challenge and obstacle in cloud adoption and therefore needs to be addressed. Researchers and practitioners (R&P) have discussed various security challenges for SaaS along with possible solutions. However, no research study exists that systematically accumulates and analyzes the security challenges and solutions. To fill this gap and provide the state-of-the-art (SOTA) picture of SaaS security, this study provides a comprehensive multivocal literature review (MVLRL), including SaaS security issues/challenges and best practices for mitigating these security issues. We identified SaaS security issues/challenges and best practices from the formal literature (FL) as well as the grey literature (GL) to evaluate whether R&P is on the same page or if controversies exist. A total of 93 primary studies were identified, of which 58 are from the FL and 35 belong to the GL. The studies are from the last ten years, from 2010 to 2021. The selected studies were evaluated and analyzed to identify the key security issues faced by SaaS computing and to be aware of the best practices suggested by R&P to improve SaaS security. This MVLRL will assist SaaS users to identify the many areas in which additional research and development in SaaS security is required. According to our study findings, data breaches/leakage, identity and access management, governance and regulatory compliance/SLA compliance, and malicious insiders are the key security challenges with the maximum frequency of occurrence in both FL and GL. On the other hand, R&P agree that up-to-date security controls/standards, the use of strong encryption techniques, regulatory compliance/SLA compliance, and multifactor authentication are the most important solutions.

**Keywords:** cloud computing; software-as-a-service (SaaS); multi-vocal literature review (MVLRL); security



**Citation:** Humayun, M.; Niazi, M.; Almufareh, M.F.; Jhanjhi, N.Z.; Mahmood, S.; Alshayeb, M. Software-as-a-Service Security Challenges and Best Practices: A Multivocal Literature Review. *Appl. Sci.* **2022**, *12*, 3953. <https://doi.org/10.3390/app12083953>

Academic Editor: Arcangelo Castiglione

Received: 18 March 2022

Accepted: 8 April 2022

Published: 14 April 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

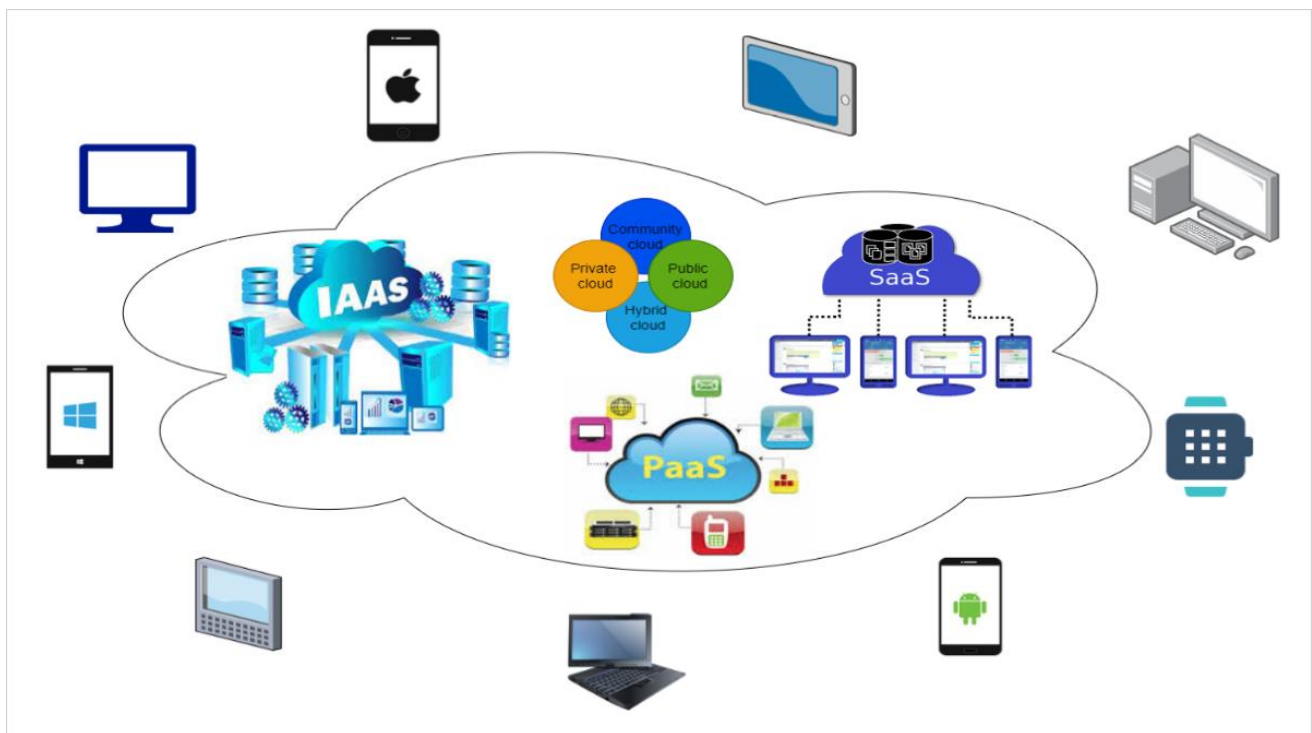


**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

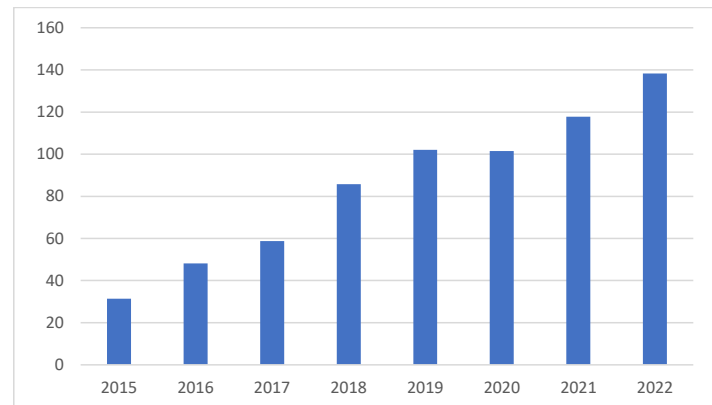
Cloud computing (CC) offers a consolidated pool of configurable computing tools and computing outsourcing processes that enable various computing services to be offered to individuals and organizations. Millions of organizations have adopted CC due to its potential benefits, such as cost efficiency, improved collaboration, scalability, flexibility, automatic software updates, business continuity, etc. [1,2] CC encompasses a wide range of services and implementation models, as shown in Figure 1. The three types of services provided by CC are platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS), and software-as-a-service (SaaS). IaaS provides options such as renting IT storage (virtual or physical) and

networking capabilities, while PaaS provides on-demand product development, training, delivery, and management tools. At the same time, SaaS is a subscription-based way of providing on-demand software applications through the cloud [3,4]. CC has four different models, namely the private cloud (PRC), the public cloud (PBC), the hybrid cloud (HYC), and the community cloud (CMC). In a PBC system, resources are shared by a group of users known as tenants. The cost of using CC is determined by how much IT infrastructure is used. On the other hand, individuals and businesses that want a PRC must have their own dedicated platform that is not shared by others. CMC is a cloud infrastructure used by users in the same industry or with common goals, and the HYC allows data and resources to be exchanged using PBC and PRC settings [5,6]. Security is one of the key challenges in all the platforms provided by CC. However, it has become a significant concern on the public SaaS cloud. The belief that storing sensitive data in a third-party data center leads to various security breaches becomes a primary obstacle to CC adoption.



**Figure 1.** CC models and services.

According to the statistics provided by Statista, the PBC SaaS market is increasing rapidly with time (as shown in Figure 2). It is a model in which the CSP hosts applications remotely and makes them accessible to consumers on-demand over the Internet. Customers benefit from the SaaS model in a variety of ways, including increased operating performance and lower costs. SaaS is quickly gaining attention as the preferred distribution model for business IT services. Most businesses, however, are still wary of the SaaS model due to a lack of insight into how their data are processed and protected. Thus, security is the top obstacle to SaaS adoption for enterprise IT infrastructures [7,8].



**Figure 2.** SaaS market size in billion USD as per Statista [9].

Various solutions for CC security in general and SaaS security are provided in the literature. However, no single solution fits all organizations under all circumstances. The security of SaaS is the joint responsibility of the cloud tenant (CT) and the cloud service provider (CSP), but customers still expect 100% security assurance from CSPs [10]. To help the SaaS CT and CSP, there is a need to provide better guidelines. This is only possible if they are aware of all possible security issues and challenges and best practices that may help overcome these challenges. To address this gap, this MVL R aims to provide a detailed overview of the opinions of researchers and practitioners (R&P) regarding SaaS security issues/challenges and best practices for secure SaaS. The objective of this MVL R is to conduct a detailed and systematic review of the scientific literature and the GL to identify SaaS security issues and challenges. This MVL R will try to answer the following research questions:

**RQ1:** What software security challenges are involved in SaaS as identified in the FL?

The aim of this question is to systematically gather and review the formal research studies published in peer-reviewed journals/conferences/workshops that focus on SaaS security issues and challenges and compile a list of potential SaaS cloud challenges. This will help SaaS CSPs and tenants to secure SaaS against internal and external threats.

**RQ2:** What software security challenges face SaaS as identified in the GL?

This research question is designed to know the practitioner's opinions on SaaS security issues/challenges. These challenges will be identified by screening the GL available on the Google search engine.

**RQ3:** Which practices are suggested by the FL for improving SaaS cloud security?

This research question aims to analyze the selected primary studies to find the best practices that help in improving the security of the SaaS cloud.

**RQ4:** Which practices are suggested by the GL for improving SaaS cloud security?

This question will identify the best practices for improving SaaS security as suggested by practitioners in this area through the analysis of the identified GL.

**RQ5:** Is there any similarity or discrepancy between R&P opinions regarding SaaS security issues and solutions?

This question will compare and analyze the results of the aforementioned four research questions to find the similarities and differences between R&P opinions.

The remaining paper organization is as follows: the background information is covered in Section 2. Section 3 summarizes the related work. The research methodology is defined in Section 4. The study's findings are presented in Section 5, which is accompanied by a review of the findings in Section 6. Section 7 concludes the paper by providing insights into future research.

## 2. Background

This section provides a general overview of some key terms related to CC with a special focus on SaaS security.

### 2.1. Cloud Computing (CC)

The cloud paradigm is not new. However, it is becoming more important to grasp the complexities of the CC language and principles as more organizations and businesses switch to cloud-based technology. According to a Cisco report, 94% of workloads will be managed by CC till 2021, compared to just 6% for conventional data centers [11]. NIST defines CC as a paradigm for providing global, useful, on-demand network access to a common pool of customizable computational resources that can be quickly provisioned and released with limited maintenance effort or intervention by service providers [12]. CC is different from traditional IT hosting systems as the user does not need to own the hardware. Rather, tenants only pay for the facilities they use [13].

### 2.2. CC Service Models

IaaS, PaaS, and SaaS are the three main service models for cloud solutions. IaaS provides customers with cloud-based storage, servers, networking, and other computing services. Although the user is still in charge of handling their programs, files, middleware, and so on, IaaS offers automated and flexible environments that give the user a lot of power and versatility. In PaaS, cloud users rent cloud-based services from service providers to build and deploy software. In other words, PaaS is a platform that makes developing, customizing, and deploying applications simpler and more effective. SaaS refers to software that is hosted, bundled, and distributed over the Internet by a third party. Enterprises will offload management and development costs to the provider by shipping business applications over the Internet. Email and customer relationship management tools are two common SaaS options [14].

### 2.3. Types of CC

PRC, PBC, and HYC are the three major cloud storage solutions. Each has its own set of benefits and drawbacks and which one a user (or company) selects will be determined by the nature of the data as well as the level of protection and management needed. A PBC is perhaps the most prominent form of CC. Both resources and supporting facilities are handled and accessed among many users off-site via the Internet (or tenants). A subscription service, such as Netflix or Hulu, is a clear example of a PBC at the individual user level. Rather than providing IT services to the public, the PRC delivers them to a small group of customers over the Internet or a private network. Various organizations adopt this option because it combines cloud mobility with greater customization and protection. Private and PBC elements are mixed in varying degrees in a HYC scheme. In relation to their freedom, the clouds in a hybrid environment operate together through an encrypted network, allowing data and applications to flow across them. This is a popular cloud solution because it provides companies with greater flexibility in fulfilling their IT needs [15,16].

