Journal of Cloud Computing:
Advances, Systems and Applications

REVIEW

Open Access

Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review

Juncal Alonso[1*], Leire Orue-Echevarria[1], Valentina Casola[2], Ana Isabel Torre[1], Maider Huarte[3], Eneko Osaba[1] and Jesus L. Lobo[1]

Abstract

The evolution of Cloud Computing into a service utility, along with the pervasive adoption of the IoT paradigm, has promoted a significant growth in the need of computational and storage services. The traditional use of cloud services, focused on the consumption of one provider, is not valid anymore due to different shortcomings being the risk of vendor lock-in a critical. We are assisting to a change of paradigm, from the usage of a single cloud provider to the combination of multiple cloud service types, affecting the way in which applications are designed, developed, deployed and operated over such heterogeneous ecosystems. The result is an effective heterogeneity of architectures, methods, tools, and frameworks, copying with the multi-cloud application concept. The goal of this study is manifold. Firstly, it aims to characterize the multi-cloud concept from the application development perspective by reviewing existing definitions of multi-cloud native applications in the literature. Secondly, we set up the basis for the architectural characterization of these kind of applications. Finally, we highlight several open research issues drawn up from the analysis carried out. To achieve that, we have conducted a systematic literature review (SLR), where, a large set of primary studies published between 2011 and 2021 have been studied and classified. The in-depth analysis has revealed five main research trends for the improvement of the development and operation DevOps lifecycle of "multi-cloud native applications". The paper finishes with directions for future work and research challenges to be addressed by the software community.

Keywords Multi-cloud native application, Hybrid cloud, Software architecture, Software design, Systematic literature review

Introduction

The Cloud Computing evolution in the last decade and its transformation into a service utility has promoted a wide adoption by the industry of applications to store and process data. With the expansion of the IoT paradigm [1], the need of computational and storage services is expected to grow in coming years, complemented by the amount of data generated at the edge of the network. The centralized nature of the traditional cloud services, that has been mainly used for replication or business continuity, is not valid anymore [2]. Until recently, Cloud Services were offered as third-party computational

*Correspondence:
Juncal Alonso
juncal.alonso@tecnalia.com
[1] TECNALIA, Basque Research and Technology Alliance (BRTA), Parque Científico y Tecnológico de Bizkaia, Astondo bidea, 700, E-48160 Derio, Spain
[2] Department of Electrical Engineering and Information Technology (DIETI), University of Napoli Federico II, Naples, Italy
[3] UPV, Department of Communications Engineering of the University of the Basque Country UPV/EHU, Faculty of Engineering, Alda. Urquijo S/N, 48013 Bilbao, Spain

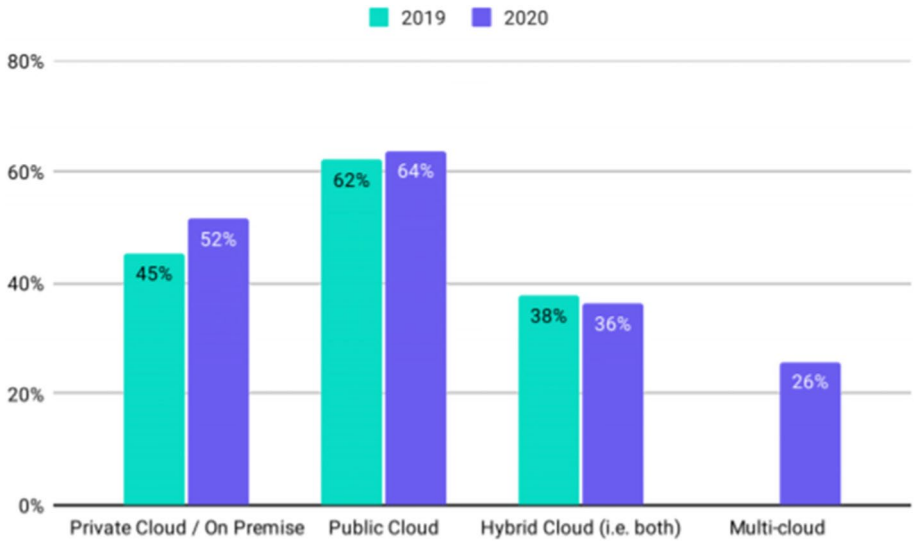

Fig. 1 CNCF survey 2020.Source: CNCF [4]

capacities, but now the offer has become more functionally diverse, context-specific and technology driven. Following this transition, users' consumption of such cloud services has evolved too, from one single Cloud Service type, and offered by one single provider, to the usage of multiple Cloud Services by one or various Cloud Providers. The sequential or simultaneous use of services from diverse providers to execute an application is called a multi-cloud approach. At business level, Hybrid Cloud is the term commonly used to identify such architectural model. Gartner defines it as "*the coordinated use of cloud services across isolation and provider boundaries among public, private and community service providers, or between internal and external cloud services*" [3]. However, as highlighted in a recent study conducted in 2020 by the CNCF [4], the term *multi-cloud* is gaining greater interest. In a nutshell, multi-cloud means using workloads across different clouds based on the type of cloud that fits the workload best. The previously mentioned CNCF survey was answered by the 140 top companies and startups committed to accelerating cloud native technologies and improving the deployment experience. As illustrated in Fig. 1, this study reports that in 2020 the use of hybrid cloud decreased slightly to 36% from 38% in 2019 while multi-cloud usage, which was a new alternative in 2020, emerged with a 26% of incidence. The primary reason behind this interest is that microservices-based software applications are getting increasingly popular, fostering flexibility for the developers to build applications for distributed complex environments such as the one resulting from the use of multiple cloud services.

Multi cloud native applications

In a nutshell, multi-cloud means using workloads across different clouds based on the type of cloud that fits the workload best.

The value proposition offered by multi cloud native applications to the industry is well known, enabling the implementation of complex IoT solutions with better performance and empowering organizations to distribute their workloads across multiple cloud environments with optimized ROI. Every resource is optimized for each application component, functional and non-functional needs such a low latency, real time, high processing requirements, superior security, or autonomy (less vendor lock-in), among others. Thus, companies conclude that multi-cloud accelerates innovation, enhances data agility, and reduces costs. Some examples where the application of multi-cloud native applications is gaining popularity are entertainment and Media (i.e. Netflix), energy sector, autonomous driving or e-health [5].

Another sign of the importance of the multi-cloud paradigm for the software industry is the appearance of new standards, and industrial frameworks, which aim to set up the multi-cloud concept and practices. As an example, the ISO/IEC JTC 1/SC "Cloud Computing and Distributed Platforms",[1] which is still under development as of 2022, provides an overview and sets out the foundational concepts for cloud computing involving multiple CSPs. Again, this draft identifies several benefits for the industry when adopting multi cloud-based solutions. These include more flexibility, higher availability

[1] https://www.iso.org/committee/601355.html

rates, resource-based optimization, better fault tolerance, decreased latency, less costs, or enhanced privacy.

The cloud-native concept

On the other hand, while multi-cloud is gaining momentum from the industrial perspective, the scientific community is still focused mostly on the "cloud-native concept" and has yet not fully addressed the challenges and issues introduced by the paradigm changes that multi-cloud poses.

This context generates confusion and ambiguity in their definitions, especially from the developers' point of view. The complexity of the infrastructural layer to be managed by the developers and operators of multi-cloud software applications is increasing in complexity. Motivated by the advent of the Cloud Continuum and the advances on virtualization technologies, which enables each single node providing computing capabilities. Developers and operators of these applications need to have a clear understanding on the concepts, terminology, architectures, and research challenges to face in the near future. In fact, this situation has motivated us to perform this survey.

In [6], authors provided a formal definition and understanding of the term "cloud-native application" and the related research trends but the same is required for the concept of "multi-cloud native" applications, which urgently needs to be characterized and understood for the following reasons: 1) a change of philosophy in how the service lifecycle of applications are today understood and managed (i.e. DevOps philosophy [7]), 2) the increasing available services offerings and interoperability capabilities, 3) the upcoming of new practices with respect to software architecture approaches such as microservices, containerization and serverless, and 4) unexplored security issues and challenges.

The main stakeholders in developing and operating multi-cloud native applications are the developers and operators. Multi-cloud application developers are relevant in the design and development, while multi-cloud application operators are important for the deployment and provisioning (operating) the service. To support both in an integrated process from the design to the operation, a DevOps approach is needed to be adopted. DevOps represents an effort to accomplish the same mutually trusting relationship for Software-as-Service, as agile did it for software as a product. Agile has taught development how to move at the same speed and with the same flexibility as business. DevOps tries to teach operations to move at the same speed and with the same flexibility as development. However, existing DevOps solutions are focused on traditional cloud applications, and the specificities of managing multi-cloud native applications have not been yet thoroughly addressed from the point of view of DevOps. While multi cloud native applications are designed, developed, deployed, and operated following the DevOps philosophy, the challenges that developers and operators face are more complex compared to a traditional – cloud or not- application DevOps process. Some examples include, 1) the need for the identification of multi cloud based architectural patterns in the design phase, 2) the incorporation of the functional and non-functional requirements of the application from the design to the deployment phase to choose the most suitable cloud service for each application component, or 3) the self-adaptive mechanisms at operation phase, among others.

The need for a multi-cloud native standard definition

Indeed, as previously indicated, terms such as multi-cloud, hybrid cloud, or multiple cloud are commonly used as synonyms, and they are usually referred to the environment or the infrastructure where the application is deployed. Therefore, the notion of multi-cloud concepts has been referred for a while in research and more nowadays with the advent of distributed architectures such as IoT, and Edge Computing. Of course, this change of paradigm, from the usage of a single cloud service provider to the combination of multiple cloud services types simultaneously, including edge services and other infrastructural resources (e.g., IoT), affects the way in which applications deployed over such a heterogeneous ecosystem are designed, developed and operated [8]. Some contributions have been proposed in the literature which provide insights about the characteristics that an application must fulfill to be identified as "cloud native" [6]. However, the understanding of "multi-cloud native" applications is still in its infancy. How an heterogenous multi-cloud environment impacts on the development and operation of those applications that are especially designed for the multi-cloud still present several "white-areas", mainly due to the lack of interoperability /portability among providers such as multi-cloud by design [9], multi-cloud applications at run-time [10] or multi-cloud security aspects [11], among others.

To the best of our knowledge, there is no work that characterizes the multi-cloud native concept from perspective of application development. With this aim, the main goals of this study are:

- to review existing definitions of what multi-cloud native application is,
- to highlight open issues in the design, development and operation of a multi-cloud application,
- to set up the basis for the architectural characterization of these applications by also extending this analysis to understand better the challenges faced by

DevOps teams during the management of the lifecycle of the application, as reported by both the industry and the academia.

Taking into consideration the aspects mentioned above and in order to have a clear picture of the current understanding of multi-cloud native applications, this work proposes a comprehensive SLR [12]. Our objective is to address the state-of-the-art of multi cloud native applications with a special focus on the application lifecycle perspective. We will bring our attention to the challenges that the developers and operators of such applications face during the entire lifecycle of the application, from its design and conceptualization to the run time and operation phases, considering also the implementation and the deployment phases.

The remainder of the paper is structured as follows. Section 2 briefly analyses some works related to similar SLRs. Section 3 describes the research methodology followed in this study and provides a general classification of the papers resulting from the literature search. Section 4 provides the analysis of the meta-data related to the selected studies serving as background information about the application development. Section 5 analyses and discusses more specific SLR results related to the research questions. Section 6 outlines open issues, research gaps and opportunities as they emerged from the review. Finally, Section 7 summarizes paper conclusions and future directions.

Related work

This section justifies the need for our study on multi-cloud native applications. Several works have analysed the literature on areas related to cloud, hybrid cloud or multi-cloud. However, up to our knowledge, none of previous survey papers have been specifically focused on structuring and analysing the characterization of multi-cloud native applications.

Cloud related topics and cloud computing-based practices have been addressed on diverse reviews or mappings. In 2017 Kratzke and Quint published a systematic mapping study on cloud native applications [6]. In this mapping, 49 primary studies were analysed and classified in order to come up with a definition for cloud-native applications, i.e., applications that were intentionally designed for the cloud. They provide a definition of the term CNA, based on the analysis that they performed, and they highlighted software engineering trends in the topic of CNA. This mapping study has served us as inspiration for the proposed literature review. We have pursued to achieve similar results, but in terms of multi-cloud native applications. Our hypothesis is that there exist specific needs in terms of architectural patterns, methods, and techniques for applications which components are going to be deployed using a distributed multi-cloud approach.

Since the beginning of the establishment of the cloud computing industry, general aspects of cloud computing have been dealt with in several studies.. El-Gazzar analysed in [13] 81 studies to determine the key issues related to the adoption cloud computing and highlighted open research topics that would be further investigated in the upcoming years such as migration processes and techniques towards cloud computing, security and trust in the cloud and cloud monitoring. They do not make any explicit mention to multi-cloud or hybrid cloud, neither from the infrastructure perspective nor from the application (architecture) point of view. Some of the aspects presented by El-Gazzar in his cloud computing adoption study still remain unclear and are object to new analysis and proposals. This is the case of Cloud monitoring. In [14], Ward and Barker performed a survey of 30 cloud resources monitoring tools and classified them into a cloud monitoring taxonomy where each tool is classified through an architecture, communication mechanism, collection mechanism, origin and use-case. Similarly, other authors have investigated on cloud trust, trustworthiness assessment and cloud security. Chiregi and Jafari [15] conducted a systematic literature review on trust evaluation state-of-the-art mechanisms. To this end they compared 28 studies in terms of integrity, security, reliability, dependability, safety, dynamicity, confidentiality, and scalability.

By discussing and examining the selected state-of-the-art mechanisms, they have detected that there is not any independent method that addresses all matters involved in trust. While they envision relevant open issues, such as evaluation of the privacy and security issues in the trust evaluation mechanisms, or the estimation of consistency in dynamic trust monitor to identify a trustworthy CSP, they do not address the specifics challenges or new requirements that multi-cloud or hybrid cloud approaches can bring into the cloud computing trust assessment. Recently, in 2019, the authors of [16] published a review about resource scheduling and security in cloud computing. In this case, they analysed how security aspects can impact the selection of Cloud resources for scheduling required workloads. Again, no specific mention to multi-cloud approaches can be found.

As the body of knowledge in cloud computing has matured, the shift towards multi-cloud approaches has gained interest in the research community and in the industry. In 2013, the authors of [17], already identified the need of multiple clouds being these, (1) to deal with peaks and resources needs, (2) to avoid vendor lock-in, (3) to react to changes in CSPs offers, (4) to consume

cloud services based on their particularities or (5) to optimize costs and improve Quality of Service (QoS). In this article, several solutions for managing the deployment of applications in multiple clouds are presented, including library-based approaches, service-based approaches and deployable solutions based on results from research projects. From the analysis of such solutions and as a conclusion, a basic list of requirements for a multi-cloud deployment is offered. Most of the requirements highlighted are related to the infrastructural aspects of multi-cloud. Nevertheless, the author already envisioned some challenges related to the application characterization when addressing multi-cloud: the support of the application portability between the connected clouds and the support for application component execution simultaneously in multiple clouds. Furthermore, it is stated that the development of a multi-cloud requires to offer solutions to multiple levels, one of it being the application and services level.