### 2.4. SaaS Cloud Computing

SaaS is one of the cloud subscription service groups along with IaaS and PaaS. It allows businesses to access the programs they need without having to host them on their own servers. It has grown in popularity since it eliminates the need for organizations to buy servers and other resources, as well as retain an in-house support team. Instead, a SaaS provider hosts their applications and provides SaaS security and maintenance. Most business product providers, such as the Oracle Financials Cloud, also sell cloud implementations of their applications [17].

### 2.5. Benefits of SaaS

The global SaaS market is projected to expand at a rate of 21% annually over the next few years, hitting \$117 billion by the end of 2022 [18]. The following key factors have contributed to the rise in popularity of SaaS.

- Scalable and on-demand resources
- Quick implementation
- Easy maintenance and upgradation
- No staffing or infrastructure cost

### 2.6. SaaS Usage

In a number of cases, SaaS might be the best alternative [19], including

1. Startups and small businesses that need to open an ecommerce site immediately and do not have the resources to deal with server or device problems.
2. Short-term projects that necessitate short, simple, and cost-effective collaboration.
3. Tax applications, for example, is an example of an application that is not used very much.
4. Applications that include connectivity to both network and mobile devices

### 2.7. SaaS Security

SaaS is a widely used CC service model where security is the major issue due to its high dependence on third parties compared to other CC service models (see Figure 3). SaaS Security refers to the defense of user privacy and corporate data in subscription-based cloud applications. SaaS applications store a vast amount of personal data that can be accessed by many users from almost any device, putting privacy and critical data at risk. A large collection of enterprise software and data were hosted on in-house servers until a few years ago. From a security standpoint, this places the whole burden of proof on the operation, but at the very least, it is obvious what needs to be covered, and how. However, as more companies embraced SaaS tools, this led to increased security concerns. Since SaaS tools are hosted in the cloud, they raise new security issues, such as susceptibility to new malware and phishing attacks, as well as the risk of client data being exposed. Businesses can protect these cloud-based programs with the right SaaS Security software and by following best security practices. As a result, a thorough review of potential security issues/challenges, as well as best practices for enhancing SaaS security, is needed [20–22].

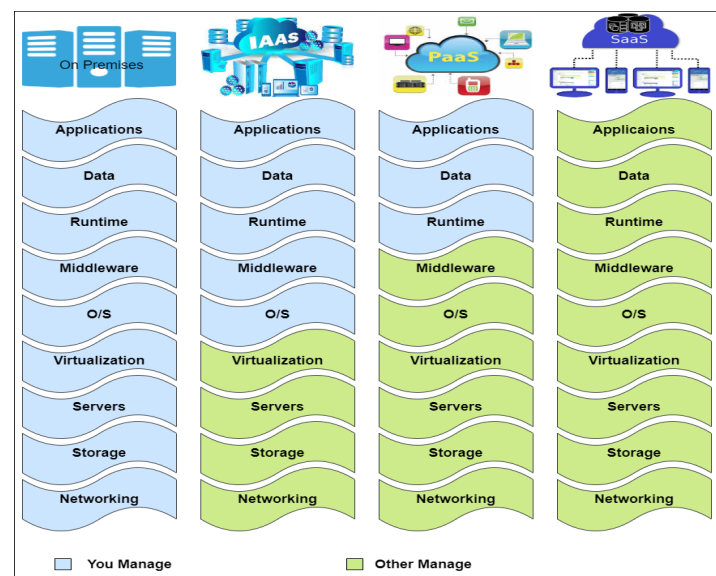


Figure 3. Comparison between three CC service models [23].



### 3. Literature Review

Before moving forward with the MVLRL, it is essential to include a review of the existing studies to understand the current state of research. This section provides a quick rundown of some current research on SaaS security issues and mitigation strategies.

Hoener performed a systematic literature review (SLR) to gather SaaS security issues and solution. This SLR identified CC security requirements from scientific publications between January 2011 and March 2013. The identified requirements were categorized into a framework to assess their frequency. This research study also identified challenges in requirement assessment and proposed a solution for it [24].

Hashizume et al. presented the security issues of three cloud service models, IaaS, PaaS, and SaaS. The main security issues in CC, as stated in this article, are storage, virtualization, and networks. This paper also makes a distinction between vulnerabilities and threats, emphasizing the importance of comprehending these problems and establishing a connection between threats and vulnerabilities to determine which vulnerabilities lead to the implementation of these threats to render the framework more resilient. To mitigate these risks, several existing solutions were also identified. According to the findings of this paper, traditional protection systems may not function well in cloud environments because they constitute a dynamic architecture made up of a variety of technologies [25].

A systematic mapping study (SMPS) was performed by Juárez and Cedillo in [26] to find the security issues of mobile computing. Based on the interpretation and assessment of 83 primary studies, this mapping study breaks down the security sub-characteristics from the ISO/IEC 25010 and compares them to the details contained in this study. The findings of the study indicate that there are sufficient studies to address the issue of confidentiality and integrity. However, accountability and non-repudiation need more attention.

A SMPS was performed by De Silva et al. to identify the security threats in CC. The aim of this study was to compile a list of the most recent publications in the literature that addressed security threats in CC. Centered on the Cloud Protection Alliance's "Top Threats to CC guide", this analysis presents metrics regarding existing research publications that deal with some of the seven security threats in CC. Furthermore, this research identified the most researched challenges, spreading the findings through 15 security domains, and identified the types of threats and solutions suggested. In view of these findings, the research focuses on publications that deal with meeting a regulatory requirement [27].

According to Zhou et al., users' use of CC technologies and applications is hampered by security and privacy concerns. The security and privacy issues raised by several CC system providers were investigated in this study. According to the results of the study, these considerations are insufficient. To meet the five goals (confidentiality, data integrity, availability, monitoring, and audit), more security techniques should be deployed in the cloud world, and privacy acts should be updated to adapt a new partnership between CSPs and CT in the cloud literature. According to the study, the CC literature needs to flourish until the protection and privacy problems are addressed [28].

Shankarwar and Pawar conduct a study of security and privacy problems as well as potential remedies. They discuss the benefits and disadvantages of the current methods to fully resolve the protection and privacy issues in the cloud world, as well as the advantages and drawbacks of existing methods to completely resolve the security and privacy issues [29]. According to Hussein and Khalid, security is still a major concern in the CC paradigm. User confidential data loss, data leakage, and the disclosure of confidential data are a few of the major security concerns. This paper presents a thorough review of the current literature on CC security issues and solutions [30].

A survey of the various security threats that pose a danger to the cloud is discussed by Kumbhar et al. This paper presents a survey focused on the various security problems that have arisen because of the nature of cloud infrastructure service distribution models. The paper discusses the security issues of three service models of CC, namely IaaS, PaaS, and SaaS in detail and provides recommendations to mitigate the mentioned threats. This paper examines CC security problems and categorizes them into different groups

depending on the category of security. Furthermore, multiple trust-based solutions are classified according to how they provide trust in a collaborative setting. The results of the paper show that trust-based approaches for the cloud exist, but this does not explicitly solve all the discussed security issues [31].

### 3.1. Motivations for the Study

The preceding discussion demonstrates that security is a significant barrier to cloud adoption, especially in the case of SaaS clouds, where the tenant is completely reliant on the CSP for data security and control. As stated in the literature review, the existing literature has highlighted numerous security issues related to CC, but there is no explicit SLR, particularly MVLR, that provides the current SOTA for SaaS security issues and solutions. To bridge the gap and to provide a detailed overview of SaaS security for R&P, we conduct this MVLR. The detail of the MVLR is presented in subsequent sections.

The aim of this MVLR is to systematically review the literature on the SOTA and state of the practice (SOTP) of SaaS security. Both peer-reviewed and non-peer-reviewed literature are included in an MVLR (i.e., a form of SLR) [32,33]. In software engineering (SE), the SLR has become the most common way to conduct a literature review [34]. SLR only considers scientific contributions and excludes the GL. Since it lacks a vast volume of information produced by SE professionals, an SLR cannot always include an existing discipline of expertise. As a result, MVLRs are drawing more focus [33,35–37]. We believe that an MVLR would be more beneficial than an SLR in the field of SaaS cloud security since there is a wide body of non-peer reviewed literature published by practitioners.

### 3.2. Contribution of the Study

In this MVLR, the basic issues and best practices for SaaS security are discussed. We looked at the current best practices to identify how to address SaaS security concerns. The following are the MLR's key contributions:

1. It offers a taxonomy of various aspects of security issues that need to be addressed.
2. It identifies best practices for improving SaaS security.

## 4. Research Methodology

The SLR and MVLR guidelines reported in the work in [34] were used to help with the framework for this MVLR. Our MVLR consists of three main phases (as shown in Figure 4). In phase-1, we develop the MVLR protocol, data extraction and analysis were undertaken in phase-2, and phase 3 provides the results, which are shown in a separate section. In the following, we discuss each phase in detail.

### 4.1. MVLR Protocol Development

The first phase of the MVLR is to develop an MVLR protocol. This phase consists of the following steps:

#### 4.1.1. Research Identification

We identified the literature by employing a search strategy focused on the five research questions listed in the paper's introduction. The aim of these questions is to gain a deeper understanding of SaaS cloud security issues and challenges and identify best practices to mitigate SaaS security issues.

#### 4.1.2. Search Strategy

The following section illustrates the search strategy that was used to acquire the relevant literature from multiple sources.

#### Sources of Data Collection

Our analysis covers the peer-reviewed FL and GL that was identified using manual and automated searches of related databases. Initially, we conducted a manual search

on Google Scholar to obtain an overview of the most recent literature and to make sure that enough literature exists in the area under research to conduct an MVL. Further, the aim of this initial search is to compile a list of primary studies that may be used for the validation of the search string. We retrieved 10 primary studies that are closely related to the posed research questions. This preliminary literature review reveals that SaaS security is a major research issue, with numerous research studies in this field. However, the problem persists, and security remains a major barrier. Further, to the best of our knowledge, there is no existing MVL on this topic. Therefore, there is a need to provide the current-SOTA picture of the SaaS security issues/challenges and best practices. In the second phase, an automated search was performed on six libraries: IEEE explorer, ACM, Science Direct, Springer, Wiley Online, and Google Scholar to retrieve the peer-reviewed literature. In the automated search, we used the advanced search option to match the search string with the title, abstract and keywords of the papers published between Jan 2010 to Jan 2021. For the GL search, we used the Google search engine similar to other MVLRs [35,36]. Since the Google search engine's algorithm retrieves and displays the most important results in the first few pages [34,36], we found the first 10 pages to be adequate for finding the most relevant literature. For example, the Google search retrieved 187,000 records for the term "SaaS security" in January 2021, however relevant content was found only in the first 10 pages.

#### Search String

To ensure a robust search through several databases, we generated a search string. For the academic literature, we generated a search string focused on:

- (a) The keywords gathered from the primary studies
- (b) Synonym and alternative words used for the identified terms
- (c) Using the logical operator AND or OR to combine these terms.

We ran several pilot searches and refined our search string to make sure that all primary studies are retrieved by applying the search string. The search string was also tailored for different libraries. In the following, we describe each part of the search string.

("SaaS" OR "software as a service" OR "Software-as-a-Service") AND ("security" OR safety OR integrity OR confidentiality OR availability) AND (issues OR challenges OR problems OR limitations) AND (Practices OR guidelines OR recommendations OR checklist)).

We used "Software-as-a-service AND security" to find the GL and applied this string on the Google search.

#### 4.1.3. Eligibility Criteria

We defined a set of inclusion and exclusion (I&E) criteria to choose the articles, as discussed in the following section. We used a narrow I&E criterion since this study is a mix of scientific FL and GL.

##### Inclusion Criteria for FL

The following points were considered for the inclusion of a FL.

- Articles are written in English and the complete text is available.
- Articles that focus on SaaS cloud security issues or challenges and solutions

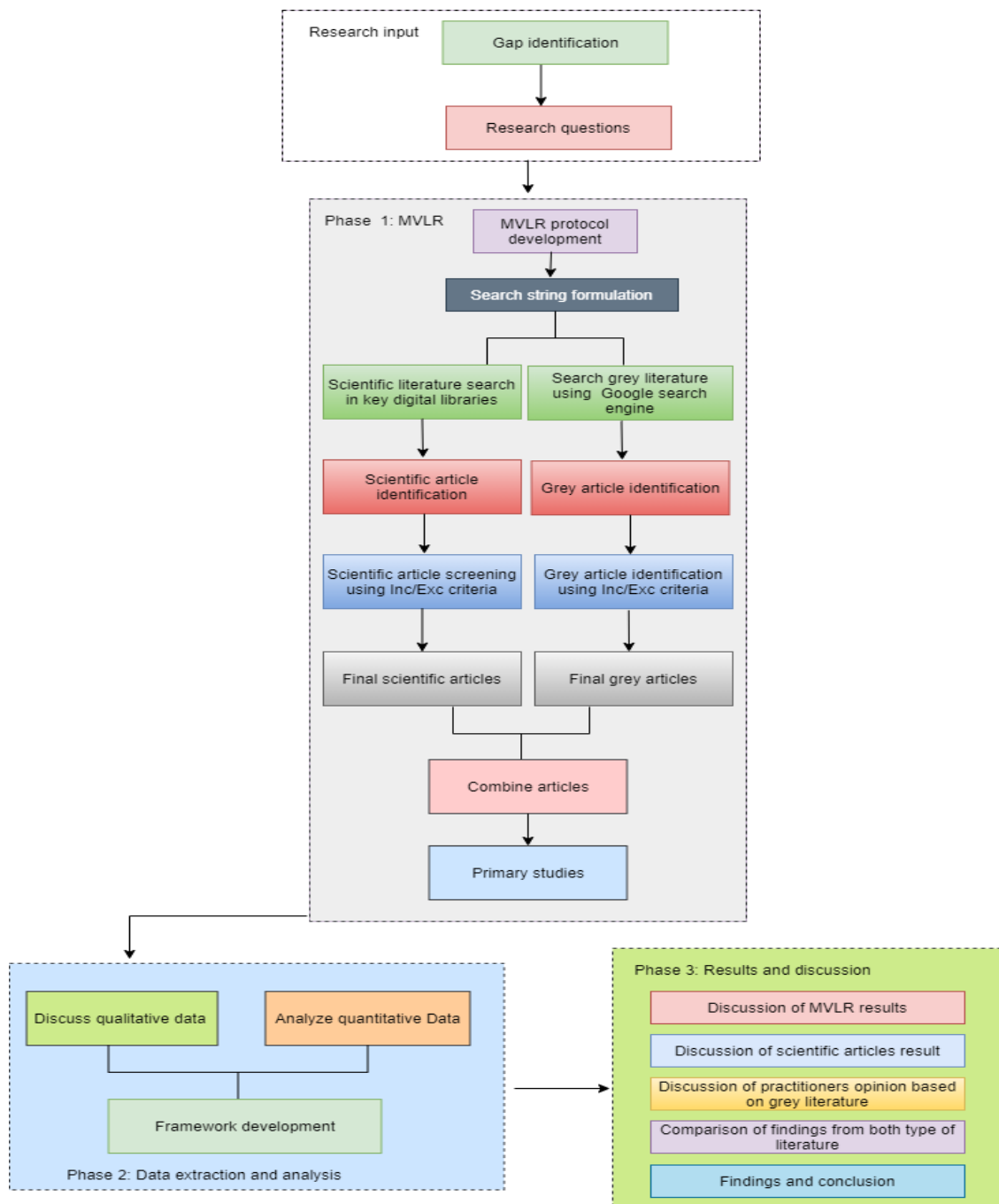
##### Exclusion Criteria for FL

- Articles whose subject matter has nothing to do with SaaS security.
- Articles not written in English.

##### Inclusion Criteria for GL

All the websites, blogs, white papers, news pages, or articles that discuss SaaS security challenges or practices to mitigate SaaS security issues were included.





**Figure 4.** MVLR methodology.

Exclusion Criteria for GL

The exclusion criteria for GL were the same as for FL. We did not consider literature that was not written in English or that was not related to SaaS security.

4.1.4. Quality Assessment (QA)

To evaluate the strength of FL and GL, we defined the separate quality assessment criteria for both types of literature. We discuss these criteria separately in the following.

Quality Assessment of FL

A QA checklist was prepared to ensure the strength of the extracted FL. This checklist includes the following points.

- The paper was cited by how many people.

The answer to this question was on a 3-point Likert scale, comprising yes, no and partial. If a paper was cited by more than 5 authors, the answer was yes, whereas if it was cited by between 1 and 5, then the answer was partial. Otherwise, the answer was no.

- Was the paper accepted in a relevant journal, or not?

The answer to this question was yes/no and it was validated by reading the journal/conference list of topics.

#### Quality Assessment of GL

The quality of the GL was evaluated based on the following questions.

- Is the publishing house a respectable one?
- Does the individual author belong to a reputable organization?
- Does the author have expertise in SaaS?

Figure 5 shows the details of the studies retrieved from different sources after applying the I&E criteria. Our search retrieved 58 scientific papers from 6 different libraries and 35 grey studies retrieved from the Google search engine (as shown in Appendices A and B).

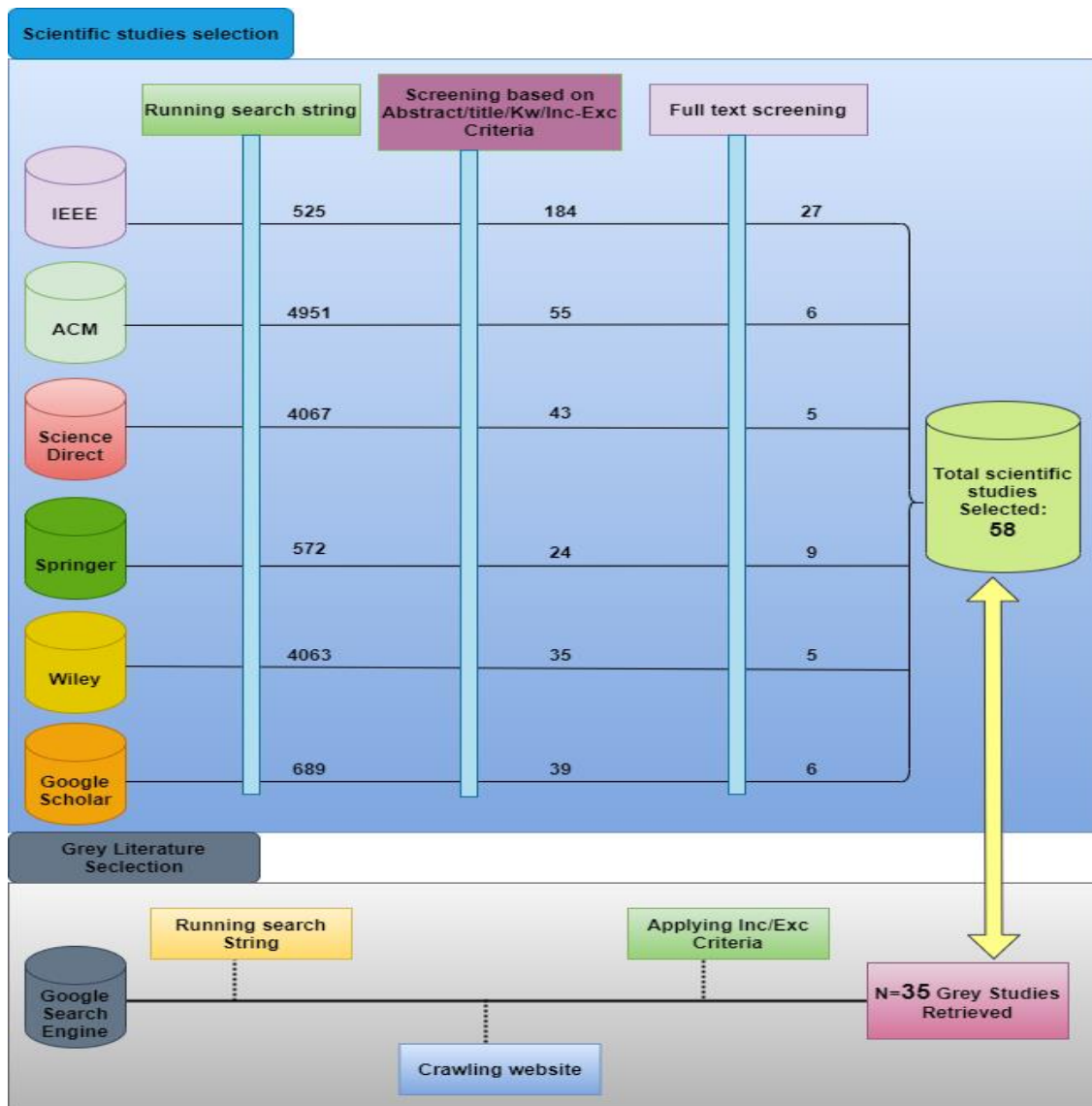


Figure 5. Article selection process for MVL.

#### 4.2. Data Extraction, Synthesis and Analysis

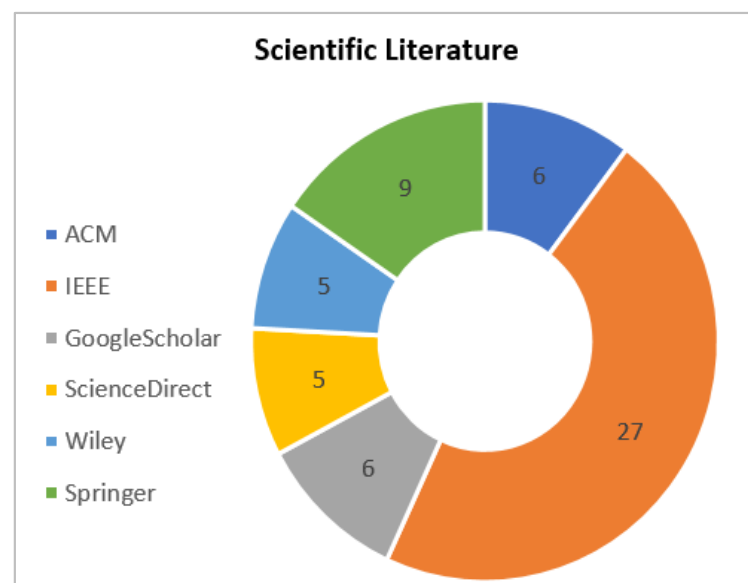
We read, evaluated, extracted data, and synthesized the results from the selected papers based on the pre-defined RQs mentioned in the introduction to this paper. We extracted relevant data from each of the chosen sources that we used to address the research questions using a pre-defined data extraction form. We also gathered some general information about the papers, such as the authors' names, the country of publication, the venue of publication (journal/conference/workshop etc.), and the year it was published. Before determining how to collect the necessary data, we performed a pilot study on a selection of ten sources.

### 5. Results

We reviewed and categorized all the FL and GL separately and together in this section to determine the existing SOTA and SOTP. Next, we compared the views of the scholars and practitioners to identify the variations and parallels.

#### 5.1. FL Analysis

This section analyzes the extracted scientific studies based on different criteria, such as the venue of publication, type of publication, year of publication, established SaaS security problems and challenges, and security best practices. The details of scientific literature retrieved from six different sources is given in Figure 6.



**Figure 6.** Details of Scientific Literature retrieved.

##### 5.1.1. Scientific Article Analysis w.r.t Venue of Publication

The distribution of studies by the venue is shown in Table 1. All the retrieved research articles are published in three venues only: journals, conferences, and workshops. We can deduce the following facts from the statistics in Table 1.

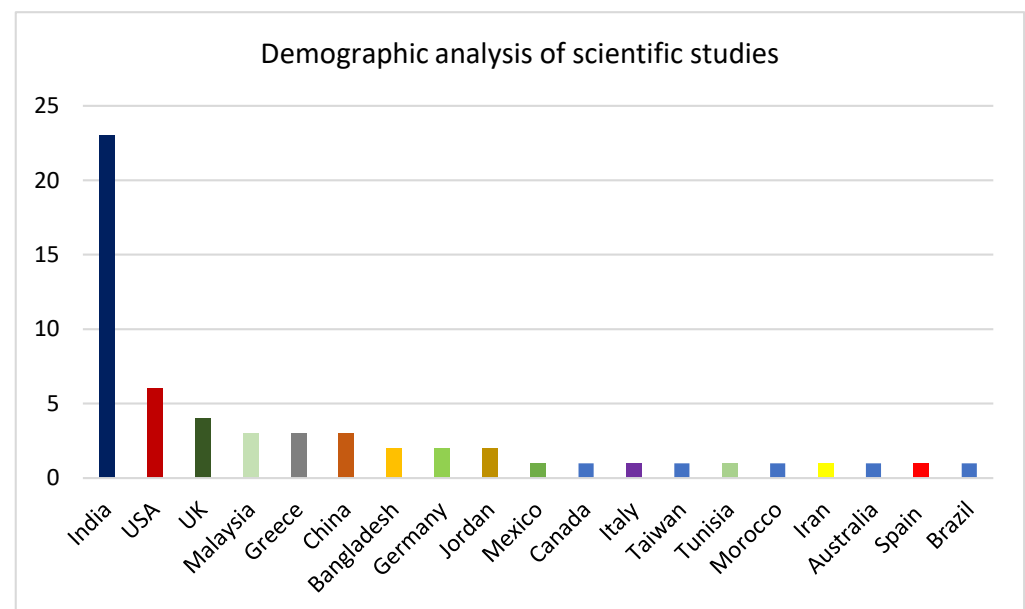
- Most of the retrieved studies that address SaaS security issues and best practices are published either in journals or conferences. There were only two studies published in workshops. One was published in the 2014 IEEE Globecom Workshop (GC Wkshps), while the other was published in IoTNAT'2016.
- IEEE, ACM, and Springer have more conference publications.
- Wiley has more journal publications.