Recently, the infrastructural aspect of multi cloud has attracted most of the attention in the research community. Management and federation of cloud resources has been one of the hottest research topics in multi-cloud. Liaqat et al. [18] conducted a review on federated resource management functions in multiple clouds, classified into resource pricing, resource discovery, resource selection, resource monitoring, resource allocation, and disaster management. They provided insights from the state-of-the-art research and prominent research directions for each function. Several of these resource management functions have been recently analysed too by other authors, such as Tomarchio et al. In [19], Lahmar and Mezni in [20], and Vakili and Navimipour in [21]. These works study existing cloud resources orchestration frameworks and Cloud service composition approaches. Again, none of these addresses the particularities, impact or needs of the analysed methods from the application architecture perspective.

On the other side of the coin, distributed architectural aspects of software applications have been addressed in diverse SLRs, starting from Service Oriented Architectures [22] and more recently on microservices [23, 24], these analysis different methods and approaches for the decomposition of the application into isolated software units are described, classified, and analysed. In most of the cases, the specific topic of multi-cloud deployments of these kinds of applications is not tackled.

As a summary of available systematic studies on cloud and multi-cloud native applications related issues, in Table 1 we have reported the main contributions of different studies analysed.

In summary cloud computing in general and multi-cloud in particular has attracted a lot of interest from the software industry and the research community in a short period of time, and the notion of multi-cloud and hybrid cloud among practitioners is growing. In addition, distributed schemes for software application design and development have been also tackled in several SLRs, including service-oriented architectures, microservices and serverless solutions. However, these studies address both aspects separately.

Table 1 Related work main contributions

Authors and Reference	Main contribution of the study
Chiregi and Jafari [25]	A systematic literature review on the state-of-the-art of trust evaluation mechanisms. They compared 28 studies in terms of integrity, security, reliability, dependability, safety, dynamicity, confidentiality, and scalability. (They address the dependence of such controls to the architecture and the missing of multi-cloud approaches to security)
El-Gazzar [26]	A study on the key issues related to the adoption of cloud computing including migration processes and techniques towards cloud computing, security and trust in the cloud and cloud monitoring (did not analyze multi-cloud specific issues while coping with independent heterogeneous architectures)
Kratzke and Quint [27]	A systematic mapping study on cloud native applications a systematic mapping study on cloud native applications (did not analyze multi-cloud specific issues)
Liaqat et al. [20]	A review on federated resource management functions in multiple clouds, classified into resource pricing, resource discovery, resource selection, resource monitoring, resource allocation, and disaster management.
Petcu [28]	Multi-cloud main requirements were identified and discussed, from an architectural perspective (not service and application level). They just highlighted the need of native-multi-cloud application to face different issues.
Tomarchio et al. [29], Lahmar and Mezni [30], Vakili and Navimipour [31]	Studies on federated resource management functions. Multi-cloud is not explicitly tackled.
Ward and Barker [32]	A survey on monitoring tools for cloud resources (did not analyze multi-cloud specific issues while coping with independent heterogeneous architectures).
Hamzehloui et al. [33], Niknejad et al. [34], Soldani et al. [35]	Studies on different methods and approaches for the decomposition of the application into isolated software units are described, classified, and analysed. The multi-cloud deployments of these kinds of applications are not tackled.

Up to our knowledge there is no work where the current status of the multi cloud approach is analysed from the application point of view. With the present SLR we try to approach both faces of the same coin, the design of distributed applications more specifically, multi-cloud, the deployment needs of those kind of applications, and how one impacts the other. Therefore, we propose to study the current state-of-the-art on multi cloud native applications, including the architectural patterns, the processes and methodologies and the challenges they pose to the DevOps teams.

Research methodology definition

A SLR is a method to identify relevant research, methods, and gaps in an existing research area. In this paper, we followed the fundamental methodology proposed in PRISMA [12] adapted to Software Engineering works [25] and updated as in [36]. Concretely we chose relevant papers from four reputable sources that are publicly accessible and already indexed in reference research databases (i.e. ACM, IEEE, Science Direct, and SpringerLink) delimiting our study to those tackling the multi-cloud issue from the application perspective. We have focused this work on studies published between 2011 and 2021 where most of the primary studies were published. However, we executed the search queries between years 2006 and 2021. This research analysis started in June 2021 thus we only considered publications until 2021 to acquire comparable information between years.

The year 2006 was selected following the approach of Kratze and Kint [6], who dated the birth of cloud the day in which the first general purpose public cloud service (namely the Simple Storage Service, S3 on 13th March 2006[2]) was launched by AWS. Nevertheless, as already introduced, the first accepted primary study is from 2011 in order to have a full 10-year gap.

For this period, we retrieved more than 900 peer-reviewed papers from journals and software engineering top conferences, where authors published research related to the multi-cloud application concept. We filtered these papers, following specific inclusion and exclusion criteria, to finally obtain 88 primary studies.

Based on the definition of Kitchenham et al. [27], where it is indicated that the systematic reviews of the literature are carried out to "*identify, analyse and interpret all available evidence related to a specific research question*", this systematic literature review aims at the following:

- To establish the body of knowledge around the concept of multi-cloud and more specifically from the application perspective,
- To better understand the challenges that the developers of these applications address and to pave the way on the multi-cloud-native -by-design concept, through the characterization and discussion of exiting challenges and proposed solutions,
- To identify the specificities of the DevOps philosophy for multi-cloud native applications highlighting the distinguishing factors from traditional cloud applications,
- To determine the main security threats and countermeasures affecting multi-cloud native applications,
- To provide baseline topics to assist with further research through the identification of research gaps and opportunities for the design, development and operation of multi-cloud native applications.

As stated before, our work was guided mainly by the PRISMA methodology [12], and it has been aligned to the general guidelines for SLRs in the context of Software Engineering [36]. PRISMA looks for an evidence-based minimum set of items aimed at helping authors to report a wide array of systematic reviews and meta-analyses. PRISMA focuses on ways in which authors can ensure a transparent and complete reporting of this type of research.

Being these principles our main basis for defining the methodology for our work, we also took into consideration guidelines and critical reflections from the general principles for the implementation of mapping studies [37]. In [38] Kitchenham et al., contrasted the main different characteristics between SLR and mapping studies. Both systematic literature reviews and systematic mapping studies are analysing primary studies defined as "*an empirical study investigating a specific research question*" [27]. However, SLR and mapping studies are so called secondary studies as they "*study all the primary studies relating to a specific research question with the aim of integrating/synthesizing evidence related to a specific research question*" [27]. In this way, SLR and mapping studies present some differences with respect to the research questions, search process, search strategy requirements, quality evaluation and results. Such differences are motivated by the specific objectives of each of the work types.

The aim of the SLR is to aggregate evidence on a concrete topic and, hence, a very specific objective needs to be formulated (i.e., whether an intervention is practically useful by the industry). On the contrary, the research questions in mapping studies are more general as they aim to discover research trends (i.e. publication trends over time, topics covered in the literature). According to guidelines for systematic maps and reviews in [27, 37] and following the strategy proposed by Kratzke in [6] we

[2] https://aws.amazon.com/releasenotes/release-amazon-s3-on-2006-03-13/ (last access 23rd of July 2021)

combined both approaches with the aim of complementarity. Therefore, as our main objective is to characterize multi-cloud native applications from the architectural perspective and from a point of view of the developer, highlighting open issues and future research trends, we have adopted this novel mixed approach, which contributes to achieve our two objectives:

- to characterize the multi cloud native application concept based on the analysis of existing studies through an SLR, and
- to discover research trends and open issues in the development and operation of multi cloud native applications.

For our research, we decided to keep the focus of the protocol for the SLR by following both the PRISMA methodology [12] and the approach proposed byKitchenham [27], as these follow a well-defined, repeatable methodology to identify and analyse the available evidence with respect to a specific research question (see Fig. 2). These outcomes are discussed in Section 3.

We have also introduced another change into the classical SLR protocol since we conducted a review of similar or related systematic reviews that could also serve as input for the interpretation and discussion of the research questions. In this case, the review process proposed for this secondary studies analysis was directed and narrowed by the search of only relevant publications with high citation indexes. The outcomes of this sub-review have been used to enhance the current study, both in terms of methodology (i.e. application of new steps in the review protocol) and for the review itself (i.e. inputs the interpretation and discussion). Finally, we used the mapping guidelines to inventorize the papers on the topic related to "cloud-native applications", mapping these into a classification that allows us to get insights on the state of practice and state of research. This approach has allowed us to discover research gaps and trends which are discussed in section 4. Next, the different applied phases are detailed.

Phase 1: review definition and planning

The main goal of this phase is twofold: first to identify the need for a review and characterize it in terms of motivation, definition and objectives and, second, to propose and set up a review protocol to identify, gather and collate the evidences for the proposed review. Figure 3 depicts the steps followed during phase 1 and the outcomes of each step. These are described in the detail in the following sections.

Review characterization

The main motivation of the execution of this SLR is the need for getting an insight on the term "multi-cloud native application", as well as the challenges that the developers and operators of such applications may face. Cloud Computing emerged a little over 10 years ago. In 2009 first NIST published in the United States the definition on Cloud Computing, with the generic initial Cloud Computing terms [41], including today's well known concepts such as IaaS, PaaS, SaaS, or public/private/hybrid cloud computing. Since then, the Cloud Computing vocabulary has evolved and is continuously adapted to new paradigms such as Internet of Services, edge computing or serverless computing. Some of these terms are well known and properly defined by the research community while others still remain fuzzy and cause confusion in the practitioners and researchers. In this regard, in 2017 Kratzke and Quint carried out a study on the term "cloud-native application", where they prove a formal definition and understanding of the term and complemented it with related research trends [6]. This work motivated us in the uptake of a similar approach for the characterization of the "multi-cloud native application" term. Multi-cloud and hybrid-cloud are often understood as synonyms. Based on our experience, the term multi-cloud has been used from diverse perspectives, being infrastructural characterization the most used one. In this respect, multi-cloud is widely understood as the combination of multiple infrastructural elements (usually cloud services) where software applications are deployed onto. On the other hand, hybrid cloud comprises cloud services from different nature typically combining public and private cloud infrastructures.

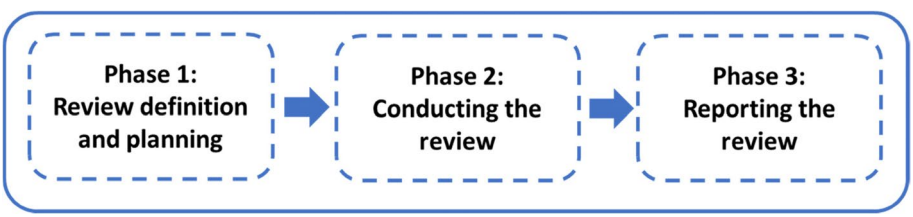

Fig. 2 Phases of SLR protocol [39, 40]

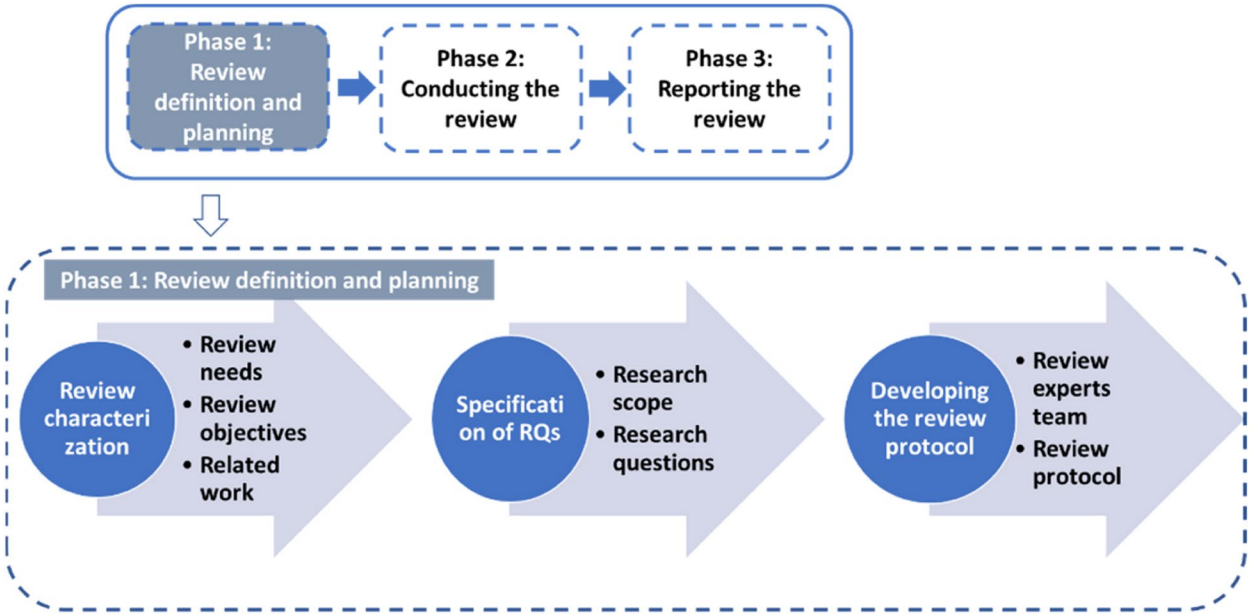

Fig. 3 Review definition and planning

Nowadays, developers of cloud-based software applications are also in charge of deploying them onto the cloud, while facing at the same time a change of philosophy in the way in which the lifecycle of an application is managed and understood, mainly driven by velocity and efficiency. This is currently achieved through the application of the DevOps philosophy [7].

Hence, developers of the applications to be deployed on the cloud need to understand better the options that cloud infrastructures and services offer them in terms of elasticity, performance or availability so that they intentionally design the software for such elastic cloud infrastructures and services. In the last years, the possibilities that cloud services offer to the DevOps teams have increased by a lot, and the combination of different cloud service offerings coming from the same or other cloud providers to deploy a software application has become a real option, especially in those applications with critical non-functional requirements (NFR) in terms of security, performance, availability of costs. In this context, the "multi-cloud native applications" term becomes crucial. Initially, in the literature and in the industry, the term multi-cloud application was referred to applications replicated over multiple cloud services, serving mainly as a backup. Now, and with the upcoming of new practices with respect to software architecture like microservices, containerization and serverless, the reality of software applications that have multiple components that can be deployed at the same time on several cloud services providers using different cloud services from each one and different are getting more and more relevance. In spite of this momentum, up to our knowledge there is no work that characterizes and addresses fully the meaning and substance of the concept of multi-cloud, hence establishing the main characteristics that have to be fulfilled in order for an application to be called multi-cloud native. What is more, from the perspective of the application. There is also a lack in the analysis and verification of the existence of specific needs of multi-cloud compared to just a traditional cloud native application.