**Table 1.** Distribution of studies w.r.t. venues.

	Journal	Conference	Workshop	Total
IEEE	0	26	1	27
ACM	1	5	0	6
Google Scholar	6	0	0	6
Science Direct	2	2	1	5
Wiley	5	0	0	5
Springer	1	8	0	9
Total	15	41	2	58

### 5.1.2. Demographic Analysis of Retrieved Scientific Studies

The author's affiliation was used to determine and rate the most involved countries in the field of SaaS security analysis. The aim of this ranking was to determine which countries' researchers are concentrating their efforts on this topic the most. If a paper had several authors, the country of the first author was selected. The demographic information of the retrieved studies is shown in Figure 7. According to Figure 7, India is the country which has published the most articles on SaaS security issues and solutions with a frequency of 23 out of 58 which is almost 40% of the total studies retrieved. The next is the USA with six out of 58 publications in the area under study, which is almost 10%. Publications from the UK were third in the pool with 4 out of 58, which is almost 7% of the total retrieved studies. Authors from Malaysia, China, and Greece each published three out of 58 studies. All the remaining studies were published by various other countries with a frequency of two and one.

**Figure 7.** Demographic analysis of scientific studies.

To classify the existing research patterns in the field of SaaS cloud security, the selected studies were also classified according to the year of publication, as shown in Figure 8. The maximum retrieved studies belong to the year 2012, 2015, and 2016 with a frequency of nine out of 58 each. Eight out of 58 studies were published in the year 2014, while seven out of 58 studies were published in 2017. Six out of 58 studies were published in 2018, three out of 58 studies were published in the year 2013 and 2019 each, while only two out of 58 studies were published in the years 2011 and 2020. The downfall in the curve of Figure 8

shows that SaaS security issues have been resolved to some extent with the advancement of the latest technologies and suitable security measures. However, some issues are still reported, which is why researchers are continuing to work in this area. The reasons for the curve’s decline can be numerous. For example, it is possible that FL and GL on SaaS security exist but do not meet our I & E criteria. Second, with time, SaaS vendors are becoming aware of the security breaches and are taking suitable measures to secure their services to satisfy SaaS users. Third, there are several SaaS vendors in the market and security is one of the important concerns to be considered by users while selecting SaaS. Therefore, SaaS vendors have started paying more attention to it.

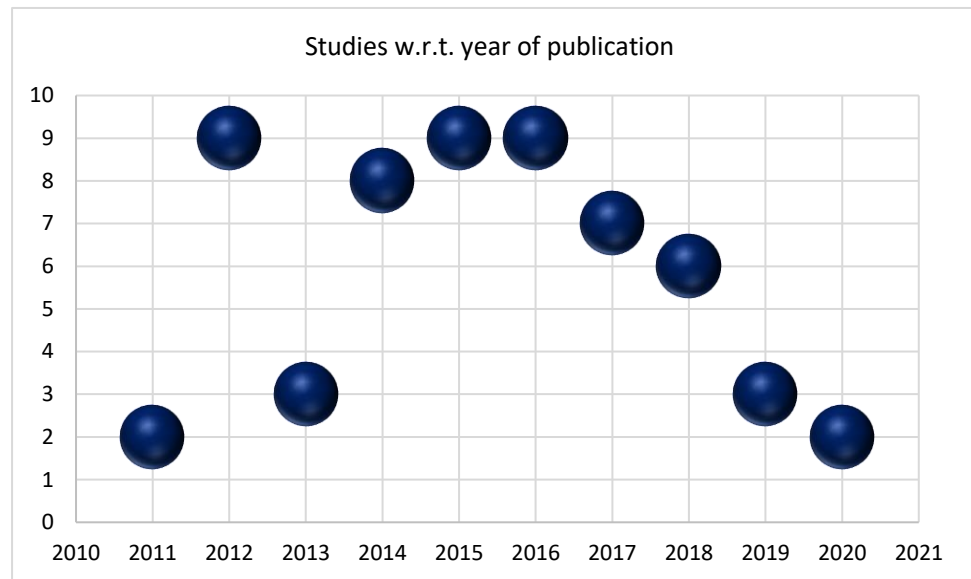


Figure 8. Retrieved studies frequency w.r.t. year of publication.

### 5.1.3. SaaS cloud Security Issues and Challenges

We selected 58 scientific studies as primary studies after applying the I&E criteria. SaaS security issues and challenges were identified after a detailed screening of these primary studies. According to the studies’ results, data loss/leakage is the key SaaS security challenge with a frequency of 41. Identity and access management and a lack of user control are the second most important challenges with a frequency of 39 each, after which is logical storage segregation and multi-tenancy/data locality with a frequency of 36. The remaining issues and challenges along with their frequency of occurrence and reference of scientific studies are detailed in Table 2.

Table 2. SaaS security issues and challenges identified from FL.

Challenges	Freq	Occurrence in FL
Data security/data loss or leakage	41	S1, S3, S4, S6, S7, S9, S11, S12, S13, S14, S15, S16, S17, S19, S22, S24, S25, S26, S27, S28, S30, S31, S32, S33, S37, S38, S39, S40, S41, S43, S45, S46, S47, S48, S50, S52, S53, S54, S55, S56, S57
Identity and access management issues	39	S3, S4, S5, S6, S7, S9, S10, S11, S12, S13, S14, S15, S16, S18, S22, S25, S26, S27, S28, S29, S30, S33, S34, S36, S37, S38, S41, S43, S44, S46, S48, S49, S50, S51, S52, S53, S55, S56, S57
Lack of user control/visibility	39	S1, S2, S4, S6, S9, S11, S12, S13, S14, S16, S17, S18, S19, S23, S24, S25, S26, S27, S28, S29, S31, S32, S35, S36, S38, S42, S43, S44, S45, S48, S49, S50, S51, S52, S53, S54, S55, S56, S58



Table 2. Cont.

Challenges	Freq	Occurrence in FL
Logical storage segregation & multi-tenancy/data locality	36	S1, S4, S5, S6, S9, S11, S12, S13, S14, S16, S17, S19, S20, S21, S24, S25, S26, S27, S28, S30, S31, S34, S38, S41, S42, S43, S45, S48, S49, S50, S51, S52, S54, S56, S57, S58
Insecure interfaces and APIs	31	S1, S4, S5, S6, S8, S9, S13, S14, S16, S27, S30, S32, S34, S36, S38, S39, S40, S41, S43, S44, S46, S47, S49, S50, S52, S53, S54, S55, S56, S57, S58
Governance and regulatory compliance/SLA compliance	30	S4, S5, S6, S9, S10, S13, S15, S16, S18, S23, S26, S27, S28, S29, S31, S34, S37, S38, S42, S43, S44, S45, S49, S51, S52, S53, S54, S55, S56, S58
Network security/shared technology	29	S4, S6, S8, S9, S10, S11, S12, S13, S14, S17, S18, S21, S22, S24, S25, S26, S27, S28, S33, S41, S48, S50, S51, S52, S53, S54, S56, S57, S58
Virtualization issues/cloud & CSP migration issues	27	S3, S5, S6, S9, S12, S13, S17, S18, S19, S23, S25, S27, S30, S31, S32, S34, S37, S38, S37, S41, S45, S48, S49, S51, S52, S55, S57
Malicious insiders	20	S1, S3, S5, S6, S9, S13, S16, S27, S28, S36, S44, S45, S46, S47, S49, S51, S53, S55, S56, S57
Backup and recovery	17	S4, S11, S12, S13, S14, S16, S24, S25, S27, S29, S30, S42, S50, S54, S55, S57, S58
Lack of trust between the cloud provider and client	10	S1, S23, S28, S38, S44, S45, S53, S55, S56, S58
Transit security	8	S10, S25, S31, S37, S40, S52, S55, S48
Insecure or incomplete data deletion	5	S16, S27, S32, S38, S41,
Lack of expertise	5	S1, S18, S23, S26, S55
Others	3	

The issues or challenges with a frequency of one are combined under the heading 'others', including not incorporating security into SDLC, documentation, and different service delivery/receiving models.

The aim of identifying these SaaS security challenges and issues is to address our research question one (RQ1). This will help SaaS customers and service providers to gain an in-depth overview of SaaS security issues. Addressing these challenges will help to improve the security of the SaaS cloud.

#### 5.1.4. SaaS Security Best Practices

We also analyzed the primary studies to extract SaaS security best practices to enhance the awareness of SaaS R&P about the SOTA. The best practices for improving SaaS security are detailed in Table 3. According to the results in Table 3, up-to-date security controls/standards represent the practice that is suggested by most researchers with a frequency of 39. The second-most mentioned practice for maintaining SaaS cloud security as suggested by the researchers is the use of strong encryption techniques with a frequency of 38. The third-most suggested practices for improving SaaS security are regulatory compliance/SLA compliance and multifactor authentication with a frequency of 24 each. The remaining best practices along with their frequency of occurrence and the studies in which they appeared are detailed in Table 3.

The best practices which were discussed in a single study only (with a frequency of one) were categorized under the heading 'others', including governments should keep their information assurance architectures secure and confidential, conduct service integrity test, interoperability management, and service conformity.

## 5.2. GL Analysis

This section analyzes the GL to obtain the practitioners' opinions about SaaS security issues and solutions. The selected GL is discussed based on different criteria, such as venue of publication, type of publication, year of publication, established SaaS security problems and challenges, and security best practices.

### 5.2.1. GL Analysis w.r.t Venue of Publication

To identify the GL related to SaaS security issues and best practices, we used the Google search engine. We applied the search string "SaaS security" on the Google search engine. The retrieved records belong to various categories, including white papers, blogs, websites, news, etc. The Google search engine retrieved thousands of records corresponding to our search string, but the relevant records were found in the first 10 pages only. We also checked the remaining few pages, but either the records were repeating, or they were not related to our search domains. The total number of selected GL was 35, as shown in Figure 9. These 35 records include 13 websites, nine blogs, eight reports, and five white papers.