Therefore, our literature review has as main objective *to achieve a common understanding of what the term "multi-cloud native application" means and its implications in other spheres such as technologies, standards and challenges taking into consideration based on the scoping that other relevant works in the area did*. This global objective can be broken down into the following sub-objectives:

- *Objective 1*: Meaning and characterization of the multi-cloud concept from the application perspective.
- *Objective 2*: Definition of the characteristics of a "multi-cloud native" application.
- *Objective 3*: Analysis of research trends and existing challenges in multi-cloud by design, development, and operation

With the objective of having a better understanding of the current challenges and the objectives to pursue

within this work we conducted, in addition, a survey on works like the one that we are proposing. The analysis of these studies is reported in Section 4.

Specification of research questions

The research questions need to be complete enough in order to allow for an adequate investigation and discussion around the main goal of the proposed review.

They are defined as follows and specified in Table 2:

RQ1: Where does the term "multi-cloud"/ "hybrid-cloud" come from?

We would like to know the origin of term multi-cloud and current existing synonyms such as "hybrid-cloud". When were they firstly used, by whom, in which context and what was the main meaning for them? Through this question we also want to analyse the evolution of the terminology over time in terms of meaning and context.

RQ2: Is there a common understanding of the term multi-cloud / "hybrid-cloud"?

This research question seeks to analyse the different meanings of the term multi-cloud "hybrid-cloud" used in the literature. There could be different contexts where the terms multi-cloud or hybrid cloud are applied. Differences in the meaning itself can also exist, i.e.: 1) multi-cloud understood at infrastructural level as different cloud services but the same cloud provider, 2) multi-cloud understood as infrastructural level as different cloud services from different cloud providers, 3) multi-cloud understood at application level as one application deployed in one cloud service and replicated as a whole in another cloud service, etc.

We want to specially analyse the works in the literature which tackle the term from the application perspective, trying to relate it to the design characteristics and pattern that a multi-cloud should follow. This question will help us to provide a definition for the term multi-cloud native application.

RQ3: Which are the architectural characteristics of "multi-cloud native"/"hybrid-cloud native" applications?

We seek to characterize multi-cloud native applications in comparison to traditional cloud applications, being cloud native or the result of a migration to a cloud – based architecture. This characterization should address multi-cloud native applications from different aspects such as technologies, standards, processes, and so on. used in the literature for their architectural definition, design and development. To this end, our aim is to identify different techniques, processes and technologies proposed in the literature to realize the concept of multi-cloud by design at application level.

This research question is broken down into the following sub-questions:

- *RQ3.1* Which architectural patterns have been proposed for multi-cloud native by design?
- *RQ3.2* Which technologies have been proposed for multi-cloud native by design?
- *RQ3.3* Which standards have been proposed for multi-cloud native by design?
- *RQ3.4* Which development processes or methodologies have been proposed for multi-cloud native by design?

RQ4: Which are the main challenges for the developers and operators of "multi-cloud native"/ "hybrid-cloud native" applications?

This question allows knowing which are the main challenges faced by both the developers and the operators of "multi-cloud native" applications as reported in the literature. In this way, we try to unveil which are the critical aspects over the application lifecycle, namely in what is called SDLC and SOLC, claimed by the researchers and practitioners. This question will allow us to identify problems, and also proposed solutions in the context of the development and operation of multi-cloud native applications while at the same time derive unsolved issues that could divert into new research trends for further work. We have decomposed the RQ4 into the following sub-questions:

- *RQ4.1* Which are the challenges that developers of multi-cloud native applications face during the development of the applications?
- *RQ4.2* Which are the challenges that operators of multi-cloud native applications face during the execution time (i.e., runtime) of the applications?
- **RQ5: Which are the main security threats and countermeasures in "multi-cloud native" applications?**

Being cyber-security and trustworthiness two of the major factors that cause the reluctance of organizations in the adoption of cloud computing, in general, and multi-cloud in particular, we have proposed this question to provide insights into this affirmation from the academic perspective. We analyse the main security threats reported in the literature as well as the taken countermeasures to prevent or deal with them and, furthermore, we pose whether multi-cloud improves security by properly diversifying the attack surface or mines it by extending the attack surface.

RQ6: Which are the promising trends in the design, development, and operation of the "multi-cloud native"/ "hybrid-cloud native" applications that can be detected?

This question allows summarizing the information collected from the previous research questions in a more generic way. For this purpose, we have analysed the information reported in the literature with respect to future trends and potential new areas of research in the context of the development and operation of multi-cloud native applications, both derived from the analysis of the main outcomes of the previous research questions.

Developing the review protocol

The review protocol aims at describing the process followed by the researchers during the execution of the SLR. As introduced in Section 2, we have developed our review protocol based on 1) the PRISMA methodology [12], and 2) the generic guidelines for SLRs in the Software Engineering domain documented by [27]. Figure 4 depicts the steps followed to conduct this SLR.

First, the recruitment of the research team is conducted. The next step is the definition of the research questions which this SLR intends to answer, as already described in the previous Section 2.1.2. After that, have defined the search keys for each of the digital libraries used in this analysis. We also set up the study selection criteria procedures within which these criteria are applied by all the researchers participating in this work including the inclusion and exclusion criteria definition, and resolution of disagreements. Next, the checklists and templates to study the quality assessment are defined. Then, we detail the data extraction procedure, the related data extraction forms and the supporting tools. Finally, we describe in detail each of the steps in the development of the review protocol.

- *Recruitment of the SLR Team*

The review team members have been selected trying to gather an interdisciplinary team covering the different relevant aspects to be addressed with the work. To this end, experts in different facets of cloud and multi-cloud were on-boarded with knowledge on cloud computing, federation of clouds, cloud security, software engineering for the cloud and at the same time, experts with different backgrounds were requested to participate (i.e., Universities, Technology centers, Industry). One of the roles of the experts participating in this SLR has been the assurance of the quality of the study as well as the validation of the works and the participation in the discussion of the results.

- *Search strategy definition for primary studies*

Based on the research questions proposed, we identified the key words to be used when carrying out the primary study searches.

We conducted our search for studies in the electronic sources listed in Table 3, following the recommendations to perform literature reviews in software engineering [27].

As for the selection of keywords, in [6], the authors analysed the meaning and characteristics of the "cloud-native" applications referring to those software developments that are intentionally designed for the cloud. Taking this as inspiration, we have tried to achieve a similar result with the term "multi-cloud native" but we discovered that as such is rarely used as such in the literature. On the other hand, relevant works addressing the characteristics of multi cloud applications do not use the term "native" so we have decided not to restrict our search string with the term native.

So far, the term multi-cloud or "hybrid cloud" are very intensively used in literature. However, the main usage of the terms is devoted to describe the infrastructural elements of the execution environment of a system. Therefore, we need to limit our results to those addressing the multi-cloud concept from the application layer perspective, rather than from the infrastructural layer point of view. In order to do that, we have included the terms "architecture", "design" and "structure". Alternative synonyms were incorporated using the Boolean "OR", while the main terms were linked using Boolean "AND". This way, by combining the keywords A, B, C and D, in Table 4, we have been able to find studies that focus on

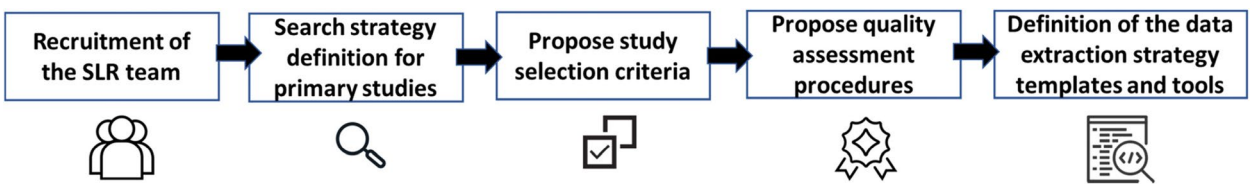

Fig. 4 Proposed literature review protocol

Table 2 Research questions

N°	Research questions
RQ1	Where does the term "multi-cloud"/ "hybrid-cloud" come from?
RQ2	Is there a common understanding of the term "multi-cloud"/ "hybrid-cloud" term?
RQ3	Which are the architectural characteristics of "multi-cloud native"/ "hybrid-cloud native" applications?
RQ3.1	Which architectural patterns have been proposed for multi-cloud native by design?
RQ3.2	Which technologies have been proposed for multi-cloud native by design?
RQ3.3	Which standards have been proposed for multi-cloud native by design?
RQ3.4	Which processes or methodologies have been proposed for multi-cloud native by design?
RQ4	Which are the main challenges for the developers and operators of "multi-cloud native"/" hybrid-cloud native" applications?
RQ4.1	Which are the challenges that the developers of the multi-cloud native application face during the development of the applications?
RQ4.2.	Which are the challenges that the operators of the multi-cloud native application face during the run-time of the applications?
RQ5	Which are the main security threats and countermeasures in "multi-cloud native" applications
RQ6	What promising trends for the design, development, and operation of the "multi-cloud native"/ "hybrid-cloud native" applications can be deduced?

Table 3 Results from the digital sources (papers might be listed in two or more sources)

Electronic Source	URL	Papers found
ACM Digital Library	http://portal.acm.org	88
IEEE Digital Library	http://ieeexplore.ieee.org	399
Science@Direct	http://www.sciencedirect.com	166
SpringerLink	https://link.springer.com/	287

Table 4 Keywords used to build the search string

Term	Keywords	Alternatives
A	Multi-cloud	"multi-cloud", "multi cloud", "multicloud"
B	Hybrid Cloud	"hybrid cloud""hybrid-cloud"
C	Architecture	"Architectures", "Architecture"
D	Design	"Designs", "Design"

multi-cloud as intended but from the application perspective. We have also considered to include the word "structure" in our search string, seeking to address the structural aspect of the application architecture but after reviewing manually the results, all the relevant papers were already included by the proposed search string. Hence, we decided not to include it, in order to avoid the inclusion of irrelevant studies in a future replication of this study. The final keywords used for the creation of the search string are presented in Table 4.

We have searched for contributions in and after 2006, following the previous study [6] where 2006 is set as the first time when the term "cloud-native" was found. We have assumed that, similarly, "multi-cloud native" related relevant studies would not present until that date. We have limited the search to contributions having the key words in their title, abstract or keywords. Full text was not intentionally included, as we wanted to search for studies where the multi-cloud and the architectural aspects were intentionally taken so much into consideration, that they should be explicitly mentioned in the title, abstract or keywords.

Following the strategy described, and after a series of tests we built the generic search string (Figure 5).

Considering that digital libraries have specific configuration and parametrization options for their digital search interfaces, we realized that we could not use this single generic search for all the digital libraries. Therefore, we decided to adapt it and create specific search strings for each bibliographic source. Several tests and discussions between the review team members were needed until we reached to an agreement where each string would kept semantically and logically equivalent. In Table 10 in Appendix the details of each specific search string are presented.

As part of the search strategy, we defined a secondary search phase by what it is called backward snow-balling [42], which implies the examination of the primary studies' references looking for other relevant papers. The selection of the studies from the snow-balling was performed during the full reading and data extraction

$$("hybrid\ cloud"\ OR\ "hybrid-cloud"\ OR\ "multicloud"\ OR\ "multi\ cloud"\ OR\ multi\text{-}cloud)\ AND\ (\text{architecture}OR\ \text{architectures}OR\ \text{design OR}\ designs)$$

Fig. 5 Used search string

Table 5 Inclusion and Exclusion criteria

Inclusion criteria
1. Keynotes, conference papers, journal papers, books and book chapters dealing with the design and characterization of applications intentionally designed to be deployed on a multi-cloud based distributed infrastructural ecosystem
2. Publication language is English
3. Peer reviewed articles
4. Keywords are included in the title and / or the abstract
5. It is clearly stated that the paper focuses on the field of software engineering
Exclusion criteria
1. Full text not available
2. Grey literature
3. The abstract or content of the paper made obvious that a contribution lays out-side the scope of the study which is the characterization of multi cloud native applications.
4. Duplicated studies
5. Proceeding letters
6. Short papers/posters

of primary studies. When relevant, they were incorporated to the set of selected works by applying of the inclusion and exclusion criteria.

- *Study selection criteria*

In Table 5, we report the inclusion and exclusion criteria that were adopted to identify the selected studies.

For the selection and management of the bibliographical works, we relied on three main tools: Parsifal,[3] Google Workspace[4] and Zotero.[5] Parsifal was used to characterize the review, create the search string, import the search studies, and create the data extraction forms. It also provided us with the capabilities to categorize the studies into included or excluded in a collaborative environment where all the researchers could participate simultaneously if desired. Furthermore, we used Parsifal to gather the results from the full text reading phases along with the information obtained from extraction of the data. Zotero was used as repository for the articles returned from the databases and also for the ones selected as primary studies to be part of this review.

We have used Google Workspace as a collaborative tool to support the discussion sessions and the classification of the studies.

[3] https://parsif.al/

[4] https://workspace.google.es/

[5] https://www.zotero.org/

- *Quality assessment procedures*

Following the approach by Tacconelli [43], who stated that *"there is no approach to assess quality. The importance of each aspect of quality will depend on the approach and nature of the review. The best approach will be determined by contextual, pragmatic and methodological considerations of the study"*, we have decided not to impose specific further restrictions to the papers in terms of quality apart from those derived from the selection criteria. To reinforce this aspect the study selection process was performed twice, i.e. each article has been read for inclusion/exclusion by two different experts. The first time, two of the review team members read all the titles and abstracts from the studies returned by the search query. Next, an expert validation phase was conducted. In this case 4 more experts read the initially selected papers and validated or refused the initial classification. Besides, the selected works were thoroughly read by the authors who approved or rejected them based on their experience.

- *Data extraction strategy*

For data extraction, it was agreed to read all the 114 selected works and complete the templates and forms designed for that purpose. These forms were devised to help us to answer the posed research questions and classifying the papers. The specific data extraction forms are detailed in the Table 10 in Appendix. The details on the forms and number of initial papers included are explained in Section 2.2.2.

Phase 2: conducting the review

During this phase the review protocol defined in Section 2.1.3 was executed. Figure 6 details the activities performed during this phase which are detailed in the next subsections.

Conduct search for primary studies

The main action of this activity was to define and apply the search strings for each of the on-line digital libraries as defined in Table 10 in Appendix and in Table 3. Overall, our search in all the databases resulted in 940 documents. All the searches were based on the title, keywords and abstract. In Fig. 7 the percentage of articles retrieved per source is shown.