**Table 3.** SaaS security best practices as identified from FL.

Practices	Freq	Occurrence in FL
Up-to-date security controls/standards	39	S2, S3, S6, S8, S10, S11, S12, S13, S14, S16, S17, S20, S22, S23, S24, S27, S28, S29, S31, S33, S36, S37, S38, S39, S40, S43, S44, S45, S46, S47, S49, S50, S51, S52, S53, S54, S56, S57, S58
Use of strong encryption techniques/standards	38	S2, S3, S5, S6, S7, S11, S12, S14, S15, S16, S17, S22, S23, S24, S25, S26, S28, S29, S30, S31, S32, S33, S36, S37, S38, S39, S42, S44, S46, S47, S49, S50, S52, S53, S54, S55, S56, S57
Regulatory compliance/SLA compliance	24	S2, S5, S6, S11, S12, S13, S16, S23, S25, S27, S28, S29, S37, S38, S42, S44, S48, S49, S50, S51, S52, S55, S57, S58
Multifactor authentication	24	S6, S11, S14, S16, S23, S26, S27, S28, S29, S33, S36, S37, S39, S41, S46, S47, S49, S50, S52, S53, S54, S55, S56, S57
Better enterprise infrastructure/proper data isolation	23	S1, S5, S6, S12, S13, S14, S17, S21, S25, S26, S28, S29, S36, S37, S38, S42, S43, S44, S50, S52, S55, S56, S57
Backing up /disaster recovery plan/proper disposal	20	S6, S12, S14, S18, S24, S25, S26, S28, S29, S36, S37, S38, S42, S43, S44, S49, S52, S53, S55, S58
Third party auditing	12	S3, S6, S12, S16, S27, S28, S31, S38, S44, S49, S50, S51, S52, S57, S58
Transit security	12	S6, S12, S16, S25, S26, S27, S36, S40, S42, S46, S52, S55
Consumer awareness/employee education/training	8	S10, S23, S24, S28, S36, S49, S50, S51
Incorporate security into SDLC	4	S35, S36, S45, S39
Others	4	

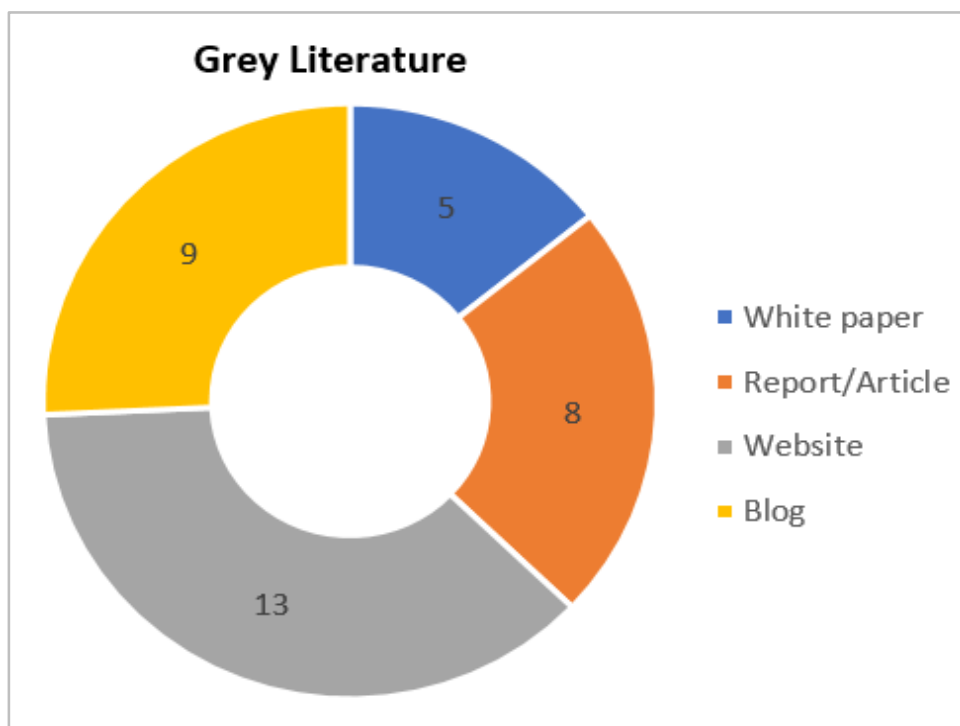


Figure 9. Details of GL retrieved.

### 5.2.2. Demographic Analysis of GL

While extracting the GL, we also collected demographic information (country in which the literature was published) to identify from which area practitioners are more active in providing their practical experience about SaaS security issues and solutions. Most of the websites and articles which were selected as GL were published in the USA, while only a few were published in other countries, including Canada, UK, India, Netherlands, and Estonia. This shows that practitioners from the USA are more concerned about CC security, especially SaaS security. However, the key aim of analyzing the GL was to extract SaaS security issues/challenges and best practices, and as some of the GL, especially websites, do not pertain to a specific year, we did not present this information.

### 5.2.3. SaaS Security Issues/Challenges Identified from GL

This section aims to answer RQ2 by identifying practitioners’ opinions on SaaS security issues. According to the obtained results, data breaches/leakages is a key challenge faced by SaaS clouds with a frequency of 21, followed by identity and access management with a frequency of 17. Loss of control/visibility, an inability to maintain regulatory compliance, and an inability to monitor data in transit to and from cloud applications constituted the third-most frequently discussed challenge facing practitioners with a frequency of 10 each. The remaining challenges, frequency of occurrence, and the GL in which it was discussed are detailed in Table 4.

Table 4. SaaS security issues and challenges (practitioners’ opinions).

Issues	Freq	Occurrence in GL Reference
Data breaches/leakage	21	GL1, GL2, GL6, GL7, GL8, GL9, GL10, GL11, GL12, GL15, GL17, GL19, GL21, GL22, GL23, GL26, GL29, GL30, GL31, GL33, GL34
Identity and access management	17	GL1, GL2, GL4, GL6, GL7, GL8, GL10, GL12, GL17, GL18, GL21, GL22, GL24, GL26, GL27, GL28, GL34

**Table 4.** *Cont.*

Issues	Freq	Occurrence in GL Reference
loss of control/visibility	10	GL4, GL5, GL6, GL7, GL8, GL10, GL12, GL18, GL24, GL31
Inability to maintain regulatory/standard compliance	10	GL1, GL5, GL6, GL7, GL8, GL12, GL24, GL26, GL30, GL31
Inability to monitor data in transit to and from cloud applications	10	GL5, GL7, GL8, GL10, GL16, GL19, GL24, GL26, GL30, GL27
Insider threats	7	GL3, GL5, GL6, GL11, GL12, GL19, GL27
Non-standard API interfaces	6	GL1, GL4, GL16, GL17, GL28, GL34
Lack of security detection expertise	6	GL4, GL5, GL8, GL19, GL22, GL33
Lack of robust service level agreements (SLAs)	6	GL8, GL12, GL15, GL18, G26, G30
Multi-tenant environment	6	GL2, GL3, GL5, GL11, GL16, GL22
Virtualization	5	GL1, GL12, GL18, GL22, G24
Backup and data destruction	3	GL1, GL26, GL30
Paying upfront and long-term	3	GL8, GL18, GL33
Heterogeneous devices	3	GL18, GL21, GL27
trust	2	GL1, GL32
SaaS deployment model	2	GL26, GL30
Cost	1	GL33

#### 5.2.4. Best Practices for Improving SaaS Cloud Security (Practitioners' Opinions)

The selected GL was evaluated to extract suitable solutions/best practices to mitigate SaaS security issues and improve security. This will provide the practitioners' opinions regarding SaaS security. The extracted results are shown in Table 5. According to the results in Table 5, 26 out of 35 practitioners emphasize data encryption to ensure the security of SaaS cloud data, while governance and regulatory/standard compliance audits were suggested by 22 out of 35 practitioners. The third commonly agreed solution for improving SaaS security was the use of backups/recovery. The remaining best practices/solutions are detailed in Table 5 along with their frequency of occurrence and the corresponding GL reference.

**Table 5.** SaaS security solutions/best practices (practitioners' opinion).

Best Practices	Freq	Occurrence in GL Reference
Data protection and encryption	26	GL2, GL3, GL4, GL6, GL8, GL9, GL10, GL12, GL13, GL14, GL15, GL16, GL17, GL18, GL19, GL20, GL21, GL23, GL24, GL25, GL27, GL28, GL29, GL30, GL34, GL35
Governance and regulatory/standard compliance audits	22	GL1, GL2, GL4, GL5, GL6, GL7, GL8, GL9, GL12, GL13, GL14, GL19, GL20, GL23, GL24, GL26, GL27, GL29, GL30, GL33, GL34, GL35
Backups/recovery	20	GL1, GL2, GL4, GL8, GL10, GL13, GL14, GL15, GL17, GL18, GL19, GL20, GL23, GL24, GL25, GL27, GL29, GL30, GL34, GL35
Use advanced threat protection mechanism	19	GL2, GL5, GL6, GL9, GL10, GL12, GL13, GL14, GL15, GL16, GL18, GL20, GL21, GL22, GL23, GL24, GL27, GL32, GL34

Table 5. Cont.

Best Practices	Freq	Occurrence in GL Reference
Multifactor authentication	18	GL1, GL2, GL3, GL4, GL6, GL9, GL10, GL11, G14, GL19, GL20, GL21, GL23, GL24, GL25, GL27, GL30, GL34
Cloud-based identity and access management solutions	18	GL2, GL4, GL11, GL12, GL13, GL14, GL16, GL17, GL20, GL22, GL25, GL26, GL27, GL28, GL30, GL31, GL34, GL35
Better enterprise infrastructure	16	GL1, GL2, GL5, GL12, GL13, GL14, GL18, GL22, GL23, GL24, GL25, GL26, GL27, GL30, GL 31, GL33
Security expertise	12	GL2, GL11, GL12, GL14, GL20, GL21, GL22, GL23, GL27, GL29, GL31, GL33
Incorporating security in the SDLC process	6	GL12, GL17, GL26, GL30, GL33, GL34
SLA management	5	GL1, GL8, GL 15, GL31, GL32
Customer Support	4	GL9, GL12, GL22, GL29
Others	3	

Some best practices were only suggested by a single practitioner. Hence, we combined all the practices with a frequency one into the category of ‘others’. The practices which fall in the category of others include: watch for OWASP’s top security issues, being careful with deadlines, and make security a priority.

## 6. Discussion

This MVLR has examined the pertinent factors that motivate the need to recognize SaaS security problems/challenges and the best practices that can resolve these security issues. We identified the current security challenges and best practices for improving SaaS cloud security issues during this study. Security improvements are being more widely recognized to accelerate SaaS cloud adoption. R&P from all over the world have been working for years to identify SaaS cloud security problems and challenges, as well as practices that can help solve these issues. However, the problem still persists, and challenges are reported from time to time. Therefore, this area has significant potential for innovation and research. Before proceeding to provide more solutions to existing security issues, there is a need to synthesize R&P opinions at a single place to provide the complete and current picture of the situation. To fill this gap, this MVLR has compiled a list of possible challenges from the FL and GL to raise the awareness of the cloud tenants as well as CSPs. Further, we also compiled practices for improving the security of the SaaS cloud both from the GL and peer-reviewed literature. This will help R&P address these issues and improve their SaaS cloud performance and adaption. In the following, we discuss these results in the light of the posed research questions.

**RQ1:** What software security challenges are involved in SaaS as identified in the FL?

This research question aimed to identify the SaaS security issues and challenges discussed by researchers in this area. A total of 58 studies were selected as primary studies after applying I&E criteria. When these studies were analyzed to find the SaaS security issues or challenges, about 18 challenges were identified from 58 primary studies. The frequency of the identified challenges was also calculated to understand the severity of each challenge. According to our results, the challenges with a higher frequency were: data security/data loss or leakage, identity and access management issues, lack of user control/visibility, logical storage segregation & multi-tenancy/data locality, insecure interfaces and APIs, and governance/regulatory compliance/SLA compliance with a frequency of 41, 39, 39, 36, 31, and 30, respectively. Network security/shared technology, virtualization issues/cloud & CSP migration issues, and malicious insiders were also key challenges with a frequency of 29, 27, and 20, respectively. Other challenges are also detailed in Table 2. The data in



Table 2 provide a detailed overview of the SaaS security issues and challenges. This study will help R&P to obtain an overview of possible security issues and challenges. Based on these identified challenges, organizations can evaluate their current security breaches and can find timely solutions for these issues.

**RQ2:** What software security challenges are involved in SaaS as identified in the GL?

Many researchers have identified general SaaS security issues from the FL. However, we did not find any study that has compiled R&P opinions together in a single study. To fill this gap and to provide a detailed overview of possible SaaS security issues as identified by academia and industry, this MVLRL also extracted SaaS security issues from the GL. A total of 35 studies were selected as the GL, which include white papers, blogs, websites, and reports. According to our findings, the key security challenges identified by practitioners include data breaches/leakage, identity and access management, loss of control/visibility, inability to maintain regulatory/standard compliance and inability to monitor data in transit to and from cloud applications with a frequency of 21, 17, 10, 10, and 10 respectively. The detailed results are presented in Table 4. This will help SaaS tenants and CSPs obtain an overview of the practitioners' opinions on SaaS security issues and challenges.

**RQ3:** Which practices are suggested by the FL for improving SaaS cloud security?

This research question aims to analyze the selected primary studies to find the best practices that help in improving the security of the SaaS cloud. The mere identification of SaaS issues or challenges is not enough. Therefore, we extracted the solutions/best practices from these studies. Hence, 58 primary studies were also evaluated to find the security best practices, with a total of 14 practices identified from the peer-reviewed FL which provides a detailed overview of academia regarding SaaS security improvement. According to our findings, the researchers consider up-to-date security controls/standards, the use of strong encryption techniques, regulatory compliance/SLA compliance, multifactor authentication, and better enterprise infrastructure/proper data isolation as key practices for improving security with a frequency of 39, 38, 24, 24, and 23, respectively. A detailed list of these practices is given in Table 3. The results in Table 3 will help SaaS tenants and CSPs in relation to security analysis and improvement.