Screening of papers and expert validation

As already introduced in Section 2.1.3, the screening of the papers was performed twice. Figure 8 details the selection process and steps. First, the two primary

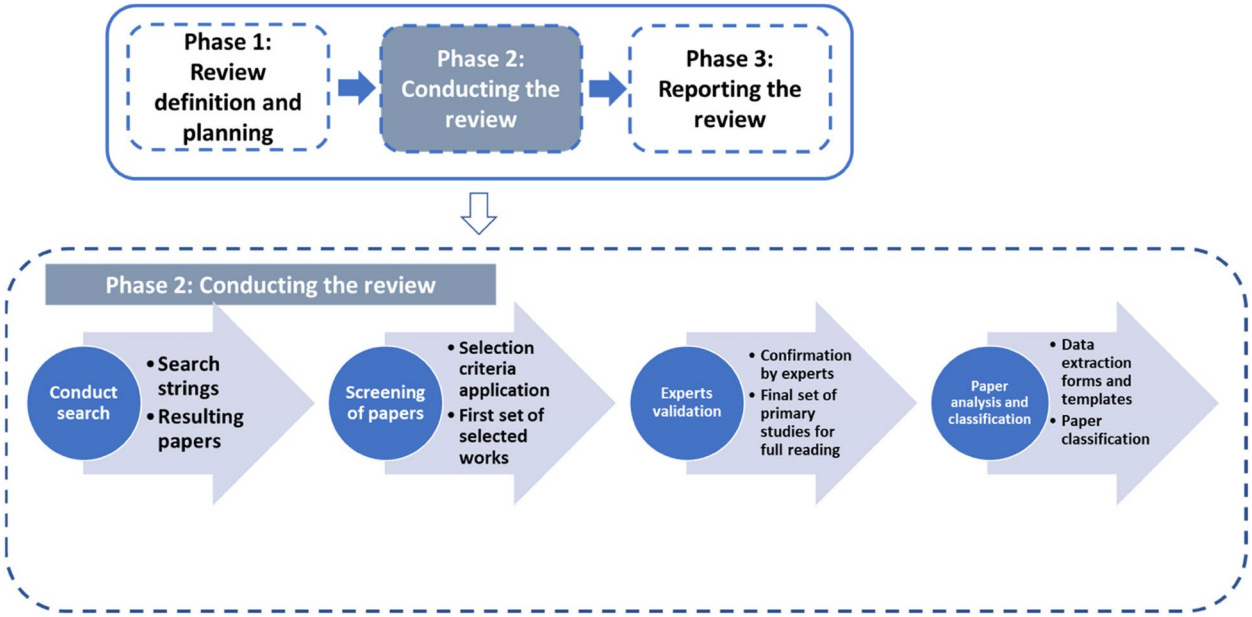

Fig. 6 Phase 2: Conducting the review

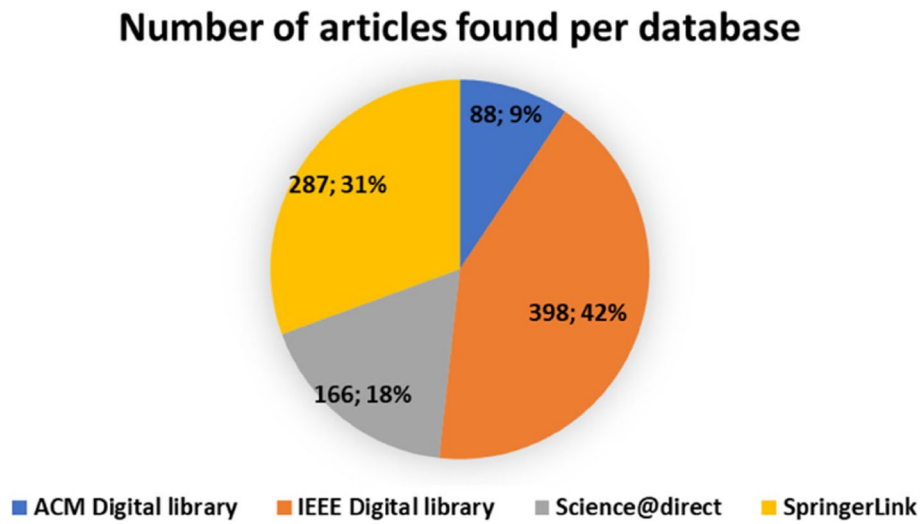

Fig. 7 Articles per source

authors applied the selection criteria into the 940 initial documents. Some of the duplicates were automatically removed by the management tools used, but others were manually excluded if a duplicate not found by the tool was detected.

In order to validate the initial selection of works and having agreed to be very inclusive in the first phase (i.e., when having questions whether including or excluding the study including it was chosen) a second phase of *papers screening* was performed by 4 experts. In this second phase, the initially selected papers were assessed again and confirmed (or not) for inclusion in the final set of primary studies for full reading. As shown in Fig. 8, from this phase the final set of 125 works were selected by the experts for full reading.

Finally, in the *expert validation* step, the full reading of all selected works was performed. From this phase 37 works were removed. During this full reading, also the snow-balling process explained beforehand was performed. As a reminder, this snow-balling process consisted of screening the references of the articles to identify potential interesting works missed in the

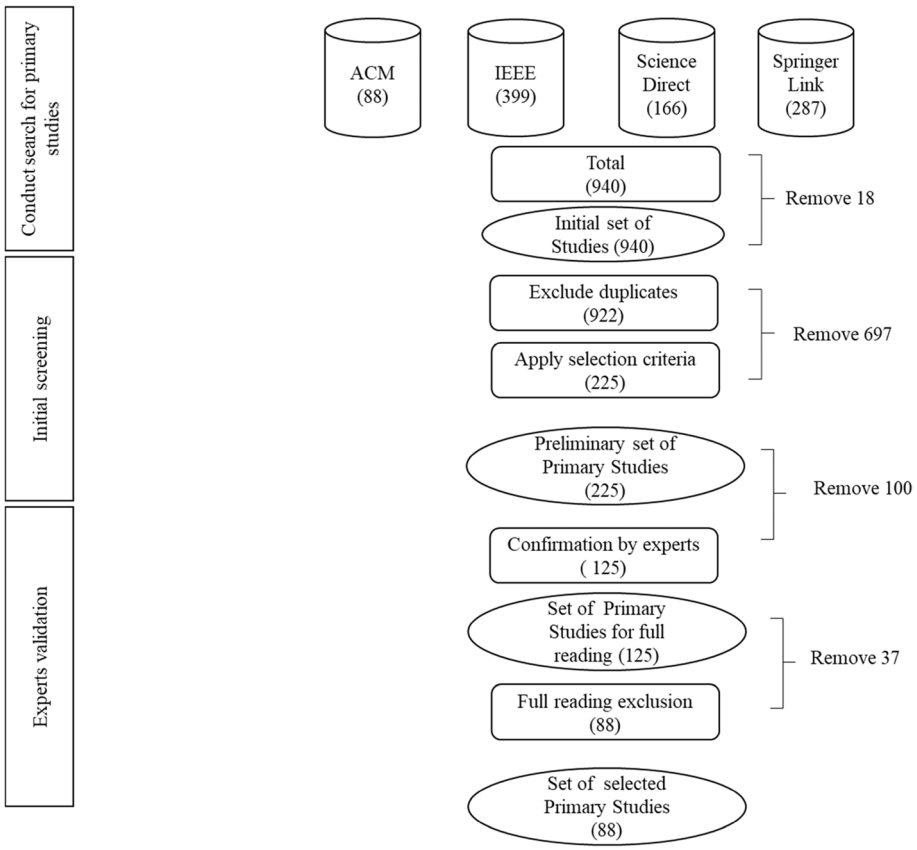

Fig. 8 Detail of the selection of primary studies during the screening of the papers

current list of primary studies. In this case, there were no new articles selected. Finally, 88 primary studies were considered for data extraction and classification.

With respect to the sources, we report in Fig. 9 the source used for the preliminary accepted papers. We noticed that IEEE library was the one returning the greater number of results while ACM returned the least of all. Considering the acceptance percentage of the papers per venue (number of papers accepted after full reading vs. selected in the initial screening), the main difference laid on the IEEE source. This can be explained as for the impact of the library and its

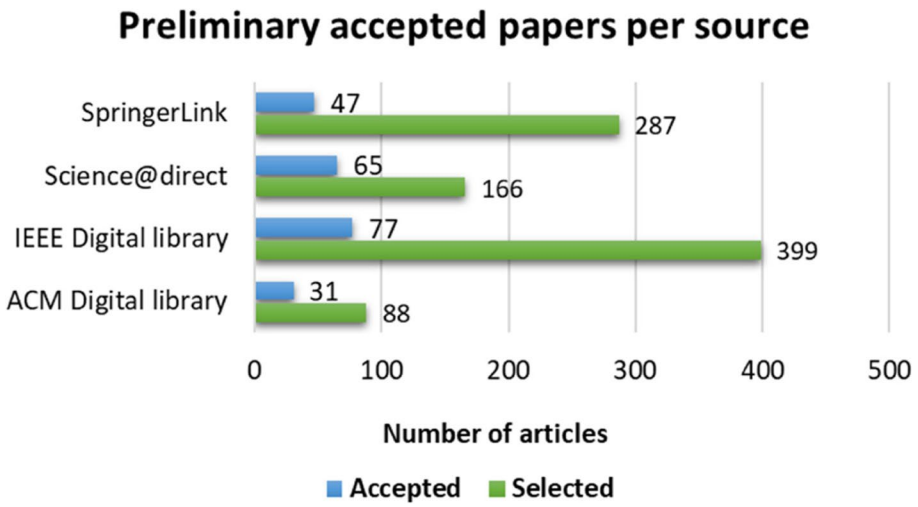

Fig. 9 Selected and preliminary accepted papers per source

relationship with the aspects related to infrastructure and execution environments, were the term multi-cloud or hybrid cloud is very commonly used. On the contrary, when specifically searching for the software architectural perspective, a great majority of the papers were discarded.

Paper analysis and classification

The first step of this activity was to create the data extraction form where to collect all the relevant data from the full reading of the selected studies. Apart from extracting basic elements for articles such as DOI, the title, the authors' name, the venue or the year of publication we have also included other relevant data that would help us to classify more accurately and analyse further the information with the end objective of finding an answer to the research questions. In Table 10 in Appendix the forms with the detailed information are presented.

The general process consisted of reading the full text and looking for the data to extract.

The full reading of the studies was performed by two researchers who also completed the data extraction form per paper. With this information, an initial classification was performed (see Table 6). The analysis and classification were supervised by the set of 4 experts (also authors of this article) who validated the classification and helped to structure the encountered information to further discuss the proposed research questions. The detailed discussions and reporting of the findings are presented in Section 3.

As introduced before, this phase included the extraction of data from 88 selected primary studies, from which we extracted data for several aspects with the aim to answer our research questions. Generic aspects, such as date or contribution types, helped us in different dimensions. For example, the date allowed us to follow up the timeline of the different addressed research topics and challenges, while the contribution types helped us to establish the maturity of the research area. All these overview results and statistics are presented in Section 3, while the detailed discussion on the research questions is reported in Section 4.

Table 6 Studies classification per multi-cloud definition

Multi Cloud Concept	Primary Study
Hybrid Cloud (public vs. private)	[44–52]
IoT or physical nodes	[53–56]
Different cloud services from different cloud providers	[8, 17, 26, 29, 31, 34, 57–73]
Multi-cloud in a broader sense	[74–76]
Federated Cloud Services	[17, 32, 77–81]
Multi-cloud Services Communities	[82]

Threats to the validity

The presented SLR aims to be as systematic as possible. However, the following risks affecting its validity have been identified.

External validity

As presented above, we have selected four scientific databases. This selection may bias the process as we may have missed some most cited articles which are not included in these databases. The impact of this threat was minimized by the snow-balling process conducted during the full reading, and by reviewing the references of each publication verifying if we lacked relevant studies. Consequently, the main threats to external validity are:

- *Validity of the population*: we reviewed a large number of documents to reduce the possibility of missing any relevant publication. When reviewing the title and abstract we e followed an inclusive approach, and when we had questions whether to include or not a paper, the decision was taken in the full reading phase. .
- *Ecological validity*: the possible errors in the materials and the tools used were minimized by using automatic tools rather than relying on manual methods.

Internal validity

The bias of individual researchers when evaluating their assigned primary studies can be another threat to validity. To overcome this threat, we followed a predefined procedure, specifically for the quality assessment, where each study was reviewed by two different experts. The selection of keywords can be also considered as a threat to internal validity. We have selected a number of synonyms well known and broadly used by the cloud community to minimize this threat.

Overview of the SLR primary studies selected

As illustrated in Fig. 8, from the initial set of 940 results, only 88 primary studies were identified as contributors to the topic of multi-cloud native applications. In this section we present the statistics referring to the research methods used, the kind of studies provided as well as the type of contributions channels discovered and the related information about these.

In particular, we present an overview of the body of knowledge found as a result of this review (considering the 88 finally selected primary studies). The primary studies were classified according to the research method used in the study, as defined in Table 10 in Appendix. Figure 10 shows the distribution of publications per types of research, namely solution proposal, validation research,

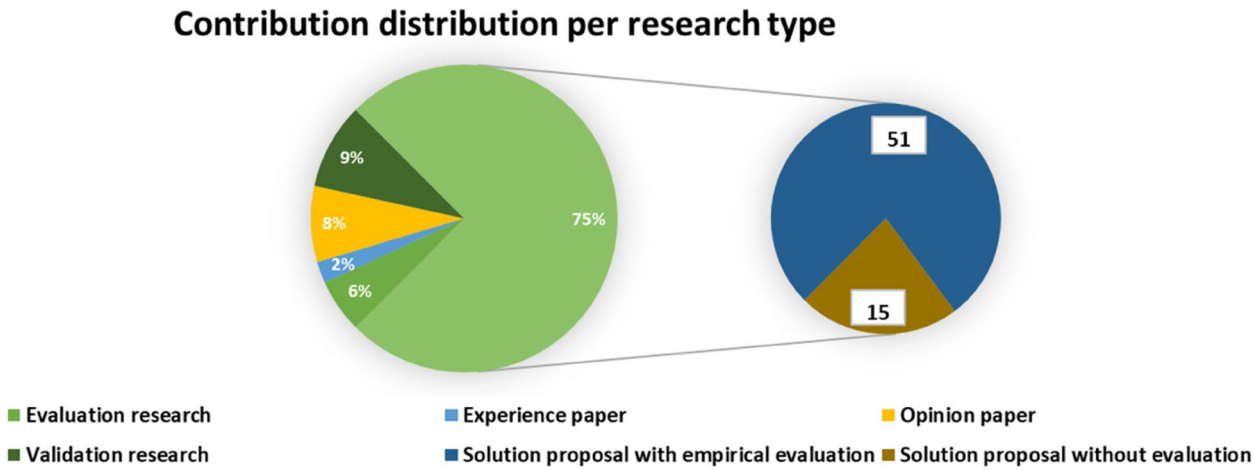

Fig. 10 Publication distribution per research type

opinion paper, experience paper or evaluation research and solution proposal. This last one can also be divided into solutions with empirical evaluation and without any evaluation.

On the pie on the left, we can notice that most of the studies included an evaluation phase of the proposed solution (75%) and 9% were classified as validation research. On the contrary 8% of the papers were opinion papers, 6% was evaluation research and 2% were experience papers. Interestingly, we only found 3 surveys/or reviews in the area (classified as part of the opinion papers), which reinforces the need of such an analysis in the topic of multi-cloud native applications. From the papers which included an evaluation phase (right most pie), 51 included an empirical evaluation while solution proposals without a full-blown validation were also significant (15 out of 66) using as evaluation method laboratory experiments and not real practitioners.

In general, the results showed that from a scientific point of view, the body of knowledge is still at an exploratory stage since a high percentage of the studies presented several solutions but without a complete and rigorous validation case. This is natural in a fast-pacing research field (multi-cloud) which is continuously impacted by lots of novel concepts and technologies which may drive new techniques or methods in the context of multi cloud.

As shown in Fig. 11, the papers reviewed were published between 2011 and 2021. This fact indicates that this topic is still gathering lot of attention from the related community. Even though some studies were published in 2011 and 2012, most were published within last 7 years. Regarding the publication channels most of the studies were published in conferences proceedings (60%), while 35% were published in journals or magazines and the remaining 5% in the form of books.

Figure 12 shows how the proposed research topics to be discussed in Section 4 were addressed by the different studies. The most addressed topics were the multi-cloud concept and the multi-cloud by design. DevOps for multi-cloud and multi-cloud security were faced by a minority of papers compared to the two previous topics. This could be due to the generic nature of the two main topics tackled (the meaning of multi-cloud and multi cloud by design) and the more specific essence of the other two (multi cloud security and DevOps for multi-cloud).

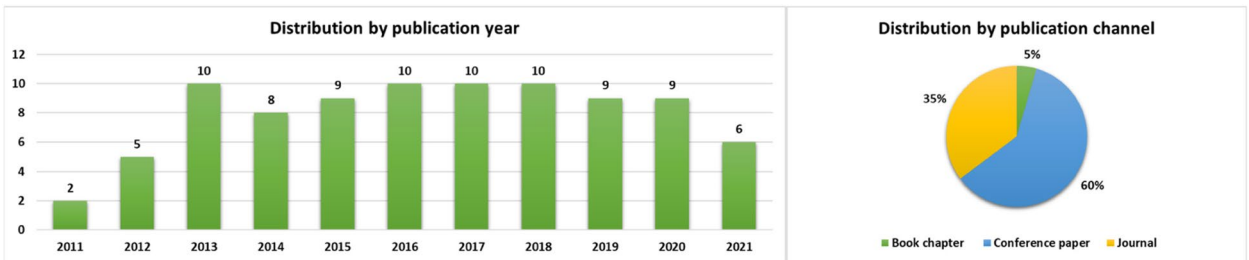

Fig. 11 Distribution by publication year and by publication channel (total number; percentage)

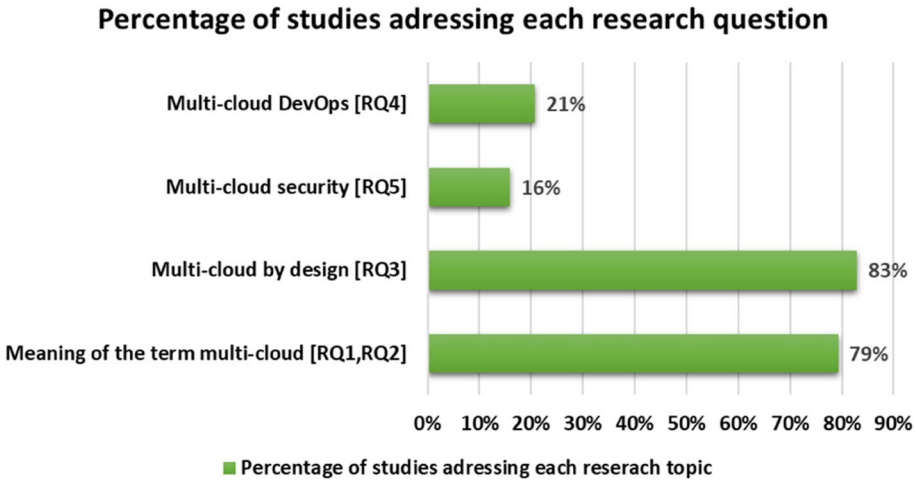

Fig. 12 Percentage of studies addressing each research question from Section 2

Discussion of research questions

Meaning of the term multi-cloud [RQ1] [RQ2]

For the characterization of multi-cloud applications, especially from the architectural point of view, in this work we tried to find out the different meanings of the term multi-cloud in the selected studies. We performed this analysis from two perspectives:

1. The analysis of the term multi-cloud in general mainly referring to the infrastructural elements composing this multi-cloud environments, to answer *RQ1. Where does the term "multi-cloud"/ "hybrid-cloud" come from?*
2. The analysis of the different existing definitions or characteristics for "multi-cloud native applications", i.e., applications which are explicitly designed to be deployed in multi-cloud scenarios in order to answer *RQ2. Is there a common understanding of the term "multi-cloud" / "hybrid-cloud" term?*

When analysing the terms used for defining or explaining the term multi-cloud several synonyms or related words come into play. We gathered these terms from the primary studies and represented in a word map in Fig. 13. It compiles a "cloud" of terms that are usually used with similar meanings but which are slightly different although usually relevant aspects that impact the way those cloud services are used and operated.

The term multi-cloud from the infrastructure layer perspective is used with several meanings which range from the cloud service deployment model (i.e. public vs. private) to the specification of the nature of the infrastructural element (i.e., virtual machines, database, storage, physical nodes). In Table 6 we classified the studies depending on how they characterize the term multi-cloud from the infrastructure point of view, coming up with these different definitions for a multi-cloud infrastructure:

From the primary studies analysed, more than the 40% of them did not provide a specific definition of the term multi-cloud, using the term without specifying its actual meaning in the context of the work presented. From the ones which did provide such a definition or explanation (the references included in Table 6), most used the term multi-cloud [8, 17, 26, 29, 31, 34, 57–73] for defining cloud services that were provided by different cloud services providers (29%). A significant number of these studies explicitly mentioned the lack of third-party services or any other intermediate layer providing federation mechanisms between these services [57, 66]. In this category, one of the studies [17] referred to both types of multi-cloud, with and without federation.

The second most relevant categorization for multi-cloud infrastructure focuses on the ownership of the cloud infrastructural services, usually referred as Hybrid Cloud to denotate the differences between public and private resources. In this sense, almost 10% of the studies [44–52] used the term multi-cloud to refer to the combination of in-house services, owned by a concrete company (the same as the one deploying the application there) and public services with more than one user (public cloud services). In this respect, [44] refers also to the concept of hybrid cloud, but with a slightly different meaning. In this primary study the authors referred to the physical distance between the client and the Cloud resources to classify them under private if the cloud vendor is located far away from client, or public, if the cloud vendor and the client are in nearby premises.

Fig. 13 Word map created with the terms collected from the definition of multi-cloud in the primary studies. The size of the font shows the frequency of the term found in the analysis. Bigger fonts are for more frequently used terms referring to multi-cloud

In this respect 8,5% of the studies [17, 32, 77–81], referred to federated cloud services, i.e. different cloud services coming from different or same providers, but that are already interoperable in the sense that an intermediate layer already provides the necessary capabilities for the usage of these services despite their peculiarities given that they are provided by different cloud providers.

Almost the 5% of the studies consider IoT environments as multi-cloud [53–56]. 4% considered a broader meaning definition for multi-cloud [74–76], including several concepts already discussed in the definition of multi-cloud infrastructures (i.e. resources form different cloud providers; aggregation of resources by a third-party broker; hybrid cloud architectures). Moreover, they add other novel concepts such as cloud continuum or osmotic computing [74].

In [38] authors merged the concept of service communities where the cloud services are categorized based on their functionality, and the concept of multi-cloud, where cloud services are grouped based on who owns such services. The combination of both approaches results in what they named as the multi-cloud services communities (Fig. 14).

Therefore, even though it does not exist any precise definition of what a "multi-cloud native" application is, we can conclude that there is a common but unconscious understanding of it across the analysed studies. We did not find any specific definition of the concept "multi-cloud native application" as such, although many of the studies characterizing multi-cloud environments also provided information about the types and the characteristics of the applications deployed on top of such multi-cloud environments (30% of the analysed works).

From the analysis of these studies, we found that multi-cloud native applications were structured into three main categories:

a) *Replicated multi-cloud applications* [34, 48, 67, 83]: applications which are deployed on multiple clouds but not at the same time. These applications make serial usage of services migrating from one cloud to another, driven by economic reasons like cost reductions, backups, emergencies, contract ending, etc. These applications are specially built to run on different clouds and to switch from one cloud to another. In this case the focus is on switching from one cloud provider to another including aspects such as data portability or interoperability.
b) *Distributed multi-cloud applications* [8, 29, 33, 40, 46, 51, 64, 73, 77, 80, 84–89]: multi-cloud applica-

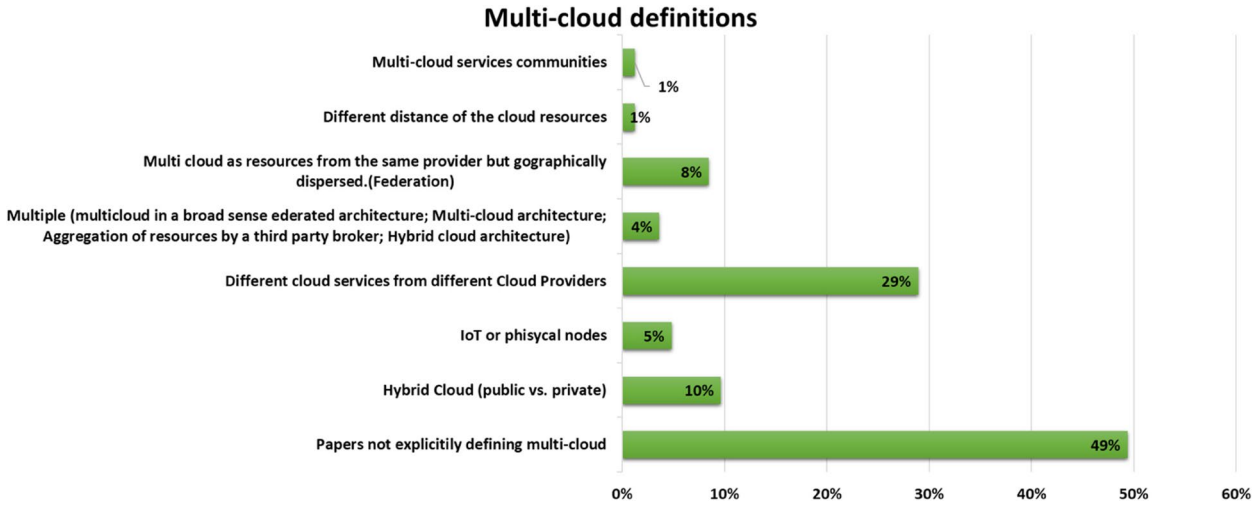

Fig. 14 Classification of Primary Studies based on their multi-cloud definition

tions with subcomponents that are explicitly simultaneously deployed on different resources from different providers, and which rely on the combined use of multiple independent cloud services. The simultaneous usage of services implies users accessing to services from multiple cloud providers and at the same time contributing to several benefits like high availability and fault tolerance, or cost reduction. The use of simultaneous multiple providers within a single application is driven by situations when a cloud provider does not provide all the functionalities required by the application. These applications can therefore exploit those cloud services which better suit their requirements respecting cost constraints, but also facing new challenges like the ones related to the control of their security, the management of such complex environments or the distributed architectural related implications for the design phase of this type of applications (i.e. partition of application logic, partition of application data).

c) *Multi-cloud applications covering the serial usage of cloud services (replicated multi-cloud applications) and the simultaneous usage of cloud services (distributed multi-cloud applications)* [44, 79].

While replicated applications do not need to coexist with more than one cloud environment, distributed multi-cloud applications are simultaneously being run into heterogenous and diverse cloud services (in terms of location, management systems, technology, interfaces, etc.). This is the kind of application that we try to characterize, understand and analyze the underlying challenges in this study.

RQ1/RQ2: Where does the term multi-cloud/"hybrid-cloud" come from? Is there a common understanding of the term multi-cloud / "hybrid-cloud"? From the almost 1000 studies initially retrieved, we identified 88 primary studies relevant to the concept of multi-cloud and hybrid cloud. From these only 47 works provided a specific definition of the term, and most of them used it to refer to cloud services that were provided by different cloud services providers (24). The other half of the studies understood the term in different ways, focusing on different aspects of cloud services to make the distinction i.e. public vs. private ownership, existence of federation mechanisms, IoT environments and cloud continuum, Cloud Services communities. We have shown clear evidence that scientific contributions in the literature compiles a cloud of terms that are usually used with similar meanings but some slightly different but usually relevant aspects that impact the way those cloud services are used and operated. With respect to the concept of multi-cloud from the application perspective, we can conclude that even if there is no precise definition of what a "multi-cloud native" application is, there exists a common but unconscious understanding across the analysed studies. From the analysis of the studies, we can derive an initial classification for multi-cloud native applications covering the following three main categories: replicated multi-cloud applications, distributed multi-cloud applications, and a combination of both. We have focused our study on the characterization and understanding of the lifecycle of distributed multi-cloud applications referring to them as multi-cloud native applications.

Multi-cloud by design [RQ3]

The goal of this question *RQ3-Which are the architectural characteristics of "multi-cloud native"/ "hybrid-cloud native" applications?* is twofold. On one hand, we aim to understand if there are agreed architectural design patterns as there exists in the case of cloud native applications, either technology agnostic [56, 90] or technology dependent [22]. On the other hand, we also aim to see which technologies, techniques and standards are used for designing multi-cloud applications.

To answer this RQ we have decoupled it in 4 sub-questions:

- *RQ3.1 Which architectural patterns have been proposed for "multi-cloud" native by design?*
- *RQ3.2 Which technologies have been proposed for "multi-cloud" native by design?*
- *RQ3.3 Which standards have been proposed for "multi-cloud" native by design?*
- *RQ3.4 Which processes or methodologies have been proposed for "multi-cloud" native by design?*

In Table 6 and in the next paragraph, we present the answers to these questions that were extracted from the papers analysed.