**RQ4:** Which practices are suggested by the GL for improving SaaS cloud security?

The experience of the people who are working in the industry is very useful in making any decision. To improve SaaS security, we also collected the opinions of practitioners who are actually working with SaaS and identified a list of practices mentioned by these practitioners. A total of 35 studies from the GL were evaluated and about 14 practices were identified from these studies that may help in improving SaaS security. According to practitioners, the most useful practices (based on frequency of occurrence) are data protection and encryption, governance and regulatory/standard compliance, and backups/recovery with a frequency of 26, 22, and 20 respectively. The complete list of practices identified from the GL is given in Table 5. The data in Table 5 will help SaaS tenants and CSPs to evaluate their current security structure and will help them in relation to further improvement.

**RQ5:** Is there any similarity or discrepancy between R&P opinions regarding SaaS security issues and solutions?

To compare academia and industry views regarding SaaS security issues and solutions, we analyzed the data presented in Tables 2–5. The security issues identified by academia and industry were almost same with a varying frequency of occurrence. Tables 6 and 7 provide the similarities and differences between R&P opinions regarding SaaS security issues /challenges and best practices, respectively.

**Table 6.** Comparison of GL and FL regarding SaaS security challenges.

Challenges Discussed in FL Only	Challenges Discussed in GL Only	Combined Issues/Challenges
Lack of trust between the cloud provider and client	Paying upfront and long-term	Data breaches/leakage
Network security/shared technology	Heterogeneous devices	Identity and access management
Not incorporating security into SDLC		Governance and regulatory compliance/SLA compliance
Different service delivery or receiving models.		Malicious insiders
Documentation		Transit security
		Non-standard API interfaces
		Backup and recovery
		Lack of expertise
		Insecure or incomplete data deletion
		Virtualization issues/cloud & CSP migration issues
		Multi-tenant environment

**Table 7.** Comparison of GL and FL regarding SaaS security best practices.

Practices Discussed in FL Only	Practices Discussed in GL Only	Combined Practices
Third party auditing	Customer Support	Up-to-date security controls/standards
Governments should keep their information assurance architectures secure and confidential	Watch for OWASP’s Top Security Issues, be careful with deadlines and make security a priority.	Use of strong encryption techniques
Conduct service integrity test		Regulatory compliance/SLA compliance
Interoperability management and service conformity.		Multifactor authentication
		Cloud-based identity and access management solutions
		Backups/recovery
		Better enterprise infrastructure
		Security expertise
		Incorporating security in the SDLC process
		Transit security

The results of Table 6 shows that R&P are almost on the same pace regarding most of the issues/challenges facing SaaS security, as shown by the data in column 3 of Table 6.

The results of Table 7 shows that R&P are on the same pace regarding the best practices for SaaS security improvement. This shows that the provided MVLRL is very helpful in identifying SaaS security challenges and solutions. According to the results of Table 7, SaaS security can be computed as

$$SS = \sum_{i=1}^4 X_i + \sum_{j=1}^2 Y_j + 2 \sum_{k=1}^{10} Z_k \tag{1}$$

where  $SS$  denotes SaaS security,  $X_i$  refers to the security best practices mentioned in FL only,  $Y_j$  refers to the security best practices mentioned in GL only, and  $Z_k$  refers to the

security best practices mentioned both in FL and GL. The coefficient 2 with  $Z_k$  shows the dual weightage of these practices as both researchers and practitioners are in agreement about them.

To calculate the security  $\sum_{i=1}^4 X_i$ , we need to assign individual weightage to each practice according to its importance to the organization. The general calculation will be computed as

$$\sum_{i=1}^4 X_i = w_1x_1 + w_2x_2 + w_3x_3 + w_4x_4 \quad (2)$$

where  $w_1 \dots w_4$  are weights assigned to different practices, in the same way

$$\sum_{j=1}^2 Y_j = w_1y_1 + w_2y_2 \quad (3)$$

$$\sum_{k=1}^{10} Z_k = w_1z_1 + w_2z_2 + w_3z_3 + w_4z_4 + w_5z_5 + w_6z_6 + w_7z_7 + w_8z_8 + w_9z_9 + w_{10}z_{10} \quad (4)$$

The total security will be measured as

$$SS = (w_1x_1 + w_2x_2 + w_3x_3 + w_4x_4) + (w_1y_1 + w_2y_2) + 2(w_1z_1 + w_2z_2 + w_3z_3 + w_4z_4 + w_5z_5 + w_6z_6 + w_7z_7 + w_8z_8 + w_9z_9 + w_{10}z_{10}) \quad (5)$$

### 6.1. Study Implications for Both Academic and Industry

The findings of this MVLRL will help SaaS tenants and CSPs to better understand the SaaS security challenges in detail. Taking benefit of this study, SaaS users will also come to know the most suitable solutions for addressing SaaS security challenges. The combined opinions of R&P will further strengthen their belief in the identified security challenges and solutions. The study also identifies the similarities and differences between SOTA and SOTP. This implies that SaaS CSPs can make real-time decisions to improve their security and SaaS adaptability. SaaS customers/tenants can also benefit from this study and play their part in improving SaaS security.

### 6.2. Research Limitations

There are some possible limitations to this research study. Since SaaS security problems and solutions constitute a complex paradigm with several terms, the search string used to find relevant articles could have missed some related terms. The study team established the I&E criteria that were used to evaluate and select the studies that were analyzed. The emphasis of this MVLRL is not on an in-depth discussion of the reported solutions' limitations. We recommend that readers use the conclusions from this article with the aforementioned shortcomings in mind. Furthermore, some of the identified security concerns do not entirely meet the security standards of certain organizations.

## 7. Conclusions and Future Work

This paper provides the details of an MVLRL that was conducted to better understand R&P opinions on SaaS security issues/challenges and solutions to improve SaaS cloud security. A total of 93 studies were extracted from the period from January 2010 to January 2021, including 58 scientific studies and 35 grey studies. The studies were retrieved using a search string and the studies which were included in this MVLRL were extracted based on defined I&E criteria. First, we evaluated the scientific studies and provided a demographic analysis of these studies to identify the countries in which researchers are more active in research in this area. We also identified the key venues for publications in this area and in which years more studies were published. However, the key aim of the MVLRL was to extract security issues/challenges and best practices to provide a complete SaaS security guide for SaaS tenants and CSPs. A total of 75 security issues and 44 best practices were extracted from 58 scientific studies, which are listed in Tables 2 and 3. The GL was also analyzed to obtain practitioners' opinions on SaaS security challenges and solutions. A total of 55 security issues/challenges and 47 best practices were identified from 35 grey studies. This MVLRL provides a broad picture of the possible SaaS security issues and solutions for

SaaS users. Further, SaaS vendors can evaluate their current security measures in the light of the mentioned security challenges and best practices. In the future, we plan to extend our research by proposing a standard solution to address SaaS security based on the issues and challenges identified in this MVL. Furthermore, we are planning to map the identified challenges with best practices in order to provide deeper insights to the SaaS vendors so that they can take appropriate measures when they encounter any security challenges.

**Author Contributions:** Conceptualization, M.H. and M.N.; methodology, M.H. and M.N.; software, M.F.A.; validation, S.M. and M.A. and N.Z.J.; formal analysis, M.H. and M.N.; investigation, M.H., M.N., S.M. and M.A.; resources, M.H., M.F.A. and M.N.; data curation, M.H.; writing—original draft preparation, M.H.; writing—review and editing, M.N., S.M., N.Z.J. and M.A.; visualization, M.H.; supervision, M.N.; project administration, M.N.; funding acquisition, M.F.A. and S.M. All authors have read and agreed to the published version of the manuscript.

**Funding:** The authors would like to acknowledge the support provided by the Deanship of Research Oversight and coordination at King Fahd University of Petroleum and Minerals, Saudi Arabia, under Research Grant DF191039.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Acknowledgments:** The authors would like to acknowledge the support provided by the Deanship of Research Oversight and coordination at King Fahd University of Petroleum and Minerals, Saudi Arabia, under Research Grant DF191039.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Appendix A. Primary Scientific Studies

- S1 Yu, Huiming, Nakia Powell, Dexter Stenbridge, and Xiaohong Yuan. “Cloud computing and security challenges”. In Proceedings of the 50th Annual Southeast Regional Conference, pp. 298–302. 2012.
- S2 Freet, David, Rajeev Agrawal, Sherin John, and Jessie J. Walker., “Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS”. In Proceedings of the 7th International Conference on Management of computational and collective intelligence in Digital EcoSystems, pp. 148–155. 2015.
- S3 Roy, Arpan, Santonu Sarkar, Rajeshwari Ganesan, and Geetika Goel. “Secure the cloud: From the perspective of a service-oriented organization”. *ACM Computing Surveys (CSUR)* 47, no. 3 (2015): 1–30.
- S4 Nishad, Lahar Singh, Jaya Paliwal, Roli Pandey, Sumitra Beniwal, and Sarvesh Kumar. “Security, Privacy Issues and challenges In Cloud Computing: A Survey”. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, pp. 1–7. 2016.
- S5 Srinivasan, Madhan Kumar, K. Sarukesi, Paul Rodrigues, M. Sai Manoj, and P. Revathy. “State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment”. In Proceedings of the international conference on advances in computing, communications and informatics, pp. 470–476. 2012.
- S6 Chraibi, Mhammed, Hamid Harroud, and Abdelilah Maach. “Classification of security issues and solutions in cloud environments”. In Proceedings of International Conference on Information Integration and Web-based Applications & Services, pp. 560–564. 2013.
- S7 Cao, Xi, Li Xu, Yuexin Zhang, and Wei Wu. “Identity-based proxy signature for cloud service in saas”. In 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems, pp. 594–599. IEEE, 2012.

- S8 Yi, Leo, and Kai Miao. "One Solution to Improve the Confidentiality of Customer's Private Business Data in SaaS Model". In 2012 International Conference on Cloud and Service Computing, pp. 138–142. IEEE, 2012.
- S9 Grover, Jitender, and Mohit Sharma. "Cloud computing and its security issues—A review". In Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1–5. IEEE, 2014.
- S10 Girma, Anteneh, Moses Garuba, and Jiang Li. "Analysis of security vulnerabilities of cloud computing environment service models and its main characteristics". In 2015 12th International Conference on Information Technology-New Generations, pp. 206–211. IEEE, 2015.
- S11 Murray, Acklyn, Geremew Begna, Ebelechukwu Nwafor, Jeremy Blackstone, and Wayne Patterson. "Cloud service security & application vulnerability". In SoutheastCon 2015, pp. 1–8. IEEE, 2015.
- S12 Tiwari, Pradeep Kumar, and Sandeep Joshi. "A review of data security and privacy issues over SaaS". In 2014 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1–6. IEEE, 2014.
- S13 Shariati, S. Mahdi, and M. Hossein Ahmadzadegan. "Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection". In 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), pp. 1078–1082. IEEE, 2015.
- S14 Pandey, Subhash Chandra. "An efficient security solution for cloud environment". In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPEs), pp. 950–959. IEEE, 2016.
- S15 Jana, Bappaditya, Jayanta Poray, Tamoghna Mandal, and Malay Kule. "A multilevel encryption technique in cloud security". In 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), pp. 220–224. IEEE, 2017.
- S16 Kaura, Wg Cdr Nimit, and Abhishek Lal. "Survey paper on cloud computing security". In 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1–6. IEEE, 2017.
- S17 Suraj, A.R., Sneha Janani Shekar, and G.S. Mamatha. "A robust security model for cloud computing applications". In 2018 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), pp. 018–022. IEEE, 2018.
- S18 Akinrolabu, Olusola, Steve New, and Andrew Martin. "Assessing the security risks of multicloud saas applications: A real-world case study". In 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 81–88. IEEE, 2019.
- S19 Narang, Ashima, and Deepali Gupta. "A Review on Different Security Issues and Challenges in Cloud Computing". In 2018 International Conference on Computing, Power and Communication Technologies (GUCON), pp. 121–125. IEEE, 2018.
- S20 Almorsy, Mohamed, John Grundy, and Amani S. Ibrahim. "Tosma: A tenant-oriented saas security management architecture". In 2012 IEEE fifth international conference on cloud computing, pp. 981–988. IEEE, 2012.
- S21 Saleh, Eyad, Johannes Sianipar, Ibrahim Takouna, and Christoph Meinel. "SecPlace: A Security-Aware Placement Model for Multi-tenant SaaS Environments". In 2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing and 2014 IEEE 11th Intl Conf on Autonomic and Trusted Computing and 2014 IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops, pp. 596–602. IEEE, 2014.
- S22 Kim, Donghoon, and Mladen A. Vouk. "A survey of common security vulnerabilities and corresponding countermeasures for SaaS". In 2014 IEEE Globecom Workshops (GC Wkshps), pp. 59–63. IEEE, 2014.