Around 14% of the studied papers do not present a clear knowledge on architectural patterns, methodologies, technologies, or standards. Moreover, 17% of the papers state that they are based on, or compliant with, existing standards such as OASIS CAMP, OASIS TOSCA or NIST Security control framework. The standards considered by the analysed papers can be divided in two categories,(1) generic purpose standards such as CAMP, TOSCA or CAMEL [45, 48, 51, 72, 91] and, (2) security related standards such as security NIST, Oauth, CSA STAR program or SAML/2 [52, 60, 91, 92].

In the first group, OASIS CAMP defines an interoperable protocol that can be used to package and deploy cloud applications, defining interfaces for provisioning, monitoring and controlling [45, 48]. OASIS TOSCA [26, 51] is a language that describes the topology of cloud services with the purpose of easing their portability. Other standards mentioned include OCCI [17, 72], CDMI [72] (whose version 1.1 became ISO/IEC 17826:2012), or CIMI [40] (whose version 1.1 became ISO/IEC 19831:2015). These standards, however, do not focus on the architectural aspects of a multi-cloud application but rather on the deployment and portability of cloud applications. In the second set where the security related aspects are addressed, authentication, authorization or privacy protocols are tackled. However, all these subjects are handled from a generic perspective and not from the specific multi cloud perspective.

Some of the papers do not consider any specific standard in their solutions [8, 70]. Rather than that, they emphasise the lack of standards specific to multi-cloud, and try to address it through the adoption of other known approaches or development philosophies such as DevOps [8].

Close to 11% of the analysed literature state that they have implemented a *multi-cloud application using a loosely coupled architecture*, based on microservices and implemented through containers [31, 32, 55, 56, 63, 66, 84, 85, 90, 93, 94]. To this end, loosely coupled architectures are applied to different domains, such as IoT [55], fog computing [32], or osmotic computing [66].

Among the most used technologies, mentioned in close to 16% of these papers [17, 26, 31, 50–52, 56, 60, 63, 69, 95], stand out Docker, VMWare, JClouds, or REST APIs, which help to realize the loosely coupled, microservices-based architectural solution. For interoperability, ontologies and semantic models appear as the most named technologies. Other approaches are also mentioned such as the usage of MOMs [96].

Modelling is an often-used solution for the design of cloud applications, as reported by 9% of the papers. To this end, there are different modelling approaches reported: 1) the traditional model-driven design (MDD, MDE) [40, 46, 54] and 2) through specifically designed cloud modelling languages such as CAMEL, or CloudML, as well as other DSL and ad-hoc developed UML profiles for cloud applications [64, 85, 87, 97].

Cloud federation is also a hot topic with respect to multi-cloud design, as 6% of the papers tackled it. It is recognised as a concrete multi-cloud architecture (also called inter cloud [39]) which enables the optimal selection of cloud services [98]. Specific cloud federation models are mentioned in the studied papers, such as multi-tier cloud federation model [81] or multi cloud communities' architectures [82]. Usually, these multi-cloud based architectures are also enabled by other technologies, like optimization techniques [98] or brokerage facilities [78] for the selection of the proper cloud services.

As anticipated in Table 6, one of the mentioned topics related to the architectural characteristics of multi-cloud applications is security. More concretely, security by design, which tries to take into account security problems from the very early application development stages [80]. Many security aspects can be considered from the beginning of the application of the development of the application or even the design. Some of the ones mentioned in the studies can be applied to multi-cloud applications but they are not multi cloud or even cloud specific [71, 73, 95] like ciphertext policy attribute- based encryption. Others can pose specific security challenges related to the multi-cloud nature of the application, like data splitting through trusted cloud services providers [52, 68] or secure networking for virtual machines in the cloud [47].

RQ3: Which are the architectural characteristics of "multi-cloud native"/ "hybrid-cloud native" applications? From the papers analysed, there is no clear consensus on what multi-cloud by design is. While there exists agreed architectural design patterns for the design of cloud native applications, after the analysis made during this literature review, we found that this is not the case for multi-cloud native applications. Some authors (17% of the studies) rely on standards which however are not focused on the architectural aspects of a multi-cloud application but rather on the deployment and portability of cloud applications. We also found that close to 11% of the analysed literature have implemented a multi-cloud application using a loosely coupled architecture, based on microservices and implemented through containers, and 9% of the studies used modelling approaches (MDE,MDD, DSL) for the design phase. From these findings we can conclude that there are no specific patterns or design methodologies proposed by the authors of the analysed studies.

Existing challenges in the development and operation of multi-cloud native applications [RQ4]

As any software application, multi-cloud native applications can be analysed from their lifecycle perspective. This is the approach we followed to answer *RQ4- Which are the main challenges for the developers and operators of "multi-cloud native"/ "hybrid-cloud native" applications?* Thus, we have extracted the identified challenges identified 1) in the design and development phase of the application, 2) in the deployment and execution phase and 3) in the operation phase of multi-cloud applications. For each of these three main phases, categories of the most mentioned challenges were identified (Tables 7 and 8) and are discussed next.

Design and development

At design and development level one of the most cited challenges are related to the requirements elicitation phase. The challenges here arise due to the heterogeneity of the cloud services where to deploy the application. This situation gives the developer powerful information to meet application's QoS requirements (from location or user preferences to resources needs) [33], maximizing the benefits of the combination of the cloud resources in use [69]. On the contrary, it introduces a new variable for the software architects who need to match their requirements specification with the heterogeneous and usually different models of cloud services. This usually requires proper risk and costs analysis methods and advanced software engineering methodologies that not only guide developers at design time but also support application providers at runtime [48]. It also impacts on the number and type of NFRs. New NFRs such as bandwidth on demand or application-specific routing requirements need to be now considered [77]. Others, such as security, may need to be considered from another point of view, as a consolidated vulnerability model as point of reference for the concrete case of multi-cloud scenarios is lacking [101]. Therefore, different methods need to be explored for an efficient utilization of available resources [79]. Another consequence from the cloud service heterogeneity and the distributed nature of multi-cloud applications is that code must be partitioned and distributed between different cloud services. Software components need to be context aware partitioned, so that they are aware of the characteristics of cloud resources where they can be deployed. NFRs optimization (cost, latency, performance), components synchronization, and data consistency are the challenges identified here [61, 67, 102, 103]. Furthermore, the utilization of more than one target deployment resource types requires a cloud agnostic design of software systems [48] and specific programming models and application architectures so that essential characteristics like scalability can be acquired at application level [45].

The heterogeneity of cloud resources is driving the challenges in the deployment phase too. The analysis and comparation of various cloud solutions is still a hard task, with several open issues such as the lack of standards and models for cloud services description and operation [33, 104] or the mapping of subsets of services/components to physical resources in an optimized manner [48, 69, 79, 81, 101].

Table 7 Multi-cloud by design topics addressed by the primary studies

Multi Cloud by Design	Primary Study
Loosely coupled	[31, 32, 55, 56, 63, 66, 84, 85, 90, 93, 94]
(Design) Patterns	[26, 35, 47, 69, 81]
Modelling languages	[29, 40, 46, 54, 64, 85, 87, 97]
Cloud federation	[39, 78, 81, 82, 98]
Security by design	[44, 47, 52, 68, 71, 73, 80, 95, 99]
Technologies	[17, 31, 50–52, 56, 60, 63, 69, 89, 92, 95, 96, 100]
Standards	[8, 17, 26, 40, 45, 48, 51, 52, 60, 63, 70, 72, 91, 92, 95]

Deployment

The application of DevOps practices and concepts is another recurring topic. Traditional development and operation (DevOps) principles are reported to be not directly applicable to multi-cloud applications and therefore they need to be reconsidered taking into account the specific needs of these kind of applications [8, 40, 48, 105]. New activities need to be considered in the DevOps loop, such as deployment configuration optimization, multi-cloud deployment, and creation and monitoring of multi-cloud application SLAs.

We have also extracted and classified the challenges identified by the primary studies during the run-time of the application. From this perspective, the interaction and cooperation among participating providers are still a

Table 8 Identified challenges in the SDLC/SOLC of multi-cloud applications

Multi-cloud application SDLC/SOLC phase	Main challenges categories	Related Primary Studies
Design and development *(RQ4.1)*	Application components NFRs compliance and resource level matching.	[33, 48, 69, 77, 79, 81, 101]
	Software components partitioning	[61, 67, 103]
	Cloud agnostic application architectural models	[45, 48]
	Lack of specific cloud security standards	[96]
Deployment *(RQ4.2)*	Cloud services heterogeneity	[33, 45, 48, 59, 85, 98, 104, 106]
	DevOps practices specific to multi-cloud	[8, 40, 48, 105]
Operation *(RQ4.2)*	Dynamic re-adaptation	[48, 66, 102, 106, 107]
	Communication layer	[77, 96]
	Lack of specific cloud standards	[26, 61, 67]
	Maintenance & evolution	[58, 65, 72, 85]
	Cloud federation	[8, 51, 67, 78, 79, 81]
	Risk management and security	[45, 98]

complex challenge to be solved, due to the heterogeneity of the cloud management systems employed by the providers. Thus, multi-provider infrastructure operation under a federation of independent clouds and/or infrastructure components is still a challenge. Apart from the technical interoperability, federation goes one step beyond. It includes the management of business workflows, SLA management and accounting [67], and automatically contract negotiation [78]. The federated model fosters the building of trustworthiness between cloud providers through a trust-based model framework that allows clients to simultaneously use services from multiple clouds without prior business agreements and without adopting common standards and specifications among cloud providers. This is achieved by the federated model itself so that efficient resource management schemes need to be developed for better management, billing and keeping track of resources accessing from different providers [79].

Operation

Automatic re-adaptation and self-healing mechanisms [48, 66, 106, 107], is another topic that is usually highlighted by authors as an unsolved challenge. A multi-cloud environment provides countless possibilities and enables an ecosystem of endless infrastructural elements. This is especially relevant when re-configuration and self-healing is needed due to unexpected failures or non-compliance of the SLAs. Here, it is required a support for dynamic adaptation (or reconfiguration) of the applications in terms of replacing a service by an equivalent one (in case of quality degradation, high cost or service unavailability [106]). It needs the automation of triggering some adaptation actions (e.g., migrate some system components from an IaaS to another offering better performances at that time) [48]. Self-healing and dynamic re-adaptation are tightly coupled with the maintenance and evolution of the multi-cloud applications.

Maintenance involves all the activities required for the correct performance of the applications during the lifetime. In this respect, two main aspects are specially seen as weaknesses, and need to be addressed nowadays. First, the monitoring of heterogeneous resources at different levels, from the low-level monitoring (where different APIs need to be used based on the CSP), to the high-level multi-cloud application SLA (where the different metrics need to be combined to get the composed SLA [58, 65]). This is especially relevant when an audit of cloud services is needed, thus technologies to efficaciously and continuously audit cloud services are still in their infancy [65]. The other aspect highlighted is the migration between cloud providers, which is still a challenge due to the proprietary nature of the technologies used and the need of seamless portability of both stateless and stateful components, keeping always the business continuity, thus guaranteeing that the application is functioning [72, 85].

Communication layer and the dependency on the network of these distributed multi-cloud applications is also an aspect to be considered [77, 96]. The quality of the connectivity is one of the fundamental factors for the cloud service performances, as perceived from the end users. This aspect becomes even more critical in multi-cloud scenarios, where VMs belonging to the same or different cloud services are deployed on geographically distributed sites. The communication system becomes more complex when switching to a Cloud-to-Edge scenario. In this case, it is necessary to balance performance and security management, and this is not trivial at all.

Security at all levels and during all the application lifecycle needs to be specially considered (*RQ4*). Public and hybrid cloud scenarios are characterized by a constant flow of data which cannot be allocated to a particular

place. This brings uncertainty regarding the various data protection legislations, which transcends national borders and therefore complicate the compliance with the Data Protection legislations worldwide [45]. At the same time, cloud consumers need to address certain outsourcing risks coming along with the adoption of cloud services, such as those concerning the risk of shadow-IT, loss of control and transparency, security and business continuity [98].

Many of these aspects, and especially those derived from the heterogeneity of the current cloud services could be improved or even solved with the application of recognized of cloud standards. However, existing efforts for cloud standardization are still in their first stages and we are not expecting to have a mature solution soon. Moreover, cloud-vendors themselves are reluctant to unification approaches as they prefer to keep their competitive edge and diversity to attract customers [61, 67]. In many cases, owing to the lack of a shared standard for services' interfaces description and incompatibilities between the adopted data formats, it can be difficult to effectively compose cloud services and exploit their full functionality [26].

RQ4: Which are the main challenges for the developers and operators of "multi-cloud native"/" hybrid-cloud native" applications?
To answer this question, we analysed the challenges and problems encountered by the developers and operators during the whole lifecycle of the multi-cloud native applications that is, in the design, development, deployment, execution and operation phases.. From the analysis of the 88 works it can be derived that most of the challenges identified have their origin in the the heterogeneity of the current cloud services and this is an issue that affects all the phases in different degrees. Indeed, this heterogeneity is getting more and more important due to the incorporation of new infrastructural elements, especially now with the advent of the cloud continuum that will increase especially the complexity of the deployment and operation of such applications. Many of these aspects, and especially those derived from the heterogeneity of the current cloud services could be improved or even solved through the use of recognized cloud standards. However, existing efforts in cloud standardization are still in their first stages and we are not expecting to have a mature solution soon. Another identified challenge is the cloud providers' reluctance of providing unification or interoperable approaches. However, unless this is regulated to a certain extent or the cloud service providers see the benefit of building an interoperable cloud stack, a solution towards this is not to be expected soon.

Main security threats and countermeasures in multi-cloud native applications [RQ5]

Security issues still represent one of the major concerns of cloud customers in the adoption of cloud solutions. When talking about multi-cloud, new security challenges arise but also new opportunities to protect data and services that shall guarantee confidentiality, integrity, and availability. As already done with other research questions in this survey, RQ5-*Which security threats and countermeasures in "multi-cloud native" applications* (about new security threats and new countermeasures) can also be seen from different perspectives as resulted by the analysis of the primary studies. In particular, the problem is tackled looking at: 1) new security issues; 2) new countermeasures and opportunities for multi-cloud architecture, addressing aspects such as data protection, access control models, novel cryptographic mechanisms, privacy preserving mechanisms, policy conflicts management; 3) novel security-by-design methodologies and frameworks for multi-cloud. For each of these three aspects, categories of the most mentioned challenges were identified (Tables 8 and 9) and are discussed next.

From a security perspective, one of the main benefits of using multi-cloud is to preserve data confidentiality by sharing data over different providers, and overcoming the four important limitations of cloud computing for data storage: loss of availability, loss and corruption of data, loss of privacy, and vendor lock-in [68]. In this scenario, the main security issues in a multi-cloud application depend on different factors [90]. Some of them are properly related to the shared-responsibility model used to deliver and deploy a cloud application, but they are exasperated by the presence of multiple independent providers, that may result possibly, in conflicts. New issues, specific to the multi-cloud environment, are in fact related to the adoption of cryptographic techniques in multi-provider environments and on the adoption of different access control policies in multi-cloud, that can easily lead to conflicting access situations. In [44, 108] the authors presented a survey on the adoption of cryptographic techniques, with related key management problems, over multiple providers. In [65, 80] authors analyzed and discussed different security solutions to deploy, configure and monitor security controls when their cooperating components are hosted by different providers and related security issues. Finally, in [73, 75] authors analyzed and discussed possible security and policy conflicts in multi-cloud.

To overcome these issues, many security countermeasures have been proposed. To cope with management and organizational issues, novel security enforcement solutions [52, 86, 92, 95] and frameworks [44, 47, 95, 113] have been thought. The majority of them focused on new countermeasures and opportunities for the multi-cloud architectures, addressing data protection, access control models, novel cryptographic mechanisms, privacy preserving mechanisms, policy conflicts management. In particular, papers [49, 52, 68, 71, 86, 95, 99, 110–112] focused on (1) improving security by splitting data and processing services [49, 68] (2) with the adoption of novel homomorphic encryption techniques [111], (3) with the definition of novel security architectures [47, 52, 71, 95] and (4) with the adoption of a unified approach to manage access control policies and mechanisms [70, 82].

Table 9 Identified challenges in the Security of multi-cloud applications

Multi-cloud Security	Main challenges categories	Related Primary Studies
Security Issues	Common security issues	[90, 108, 109]
	Novel cryptographic techniques for multi-cloud	[44, 108]
	Security and policy conflicts in multi-cloud	[73, 75]
	Sharing security components and mechanisms in multi-cloud	[65, 80]
Security Countermeasures	Improving (Data) Security with multi-cloud	[35, 49, 52, 68, 71, 86, 95, 110–112]
	Security enforcement framework	[52, 86, 92, 95]
	Novel architecture to enforce security	[30, 44, 45, 113]
	Unified Access Control models	[70, 82]
Security-by-design methodologies	Security-by-design and SecDevOps	[57, 69, 91]
	Evaluating Security	[113]
	Security Framework and PaaS	[69, 87]
	Optimization and SLA driven design	[57, 91]
	Security driven management and provisioning	[96, 114]

Our survey concludes the analysis of different security life cycle management methodologies to introduce security-by-design approaches [91, 114] while developing multi-cloud applications.

The increasing security concerns in cloud environments, with wider attack surfaces and possible conflicting policies, has led many cloud customers to be now interested in knowing the security assessment of their applications. In view of this, it thus becomes necessary to ensure adequate transparency and security awareness in multi-cloud environments. Authors in [113] exploited the possibility to model and evaluate security, and to develop frameworks and platforms to provide security with a quantitative approach. Authors in [69, 91] introduced a security data model to manage security properties with Security SLAs. Other papers try to use quantitative approaches in the early design stages to drive the design and development of application components over properly selected resources [96, 114], or based on optimized configurations [57].

RQ5: Security threats and countermeasures in "multi-cloud native" applications. Security issues still represent one of the major concerns of cloud customers in the adoption of cloud solutions. During this review, we have analyzed security aspects from 3 perspectives: 1) new security issues; 2) new countermeasures and opportunities for the the multi-cloud architectures, addressing data protection, access control models, novel cryptographic mechanisms, privacy preserving mechanisms, policy conflicts management; and 3) novel security-by-design methodologies and frameworks for the multi-cloud. From this analysis we can conclude that the increasing security concerns in cloud environments, with wider attack surfaces and possible conflicting policies, related to the shared-responsibility model, it becomes necessary to ensure adequate transparency and security awareness in multi-cloud environments. Some solutions have been proposed using SLA based models or quantitative approaches to address these issues although they are in the early design stages. Moreover, policy related and standard based solutions are still needed to assure the trustworthiness of the cloud services in complex multi-cloud environments.

Research gaps and opportunities for the design, development, and operation of the multi-cloud applications [RQ6]

In this section we discuss *RQ6-What promising trends for the design, development, and operation of the "multi-cloud native/hybrid-cloud native" applications can be deduced?* As a result, from the analysis of the selected studies, we can conclude that the topic of multi-cloud appears to be highly relevant for researchers and practitioners. The software community has heavily contributed to its body of knowledge from the birth of cloud computing, and the results of this study demonstrate the great significance of multi-cloud to both the academic and industrial communities. However, in what respects the clear understanding and characterization of the term is still unachieved.

Each of the four themes identified, namely, 1) characterization of multi-cloud and multi-cloud native applications, 2) multi-cloud by design, 3) Development and operation approaches for multi-cloud and 4) secure multi-cloud native applications present opportunities for future research. However, the topics are explored in the literature at different levels, thus offering different research opportunities. The current research has been mostly focused on factors such as resource allocation, cloud federation, virtualization, and modelling for the cloud. From our study we have broadly identified the following opportunities for future research (Table 10):

- **Characterization of the cloud continuum and its relationship with the cloud osmotic computing paradigm** [74]. Cloud continuum is an emerging research topic that has arisen from the characterization of complex environments where every element

Table 10 Overview of research gaps and opportunities identified

Research topic	Research gaps and opportunities
Multi-cloud concept [RQ1, RQ2]	• Cloud continuum characterization and understanding • Incorporation of new paradigms to the multi-cloud concept: fog computing, osmotic computing
Multi-cloud by design [RQ3]	• Architectural patterns for multi-cloud native applications • Means and methods to model at high level of abstractions (platform/technology independent) heterogeneous infrastructural elements and application components. • Linking the applications models to the infrastructural models through NFRs characterization especially network, communications, security (i.e. especially data sharing) or even legal
DevOps for multi-cloud [RQ4]	• Lightweight benchmarking and multi-objective optimization for the selection of the best combination of infrastructural elements. • Federation models for the cloud continuum, including IoT and networks elements to the traditional cloud services. • Application self-healing and migration at run time, with special focus on data portability and stateful components
Multi-cloud security [RQ5]	• Standard security models or SLAs to evaluate security • Conflicting security policies • Frameworks to provide, assess and monitor security with a quantitative approach • Trustable cloud services • Cloud security posture management
Multi-cloud certification	• Compositional cloud certification and combination with IoT and 5G certification

at the infrastructural layer can be considered as part of such a continuum. Several approaches define and address the term multi-cloud from a restricted perspective where the adjective "multi" is in fact defining only two or three different types of cloud elements (e,g, virtual machine, storage, database). The rapid development of emerging cloud and edge services, fog, and the Internet of Things (IoT) covering the whole continuum – hence the name cloud continuum has resulted in a much more complex 1) management of services due to their heterogeneity, and 2) service classification, allocation of resources and provisioning.. **Osmotic computing** is a new paradigm that allows the service migrations leveraging FaaS and a hybrid architectural style which combines both microservices and serverless architectures. Current approaches like the one described above still focus a lot on the "infrastructural" side of the problem (i.e. resource allocation, migration) while leaving aside the implications at application and data level. Special attention to **data portability, and stateful components migration at run time** are identified as areas for future research.

- Although the usage of loosely coupled architectures based on microservices and implemented through containers are emphasized in many primary studies, we discovered that **currently design application patterns for multi-cloud native applications are underdeveloped**. In [48] an approach is presented where the focus is on portability between different given CSPs but no software design patterns are further provided. Besides the need of technology and CSP agnostic patterns a clear gap appears in solutions which focus on the **architectural aspects of a multi-cloud application** rather than on the deployment and portability of cloud applications. Again, the focus needs to be shifted form the infrastructural layer to the application layer. In this sense, further investigation is needed on new approaches for stateful and stateless application components design and partition, lightweight design profiles of software components to be deployed on the edge (or on the cloud continuum), or reference architecture models for multi-cloud native applications in its broader sense.
- The **application of the DevOps principles to the life-cycle of multi-cloud applications** presents a clear opportunity for future research as different activities inside the DevOps cycle need to be adapted to the multi cloud context. As identified in Section 4.3 a further, more detailed, classification of resources that allow for a better matching and resource allocation to comply and fulfill the NFRs of the different application components are needed as claimed by the majority of the studies. The heterogeneity of models for the characterization of the different infrastructural elements is one of the key research areas. While several standards like OASIS CAMP [115], OASIS TOSCA [116] or CIMI [117] try to provide stable and common interfaces to describe the topology of such cloud services, the multi-cloud notion has not yet been fully incorporated. In this sense, the description and characterization of the

whole cloud continuum including, at the same time, traditional cloud resources, IoT elements and edge services need to be incorporated into the standards. Furthermore, the incorporation of these new infrastructural elements on the board game opens up the types of NFR to be considered to a new level. Here the definition of the novel NFR related to the network, communications, security (i.e. especially data sharing) or even legal plays a key role that needs to be included to the requirements definition phase.

- Similarly, the **context aware design of multi-cloud applications** is another open topic that still poses several challenges for the research community. NFRs optimization (cost, latency, performance), components synchronization, data consistency and cloud agnostic design of software systems are the challenges identified here [45, 48, 59, 85, 98, 106].
  In this respect, once the NFRs from both sides (multi cloud application components and as a whole and infrastructural element available) are clearly described and classified, they need to be matched in the sense that the best combination of infrastructural elements needs to be selected both for each application component and for the complete application as a whole. In the analyzed studies, techniques such as optimization or benchmarking have been commonly used but they are usually restricted to performance and workload. In the new context of cloud continuum other approaches like lightweight benchmarking and multi-criteria optimization need to be addressed.
- To address the challenges of the operation of multi-cloud native applications, the **federated model** of such heterogenous services is to be proposed to leverage from its benefits [8, 51, 67, 78, 79, 81]. Nevertheless, even if solutions for federation of cloud services are getting to be realized, they need to be expanded to address the whole cloud continuum. The communication layer for instance, and the dependency on the network of these distributed multi-cloud applications is also an aspect that needs to be further considered and investigated in the federated model [77, 96]. New, lightweight elements such as sensors, edge nodes or IoT gateways included in the cloud continuum need to be taken into account in such a federated model. Thus, new models for the characterization of such elements need to be researched. These models should include the description of such elements at different levels of abstraction but also how those elements can be incorporated into the management of business workflows, such as SLA management and accounting [67], and automatically contracting negotiation [78]. More specifically, SLA management and accounting lead to the necessity of the incorporation of new methods and techniques for the monitoring of new elements, more lightweight ones, and networking elements.
- **Re-configuration and self-healing of the multi-cloud native applications** at run-time is also attracting more and more interest in the research community. In this context, the solutions proposed so far are specific for concrete scenarios such as IoT or traditional cloud environments. Other solutions are focused on specific steps of the self-healing, self-configuration process, or in the resolution of specific problems such as scalability, or trust enforcement. However, the cross- and multi-layer as well as the networking aspects are still challenges that have not been addressed in a generic way, covering the whole self-healing process from the discovery to the configuration of the resources, for the network preparation and deployment of all software layers. This process presents further challenges and complexity when addressing not only the portability of the computational components (stateless components) but also the portability of data, or stateful components. One of the enablers for such portability, from the application point of view is based onadoption of container-based technologies, such as Docker. However, containerisation per se does not solve the data portability problem. When porting components between two cloud providers, data need to be moved and kept synchronized (at three different levels—blocks, files, or transactions) while maintaining the integrity and confidentiality of the data, and most container-based solutions do not handle this properly. Manual configuration is still needed, and computation components and those holding the business logic are decoupled from components that hold the data which is stored in a database or other type of storage. Consequently, data portability introduces new requirements added to the already time consuming, error prone and mainly manual activity of porting application components over different infrastructural elements such as: 1) establishing the right networking conditions, so that data can be accessed from the required microservice with the required (network) conditions; 2) handling persistent data storage, during a redeployment; 3) database automatic configuration so that it can be re-deployed without manual intervention, 4) automatic checking of the integrity of the data.

- When talking about multi-cloud, **new security challenges** arise but also new opportunities to protect data and services and to guarantee confidentiality, integrity, and availability. The adoption of multi-cloud applications has significantly facilitated the usage of file storage solutions in users, trying to overcome some of the common security issues in cloud architectures such as loss of availability, loss and corruption of data, loss of privacy, and vendor lock-in [108]. Despite this, specific security issues have been analyzed and proper countermeasures have been presented to propose unified approaches, access control policies and frameworks, to preserve data confidentiality and privacy preserving techniques. However, in order to improve the trust in these cloud services, it is required not only to ensure adequate transparency and security awareness in multi-cloud environments but also to push for the adoption of standard security models, or SLAs to evaluate security-related metrics, and to develop frameworks to provide, or to assess and monitor security with a quantitative approach. As an example, cloud users may have concerns about what CSPs intend to do with their (potentially confidential) data, and therefore technologies that realize the proper countermeasures to address this issue have been proposed [71]. Following the shared-responsibility model of cloud services, customers ofcloud services are responsible for all aspects of their application security and should take the necessary steps to protect their application to address application-level threats in a multi-tenant and hostile internet environment [90]. In addition to technical solutions, regulations, certification frameworks and policies need to be put in place so that consumers of the cloud services are sure that they are consuming secure and trustable resources. Current existing standards in cloud security present a big fragmentation The scope of the security controls differ and also the conformity assessment methods applied [28]. To address this issue the European Commission through ENISA, the European Union Agency for Cybersecurity, is working on a candidate European Cloud Services Scheme (EUCS) [118] which would be compliant with the European cloud certification framework defined under the Cybersecurity Act [119]. The implementation of the measures and requirements derived from such a framework results in new research challenges that will drive the research in the area of Cloud Certification, especially with respect to the following topics: Compositional cloud services certification and composability with IoT and 5G certifications, reuse of evidence, continuous compliance and auditing, and cloud security posture management.
- Many of these aspects, and especially those derived from the heterogeneity of the current cloud services could be improved or even solved to a greater extent with **the application of recognized of cloud standards** and interoperable open APIs. However, existing efforts in cloud standardization are still in their initial stages and we are not expecting to have a mature solution soon, especially taking into consideration the timeframe that standards need to become operational.. Moreover, cloud-vendors themselves are reluctant to unification approaches as they prefer to keep their competitive edge and diversity to attract customers [61, 67]. Open APIs and specifications promoting interoperability and portability in the whole cloud continuum stack is therefore a topic that needs to be considered.