- S23 Saa, Pablo, Oswaldo Moscoso-Zea, Andrés Cueva Costales, and Sergio Luján-Mora. "Data security issues in cloud-based Software-as-a-Service ERP". In 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1–7. IEEE, 2017.
- S24 Patil, Sulabha, Raiiv Dharaskar, and Vilas Thakare. "Digital Forensic in Cloud: Critical Analysis of Threats and Security in IaaS, SaaS and PaaS and Role of Cloud Service Providers". In 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), pp. 1–7. IEEE, 2017.
- S25 Maheshwari, Ritu, Aayushi Toshniwal, and Avnish Dubey. "Software As A Service Architecture and its Security Issues: A Review". In 2020 Fourth International Conference on Inventive Systems and Control (ICISC), pp. 766–770. IEEE, 2020.
- S26 Moghaddam, Faraz Fatemi, Mohammad Ahmadi, Samira Sarvari, Mohammad Es-lami, and Ali Golkar. "Cloud computing challenges and opportunities: A survey". In 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN), pp. 34–38. IEEE, 2015.
- S27 Bokhari, Mohammad Ubaidullah, Qahtan Makki, and Yahya Kord Tamandani. "A survey on cloud computing." In Big Data Analytics, pp. 149–164. Springer, Singapore, 2018.
- S28 Tianfield, Huaglory. "Security issues in cloud computing". In 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 1082–1089. IEEE, 2012.
- S29 Banka, Ankit, Anshul Saravgi, Mangal Sain, and Hoon Jae Lee. "Exploration of security parameters to evaluate SaaS". In 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1–6. IEEE, 2013.
- S30 Chouhan, Pushpinder Kaur, Feng Yao, and Sakir Sezer. "Software as a service: Understanding security issues". In 2015 science and information conference (sai), pp. 162–170. IEEE, 2015.
- S31 Ahmed, Iqbal. "A brief review: security issues in cloud computing and their solutions." *Telkonnika* 17, no. 6 (2019).
- S32 Kanickam, S. Hendry Leo, L. Jayasimman, and A. Nisha Jebaseeli. "A survey on layer wise issues and challenges in cloud security". In 2017 World Congress on Computing and Communication Technologies (WCCCT), pp. 168–171. IEEE, 2017.
- S33 Nowrin, Itisha Nowrin, and Fahima Khanam Khanam. "Importance of Cloud Deployment Model and Security Issues of Software as a Service (SaaS) for Cloud Computing". In 2019 International Conference on Applied Machine Learning (ICAML), pp. 183–186. IEEE, 2019.
- S34 Ahmed, Hussam Alddin S., Mohammed Hasan Ali, Laith M. Kadhum, Mohamad Fadli Zolkipli, and Yazan A. Alsariera. "A review of challenges and security risks of cloud computing". *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)* 9, no. 1–2 (2017): 87–91.
- S35 Aljawarneh, Shadi A., and Muneer O. Bani Yassein. "A conceptual security framework for cloud computing issues". *International Journal of Intelligent Information Technologies (IJIIT)* 12, no. 2 (2016): 12–24.
- S36 Díaz de León Guillén, Miguel Ángel, Víctor Morales-Rocha, and Luis Felipe Fernández Martínez. "A systematic review of security threats and countermeasures in SaaS". *Journal of Computer Security Preprint*: 1–19.
- S37 Srinivasu, N., O. Sree Priyanka, M. Prudhvi, and G. Meghana. "Multilevel classification of security threats in cloud computing". *International Journal of Engineering and Technology (UAE)* 7, no. 1.5 (2018): 253–257.
- S38 Sinjilawi, Yousef K., Mohammad Q. Al-Nabhan, and Emad A. Abu-Shanab. "Addressing Security and Privacy Issues in Cloud Computing". *Journal of Emerging Technologies in Web Intelligence* 6, no. 2 (2014).
- S39 Kaur, S., and S. Khurmi. "A review on security issues in cloud computing". *IJCST Int. J. Comput. Sci. Technol* 7, no. 1 (2016).

- S40 Elsayed, Marwa, and Mohammad Zulkernine. "Offering security diagnosis as a service for cloud SaaS applications". *Journal of information security and applications* 44 (2019): 32–48.
- S41 Khan, N. and Al-Yasiri, A., 2016. Identifying cloud security threats to strengthen cloud computing adoption framework. *Procedia Computer Science*, 94, pp.485–490.
- S42 Krishna, B. Hari, S. Kiran, G. Murali, and R. Pradeep Kumar Reddy. "Security issues in service model of cloud computing environment". *Procedia Computer Science* 87 (2016): 246–251.
- S43 Loganayagi, B., and S. Sujatha., "Enhanced cloud security by combining virtualization and policy monitoring techniques". *Procedia Engineering* 30 (2012): 654–661.
- S44 Tang, Changlong, and Jiqiang Liu. "Selecting a trusted cloud service provider for your SaaS program". *Computers & Security* 50 (2015): 60–73.
- S45 Ficco, Massimo, Francesco Palmieri, and Aniello Castiglione. "Modeling security requirements for cloud-based system development". *Concurrency and Computation: Practice and Experience* 27, no. 8 (2015): 2107–2124.
- S46 Iqbal, Salman, Miss Laiha Mat Kiah, Nor Badrul Anuar, Babak Daghighi, Ainuddin Wahid Abdul Wahab, and Suleman Khan. "Service delivery models of cloud computing: security issues and open challenges". *Security and Communication Networks* 9, no. 17 (2016): 4726–4750.
- S47 Liu, Chia-Hui, Fong-Qi Lin, Chin-Sheng Chen, and Tzer-Shyong Chen. "Design of secure access control scheme for personal health record-based cloud healthcare service". *Security and Communication Networks* 8, no. 7 (2015): 1332–1346.
- S48 Mezni, Haithem, Mokhtar Sellami, and Jaber Kouki. "Security-aware SaaS placement using swarm intelligence". *Journal of Software: Evolution and Process* 30, no. 8 (2018): e1932.
- S49 Simou, Stavros, Christos Kalloniatis, Stefanos Gritzalis, and Haralambos Mouratidis. "A survey on cloud forensics challenges and solutions". *Security and Communication Networks* 9, no. 18 (2016): 6285–6314.
- S50 Babu, LD Dhinesh, P. Venkata Krishna, A. Mohammed Zayan, and Vijayant Panda. "An analysis of security related issues in cloud computing". In *International Conference on Contemporary Computing*, pp. 180–190. Springer, Berlin, Heidelberg, 2011.
- S51 Doelitzscher, Frank, Christoph Reich, Martin Knahl, Alexander Passfall, and Nathan Clarke. "An agent based business aware incident detection system for cloud environments". *Journal of Cloud Computing: Advances, Systems and Applications* 1, no. 1 (2012): 1–19.
- S52 Gonzalez, Nelson, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Näslund, and Makan Pourzandi. "A quantitative analysis of current security concerns and solutions for cloud computing". *Journal of Cloud Computing: Advances, Systems and Applications* 1, no. 1 (2012): 1–18.
- S53 Venkatakotireddy, G., B. Thirumala Rao, and Naresh Vurukonda. "A Review on Security Issue in Security Model of Cloud Computing Environment". In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, pp. 207–212. Springer, Singapore, 2018.
- S54 Hashizume, Keiko, David G. Rosado, Eduardo Fernández-Medina, and Eduardo B. Fernandez. "An analysis of security issues for cloud computing". *Journal of internet services and applications* 4, no. 1 (2013): 1–13.
- S55 Georgiou, Dimitra, and Costas Lambrinouidakis. "Cloud computing security requirements and a methodology for their auditing". In *International Conference on e-Democracy*, pp. 51–61. Springer, Cham, 2015.
- S56 Vesyropoulos, Nikos, Christos K. Georgiadis, and Elias Pimenidis. "Ensuring cloud security: Current concerns and research challenges". In *International Conference on e-Democracy*, pp. 3–10. Springer, Cham, 2013.
- S57 Singh, Ajit. "Security concerns and countermeasures in cloud computing: a qualitative analysis". *International Journal of Information Technology* 11, no. 4 (2019): 683–690.

- S58 Kaur, Puneet Jai, and Sakshi Kaushal. "Security concerns in cloud computing". In international conference on high performance architecture and grid computing, pp. 103–112. Springer, Berlin, Heidelberg, 2011.

### Appendix B. Grey Literature

- GL1 "Cloud Security: Evaluating Risks within IAAS/PAAS/SAAS" by TechTarget, Access Date: 3 March 2021, [https://cdn.ttgtmedia.com/searchSecurity/downloads/Char\\_Sample\\_Cloud%20Security-Evaluating\\_Risks\\_within\\_IAAS\\_PAAS\\_SAAS.pdf](https://cdn.ttgtmedia.com/searchSecurity/downloads/Char_Sample_Cloud%20Security-Evaluating_Risks_within_IAAS_PAAS_SAAS.pdf)
- GL2 "Security concerns overcome: Customer moving to SaaS" A cloud security study by InfoTech Research Group, May 2016, Access Date: 3 March 2021, [https://www.insight.com/en\\_US/content-and-resources/brands/adobe/security-concerns-overcome-moving-to-saas.html](https://www.insight.com/en_US/content-and-resources/brands/adobe/security-concerns-overcome-moving-to-saas.html)
- GL3 "Cloud adoption and Risk report" by McAfee, May 2020, Access Date: 3 March 2021, <https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-adoption-risk.html>
- GL4 "Leveling up SaaS security with cloud detection and response", white paper by OBSIDIANSECURITY.com, Access Date: 3 March 2021, <https://go.obsidiansecurity.com/leveling-up-saas-security-with-cdr-wp>
- GL5 "Cloud computing security issues" by McAfee, Accessed from <https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/security-issues-in-cloud-computing.html>, Access Date: 3 March 2021
- GL6 "7 Key Security Risks to Address when Adopting SaaS Applications", <https://blog.sonicwall.com/en-us/2019/09/7-key-security-risks-to-address-when-adopting-saas-applications/>, Access Date: 3 March 2021
- GL7 "5 problems with SaaS security tops customer concerns on software-as-a-service", <https://www.networkworld.com/article/2219462/5-problems-with-saas-security.html>, Access Date: 3 March 2021
- GL8 "10 SaaS security Risks and concern every user has", <https://financesonline.com/10-saas-security-risks-concerns-every-user/>, Access Date: 3 March 2021
- GL9 "5 SaaS Security Concerns and How to Address Them", 5 SaaS Security Concerns and How to Address Them ([g2.com](https://g2.com)), Access Date: 3 March 2021
- GL10 "Top 5 Cloud Security Issues Experienced with SaaS and Its Solutions", <https://socialnomics.net/2020/09/09/top-5-cloud-security-issues-experienced-with-saas-and-its-solutions/>, Access Date: 3 March 2021
- GL11 "Why SaaS Is the Epicenter for Security Threats", <https://securityboulevard.com/2020/07/why-saas-is-the-epicenter-for-security-threats/>, Access Date: 3 March 2021
- GL12 "SAAS SECURITY CHECKLIST: BEST PRACTICES TO PROTECT YOUR SAAS APPLICATION", <https://medium.com/@Imagination/saas-security-checklist-best-practices-to-protect-your-saas-application-22bbeb06357d>, Access Date: 3 March 2021
- GL13 "Best Practices for SaaS Security", <https://www.moodyanalytics.com/articles/2018/best-practices-for-saas-security>, Access Date: 3 March 2021
- GL14 "How to ensure your SaaS solutions are secure", <https://www.securitymagazine.com/articles/93680-how-to-ensure-your-saas-solutions-are-secure>, Access Date: 3 March 2021
- GL15 "Three Major Security Issues to Consider with SaaS and Cloud Solutions", <https://www.passwordprotectedlaw.com/2017/03/three-major-security-issues-to-consider-with-saas-and-cloud-solutions/>, Access Date: 3 March 2021
- GL16 "SaaS Security risks come to the fore at Cisco Live 2018", <https://www.cisco.com/c/en/us/solutions/cloud/saas-security-risks.html>, Access Date: 3 March 2021
- GL17 "SaaS Security Guide: How to Protect Your Product and User Data", <https://www.codica.com/blog/saas-application-security/>, Access Date: 3 March 2021
- GL18 "How to Minimize the Cloud Security Risks for SaaS Application", <http://blog.andolsoft.com/2019/05/how-to-minimize-the-cloud-security-risks-for-saas-application.html>, Access Date: 3 March 2021

- GL19 “4 SaaS and Slack Security Risks to Consider in 2020”, <https://nightfall.ai/resources/saas-slack-security-risks-2020/>, Access Date: 3 March 2021
- GL20 “Security for SaaS applications starts with collaboration”, <https://searchcloudsecurity.techtarget.com/feature/Security-for-SaaS-applications-starts-with-collaboration>, Access Date: 3 March 2021
- GL21 “KEY CYBERSECURITY THREATS IN THE SAAS INDUSTRY”, <https://www.identityglobal.com/news/key-cybersecurity-threats-in-the-saas-industry/40222/>, Access Date: 3 March 2021
- GL22 “Securing software as a service”, <https://www.mckinsey.com/business-functions/ri-sk/our-insights/securing-software-as-a-service#>, Access Date: 3 March 2021
- GL23 “How to Ensure Security in Your SaaS Application”, <https://towardsdatascience.com/how-to-ensure-security-in-your-saas-application-8873698837de>, Access Date: 3 March 2021
- GL24 “SaaS Security: Basic Principles and Best Practices”, <https://saasmetrics.co/security/>, <https://saasmetrics.co/security/>, Access Date: 3 March 2021
- GL25 “SaaS Security Best Practices to Keep in Mind”, <https://cybersecurity.att.com/blogs/security-essentials/basic-best-practices-for-secure-internal-software-as-a-service-saas-applications>, Access Date: 3 March 2021
- GL26 “Building Secure SaaS Application using SaaS-Tenant Framework: A Cloud Security Perspective for Application Providers”, <https://www.saas-tenant.com/white-paper/Securing-SaaS-Applications.htm>, Access Date: 3 March 2021
- GL27 “SAAS INFORMATION SECURITY CHECKLIST: PROTECT YOUR PRODUCT AND USER DATA”, <https://freshcodeit.com/freshcode-post/saas-information-security-checklist>, Access Date: 3 March 2021
- GL28 “SaaS Security”, <https://www.ssh.com/cloud/saas/security>, Access Date: 3 March 2021
- GL29 “SaaS Security Best Practices: Is Your SaaS Solution Protecting Data?”, <https://www.profitwell.com/recur/all/saas-security/>, Access Date: 3 March 2021
- GL30 “Software as a Service (SaaS) security guidance”, <https://www.ncsc.gov.uk/collecton/saas-security/saas-security-principles>, Access Date: 3 March 2021
- GL31 “How to Overcome Cloud Security Challenges [+ Solutions]”, <https://www.compuqip.com/blog/cloud-computing-security-challenges>, Access Date: 3 March 2021
- GL32 “SaaS Security Best Practices: Tackling the Trust Discrepancy”, SaaS Security Best Practices: Tackling the Trust Discrepancy (teamsupport.com), Access Date: 3 March 2021
- GL33 “How to Mitigate the Top 5 Risks of SaaS at Scale”, <https://productiv.com/how-to-mitigate-the-top-5-risks-of-saas-at-scale/>, Access Date: 3 March 2021
- GL34 “SaaS Security Checklist: Best Practices for Protecting SaaS Apps”, <https://dev.to/codicacom/saas-security-checklist-best-practices-for-protecting-saas-apps-5279>, Access Date: 3 March 2021
- GL35 “The SaaS security checklist—Keep data safe with end-to-end encryption”, <https://tresorit.com/blog/the-saas-security-checklist-keep-data-safe-with-end-to-end-encryption/>, Access Date: 3 March 20.

## References

1. Kundu, A.; Banerjee, A.; Saha, P. Introducing new services in cloud computing environment. *Int. J. Digit. Content Technol. Appl. AICIT* **2010**, *4*, 143–152.
2. Alshehri, M. An effective mechanism for selection of a cloud service provider using cosine maximization method. *Arab. J. Sci. Eng.* **2019**, *44*, 9291–9300. [CrossRef]
3. Che, J.; Duan, Y.; Zhang, T.; Fan, J. Study on the security models and strategies of cloud computing. *Procedia Eng.* **2011**, *23*, 586–593. [CrossRef]
4. Nasr, A.A.; El-Bahnasawy, N.A.; Attiya, G.; El-Sayed, A. Cost-effective algorithm for workflow scheduling in cloud computing under deadline constraint. *Arab. J. Sci. Eng.* **2019**, *44*, 3765–3780. [CrossRef]
5. Arunkumar, G.; Venkataraman, N. A novel approach to address interoperability concern in cloud computing. *Procedia Comput. Sci.* **2015**, *50*, 554–559. [CrossRef]
6. Goumidi, H.; Aliouat, Z.; Harous, S. Vehicular cloud computing security: A survey. *Arab. J. Sci. Eng.* **2020**, *45*, 2473–2499. [CrossRef]

7. Chen, Y.-S.; Wu, C.; Chu, H.-H.; Lin, C.-K.; Chuang, H.-M. Analysis of performance measures in cloud-based ubiquitous SaaS CRM project systems. *J. Supercomput.* **2018**, *74*, 1132–1156. [CrossRef]
8. Humayun, M. Role of emerging IoT big data and cloud computing for real time application. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 494–506. [CrossRef]
9. Statista. Global Public Cloud Application Services (SaaS) Market Size 2015–2022. Available online: [https://www.statista.com/statistics/505243/worldwide-software-as-a-service-revenue/#:~:text=Global%20public%20cloud%20application%20services%20\(SaaS\)%20market%20size%202015%2D2022&text=In%202021%2C%20the%20software%20as,approximately%20145.5%20billion%20U.S.%20dollars](https://www.statista.com/statistics/505243/worldwide-software-as-a-service-revenue/#:~:text=Global%20public%20cloud%20application%20services%20(SaaS)%20market%20size%202015%2D2022&text=In%202021%2C%20the%20software%20as,approximately%20145.5%20billion%20U.S.%20dollars) (accessed on 6 April 2021).
10. Kumar, P.R.; Raj, P.H.; Jelciana, P. Exploring data security issues and solutions in cloud computing. *Procedia Comput. Sci.* **2018**, *125*, 691–697. [CrossRef]
11. C. Report. Cloud Traffic Projected to Represent 95% of Global Data Center Traffic by 2021: Study. CIO.com. The Economics Time. 2018. Available online: <https://cio.economictimes.indiatimes.com/news/cloud-computing/cloud-traffic-projected-to-represent-95-of-global-data-center-traffic-by-2021-study/62815965> (accessed on 6 April 2021).
12. Asadi, Z.; Abdekhoda, M.; Nadrian, H. Cloud computing services adoption among higher education faculties: Development of a standardized questionnaire. *Educ. Inf. Technol.* **2020**, *25*, 175–191. [CrossRef]
13. Luo, X.; Zhang, W.; Li, H.; Bose, R.; Chung, Q.B. Cloud computing capability: Its technological root and business impact. *J. Organ. Comput. Electron. Commer.* **2018**, *28*, 193–213. [CrossRef]
14. Freet, D.; Agrawal, R.; John, S.; Walker, J.J. Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS. In Proceedings of the 7th International Conference on Management of Computational and Collective intelligence in Digital EcoSystems, Caraguatutuba, Brazil, 25–29 October 2015; pp. 148–155.
15. Microsoft Azure. What are Public, Private, and Hybrid Clouds? An Intro to Cloud Service Deployment Options. Available online: <https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/> (accessed on 6 April 2021).
16. Felter, B. The Different Types of Cloud Computing and How They Differ. 2021. Available online: <https://prooncall.com/the-different-types-of-cloud-computing-and-how-they-differ/> (accessed on 6 April 2021).
17. Palos-Sanchez, P.R.; Arenas-Marquez, F.J.; Aguayo-Camacho, M. Cloud computing (SaaS) adoption as a strategic technology: Results of an empirical study. *Mob. Inf. Syst.* **2017**, *2017*, 2536040. [CrossRef]
18. Top 5 Advantages of Software as a Service (SaaS). IBM Cloud Team. 2020. Available online: <https://www.ibm.com/cloud/blog/top-5-advantages-of-software-as-a-service> (accessed on 6 April 2021).
19. Watts, M.R.S. SaaS vs. PaaS vs. IaaS: What's The Difference & How To Choose. BMC. 2019. Available online: <https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/> (accessed on 6 April 2021).
20. Soofi, A.A.; Khan, M.I.; Talib, R.; Sarwar, U. Security issues in SaaS delivery model of cloud computing. *Int. J. Comput. Sci. Mob. Comput.* **2014**, *3*, 15–21.
21. Popović, K.; Hocenski, Ž. Cloud computing security issues and challenges. In Proceedings of the 33rd International Convention MIPRO, Opatija, Croatia, 24–28 May 2010; pp. 344–349.
22. Patel, N.S.; Rekha, B. Software as a Service (SaaS): Security issues and solutions. *Int. J. Comput. Eng. Res.* **2014**, *4*, 68–71.
23. Lau, W. A Comprehensive Introduction to Cloud Computing. RedGate Hub. 2011. Available online: <https://www.red-gate.com/simple-talk/cloud/platform-as-a-service/a-comprehensive-introduction-to-cloud-computing/> (accessed on 6 April 2021).
24. Hoener, P. Cloud Computing Security Requirements and Solutions: A Systematic Literature Review. Bachelor's Thesis, University of Twente, Enschede, The Netherlands, 2013.
25. Hashizume, K.; Rosado, D.G.; Fernández-Medina, E.; Fernandez, E.B. An analysis of security issues for cloud computing. *J. Internet Serv. Appl.* **2013**, *4*, 5. [CrossRef]
26. Juárez, D.X.J.; Cedillo, P. Security of mobile cloud computing: A systematic mapping study. In Proceedings of the 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM), Salinas, Ecuador, 16–20 October 2017; pp. 1–6.
27. da Silva, C.M.R.; da Silva, J.L.C.; Rodrigues, R.B.; do Nascimento, L.M.; Garcia, V.C. Systematic mapping study on security threats in cloud computing. *arXiv* **2013**, arXiv:1303.6782.
28. Zhou, M.; Zhang, R.; Xie, W.; Qian, W.; Zhou, A. Security and privacy in cloud computing: A survey. In Proceedings of the 2010 Sixth International Conference on Semantics, Knowledge and Grids, Beijing, China, 1–3 November 2010; pp. 105–112.
29. Shankarwar, M.U.; Pawar, A.V. Security and privacy in cloud computing: A survey. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, Bhubaneswar, India, 14–15 November 2014; Springer: Cham, Switzerland, 2015; pp. 1–11.
30. Hussein, N.H.; Khalid, A. A survey of cloud computing security challenges and solutions. *Int. J. Comput. Sci. Inf. Secur.* **2016**, *14*, 52.
31. Kumbhar, N.N.; Chaudhari, V.V.; Badhe, M.A. The comprehensive approach for data security in cloud computing: A survey. *Int. J. Comput. Appl.* **2012**, *39*, 23–29.
32. Tom, E.; Aurum, A.; Vidgen, R. An exploration of technical debt. *J. Syst. Softw.* **2013**, *86*, 1498–1516. [CrossRef]
33. Garousi, V.; Felderer, M.; Mäntylä, M.V. The need for multivocal literature reviews in software engineering: Complementing systematic literature reviews with grey literature. In Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering, Limerick, Ireland, 1–3 June 2016; pp. 1–6.



34. Kitchenham, B.; Brereton, O.P.; Budgen, D.; Turner, M.; Bailey, J.; Linkman, S. Systematic literature reviews in software engineering—a systematic literature review. *Inf. Softw. Technol.* **2009**, *51*, 7–15. [[CrossRef](#)]
35. Garousi, V.; Mäntylä, M.V. When and what to automate in software testing? A multivocal literature review. *Inf. Softw. Technol.* **2016**, *76*, 92–117. [[CrossRef](#)]
36. Garousi, V.; Felderer, M.; Hacaloğlu, T. Software test maturity assessment and test process improvement: A multivocal literature review. *Inf. Softw. Technol.* **2017**, *85*, 16–42. [[CrossRef](#)]
37. Bhatta, N. Emerging ethical challenges of leadership in the digital era: A Multivocal literature review. *Electron. J. Bus. Ethics Organ. Stud.* **2021**, *26*, 30–46.