RQ6: Which research gaps and opportunities for the design, development, and operation of the "multi-cloud native"/ "hybrid-cloud native" applications can be deduced? Finally, several opportunities for future research were identified due to the freshness of the concept and its relevance for the software industry. We identified a number of research gaps for each of the 4 themes identified, namely, 1) characterization of multi-cloud and multi-cloud native applications, 2) multi-cloud by design, 3) DevOps for multi-cloud and 4) secure multi-cloud native applications. All these four topics represent opportunities for future research. The research to date has focused mainly on factors such as resource and workload allocation, cloud federation, virtualization, and modelling for the cloud. More concrete opportunities for future research include characterization of the cloud continuum, including federated models for cloud and the incorporation of the network elements and edge services into the paradigm, new approaches for the design and partition of stateful and stateless application components especially with the advent of the edge, lightweight design profiles of software components to be deployed on the edge, context aware design of multi-cloud applications, NFRs optimization (e.g., cost, latency, performance), data consistency and integrity, cloud agnostic design of software systems, re-configuration and self-healing mechanisms for multi-cloud native applications which can be extended to the whole continuum, portability of data and stateful components at runtime, and compositional cloud certification, as well as the combination of cloud, IoT and 5G certification

Conclusions

While cloud computing has been an effective way of acquiring computation and storage as a service for many applications, it may not be suitable to handle the endless data generated by IoT devices and largely support heterogeneous application requirements such as those posed by multi-cloud applications. Some of the limitations of the traditional cloud paradigm specially applies to applications that need to comply with strict real time response and low latency requirements or those giving support

to critical infrastructures. To overcome this situation, new approaches that effectively and efficiently leverage distributed computational and storage infrastructural resources and services are necessary. These approaches must seamlessly combine resources and services at the edge (edge computing), in the core (cloud computing), and along the data path (fog computing). As a result, applications running in such heterogenous environments what we have called "multi cloud native applications" in the context of this article, need to be properly defined, designed, deployed, and operated. The lack of an appropriate understanding of the concept or of a design and operation strategy of such kind of applications risk unpredicted costs, vendor lock in and other unwanted outcomes.

Multi-cloud is used to describe un-like and heterogeneous concepts especially tackled to the infrastructural layer, ranging from the ownership of the elements to the relationship of these elements (i.e. federation) addressing many other relevant concepts. However, the lack of a common understanding of the term is even more relevant when the multi-cloud is referred to the potential of the application to be deployed on a heterogeneous environment with multiple services, resources and layers interplaying with each other. While cloud native applications have been described and characterized in the literature [6, 120, 121], we have not found any work trying to characterize and understand the specificities of "multi-cloud native applications" and more specifically, their particularities with respect to their design, development, and operation. In general, although the topic appears to be promising and the interest by the market has been demonstrated, the research on multi-cloud native applications seems to be still in its infancy, providing a range of new opportunities for researchers.

This study has provided a structured understanding of the body of knowledge of multi-cloud applications, with a list of references relevant to multi-cloud systematically collected and analysed. By using an established SLR method, we have identified, classified, and analysed primary studies related to multi-cloud native applications.

Our critical discussion of the identified research open aspects showed that there is room and need to continue investigating and experimenting on the topic. We identified some promising research directions (see Fig. 15) as well as currently unresolved issues. As demonstrated by our study, it is can be stated that multi cloud native applications can be classified into three main categories,1) those covering replicated applications, 2) those that are fully distributed applications, and 3) a combination of both. Known techniques and approaches such as MDD or microservices based architectures have been applied in the design of multi cloud native applications. However, from the results obtained in our analysis,

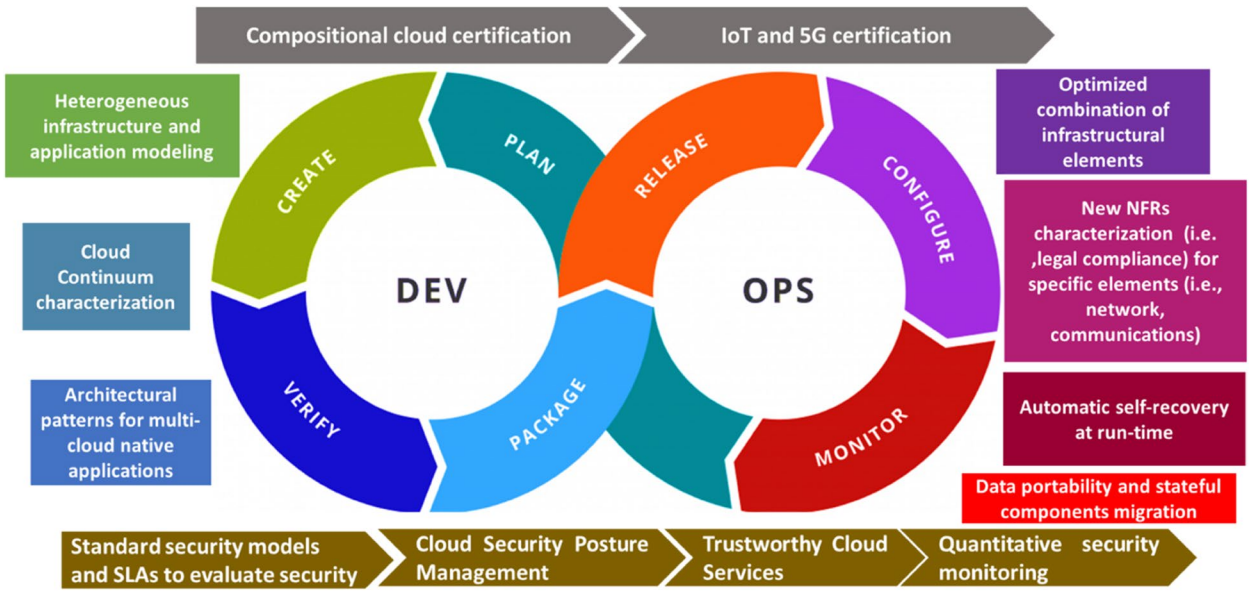

Fig. 15 Overview of the identified research trends in the DevOps lifecycle of multi cloud native applications

there are no specific architectural patterns or proposed design methods specific for multi cloud and its intrinsic heterogeneity, which has proven to be the most important challenge identified by developers and operators of these kind of applications.. One of the envisioned solutions in the mid-term could be the creation and application of cloud standards or in its defect, the publication of open specifications and APIs. Moreover, the enforcement of policies and regulations in addition to the standards could also contribute to increase the interoperability and trustworthiness of cloud services in multi cloud complex environments overcoming important security issues such as wider attack surface, shared responsibility, and conflicting security policies. Nevertheless, existing efforts for cloud standardization are still in their first stages and we are not expecting any mature solution soon.

In regards to development and operation of multi-cloud applications our study has yielded several interesting results. As already mentioned, heterogeneity is reported by DevOps teams as the biggest challenge in multi-cloud applications. In this respect, the lack of specific DevOps practices covering end-to-end the SDLC and SOLC of multi-cloud applications has been highlighted. Selecting and automatically contracting cloud services to realize the deployment of multi-cloud applications, where non-functional requirements of the components of the application and the application as a whole is critical, is another issue that remains unsolved. Here different optimization mechanisms based on artificial intelligence algorithms could be used. The operation of multi-cloud applications still poses several challenges, especially in what regards the automatic configuration, provisioning and management of multiple cloud services with different technologies but also in the dynamic re-adaptation and configuration of the application when a breach in a metric of the SLA has occurred. A dynamic re-adaptation may involve the portability of data and stateful components on-the-fly, which currently cannot be fully achieved due to vendor lock-in, the lack of standards and open interoperability mechanisms. These are issues that still need to be pushed forward in the research agendas, as no mature technical solution is envisioned soon.

From our survey we can conclude that the research up to date has focused mainly on factors such as resource and workload allocation, cloud federating mechanisms, virtualization, and modelling for the cloud in order to address the current shortcomings on multi-cloud and the concept of multi-cloud. Taking this as baseline, we have been able to identify future research areas, being the most relevant ones the following, 1) characterization of the cloud continuum, including federated models for the cloud 2) incorporation of the network elements into the multi cloud paradigm, 3) proposal of new approaches for design and partition of stateful and stateless application components 4) lightweight design profiles for software components to be deployed on the edge, 5) context aware design and architecture of multi-cloud applications architecture that can therefore be extended to the edge, 6) NFRs optimization (cost, latency, performance), 7) components synchronization, data consistency and cloud agnostic design of software systems,8) re-configuration and self-healing mechanisms for multi-cloud native applications as well as 9) compositional cloud certification, and 10) the combination of cloud, IoT and 5G certifications and 11) security mechanisms to achieve trustable cloud services, application and enforcement of policies, and approaches for security monitoring, among others.

We believe our work contributes to a more precise understanding of the term and concept of multi cloud from the application design, deployment, and operation perspective. Especially, researcher and practitioners can use the findings we have made to establish the baselines for further research and adapt and apply DevOps philosophy for complex multi cloud environments.

Our future research work derived from this study is as follows:

- To extend the study analysing the multi-cloud approach in a broader sense, as the multi-cloud concept is under continuous evolution. Edge services, fog computing and the cloud continuum can also be considered and incorporated to the analysis of the multi-cloud term so that the study accommodates the continuum computing also in the selected works.
- To conduct a questionnaire survey for the validation of the SLR findings, focusing specially on practitioners also covering the industrial sector perspective.
- To further detail the discovered challenges for the development and operation of multi-cloud applications and prioritize them following a multi-dimension and multi-criteria methodology with the objective of deriving specific recommendations for researchers, practitioners and policy makers in the relevant topics.

Appendix

Table 11.

Table 11 Format of the form for extracting the data for the analysis of the primary studies

Form data	Explanation	Values
Generic information	Generic information about each of the primary studies	Not applicable
Responsible researcher	Name of the expert analysing the primary study.	Juncal Alonso, Valentina Casola, Leire Orue-Echevarria, Ana Isabel Torre
Accepted/rejected	Inclusion or rejection decision.	Accepted/Rejected
Paper Id	Paper Id	1–114
Paper Title	Full title of the primary study	NA
Abstract	Abstract of the primary study	NA
Key words	Key words defined by the primary study	NA
Abstract	Abstract from the primary study	NA
Author	Author/Authors	NA
Year	Year of publication of the primary study	2006–2020
Doi	Digital Object Identifier of the primary study	NA
Comments	Any relevant comment made by the expert about the primary study	NA
Source link	Link to the primary study	NA
Number of citations	Number of citations of the primary study	1–500
Length	Length (number of pages)	1–50
Venue Type	Type of the venue where the primary study was published	Conference, Journal, Book
Venue	Name of the venue where the primary study was published	NA
Research Type	Type of the research corresponding to the primary study	Evaluation research, Experience paper, Opinion paper, Philosophical paper, Solution proposal, Validation research
Case Study	Type of the case study where the primary study was validated	Academic case study (e.g. with students), Action research, Controlled experiment with practitioners, Industrial Case study, Laboratory experiments (machine or human), Mathematical analysis and proof of properties, Practitioner targeted survey Prototyping Simulation as an empirical method
Information for RQ1/RQ2		
RQ1/RQ2: Meaning of the term multi-cloud generic	Definition of the term multi-cloud (if any) in the primary study	NA
RQ1/RQ2: Meaning of the term multi-cloud native application	Definition of the term multi-cloud native application (if any) in the primary study	NA
Information for RQ3		
RQ3: multi-cloud by design: architectural patterns	Multi-cloud architectural patterns identified in the primary study	NA
RQ3:multi-cloud by design: technologies	Technologies related to multi-cloud cited by the primary study	NA
RQ3:multi-cloud by design: standards	Standards related to multi-cloud cited by the primary study	NA
RQ3:multi-cloud by design: process	Processes followed/identified by the primary study for the design of multi-cloud applications	NA
Information for RQ5		
RQ5: Main security threats and countermeasures in multi-cloud native applications	Security threats and countermeasures identified by the primary study affecting in multi-cloud native applications	NA
Information for RQ6		
RQ6: Future trends in multi-cloud /hybrid cloud	Future research trends related to the design and operation of multi cloud native applications identified in the primary study	NA
Information for RQ4		
RQ4: multi-cloud challenges: design	Design challenges cited in the primary study for multi-cloud native applications	NA
RQ4: multi-cloud challenges: development & execution	Development and execution challenges cited in the primary study for multi-cloud native applications	NA
RQ4: multi-cloud challenges: operation	Operation challenges cited in the primary study for multi-cloud native applications	NA
multi-cloud benefits general	Benefits of multi-cloud native applications identified by the primary study	NA
multi-cloud drawbacks: general	Drawbacks of multi-cloud native applications identified by the primary study	NA

Abbreviations

ACM	Association for Computing Machinery
API	Application Programming Interface
AWS	Amazon Web Services
CAMEL	The Cloud Application Modelling and Execution Language
CAMP	Cloud Application Management for Platforms
CB	Cloud Broker
CDMI	Cloud Data Management Interface
CIMI	Cloud Infrastructure Management Interface
CNA	Cloud Native Application
CNCF	Cloud Native Computing Foundation
CP	Cloud Provider
CSA STAR	Cloud Security Alliance for Security, Trust and Assurance Registry
CSLA	Cloud Service Level Agreement
CSP	Cloud Service Provider
DOI	Digital Object Identifier
DSL	Domain Specific Languages
ENISA	European Union Agency for Cybersecurity
EUCS	European Cloud Services Scheme
FaaS	Functions-as-a-Service
IaaS	Infrastructure as a Service
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISO	International Organization for Standardization
MDD	Model Driven Development
MDE	model Driven Engineering
MOM	Message Oriented Middleware
NFR	Non-Functional Requirements
NIST	National Institute of Standards and Technology
OCCI	Open Cloud Computing Interface
PaaS	Platform as a Service
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
QoS	Quality of Service
REST	REpresentational State Transfer
ROI	Return Of Investment
RQ	Research Question
SaaS	Software as a Service
SAML/2	Security Assertion Markup Language 2.0
SDLC	Software Development Lifecycle
SLA	Service Level Agreement
SLR	Systematic Literature Review
SM	Systematic Mapping
SOLC	Software Operation Lifecycle
TOSCA	Topology and Orchestration Specification for Cloud Applications
UML	Unified Modelling Language

Acknowledgements
We thank the Cloud expert Ana Juan Ferrer for her valuable advice and suggestions to improve the manuscript.

Authors' contributions
This research work is a part of JA's Ph.D. work, which is being conducted under the supervision of MH. The paper presents extensive review of the multi-cloud concept from the application's perspective and provides directions for future work and research challenges to be addressed by the software community. The work presented in this paper was carried out during July 2021–January 2022. JA, LO, VC, AT and MH contributed to the design and implementation of the research and to the analysis of the results. JA, LO, and VC wrote the manuscript in consultation with EO and JL. The authors read and approved the final manuscript.

Funding
This work has been partially funded by the European projects DECIDE (Horizon 2020 research and innovation programme, under grant agreement 731533), PIACERE (Horizon 2020 research and innovation Programme, under grant agreement no 101000162), MEDINA (Horizon 2020 research and innovation Programme, under grant agreement no 952633), from the University of Naples Federico II (Finanziamento delle Ricerca di Ateneo 2020) and SwForum.eu (Horizon 2020 research and innovation Programme, under grant agreement no 957044).

Availability of data and materials
Data is available upon request to the corresponding author.

Declarations

Competing interests
On behalf of all authors, the corresponding author states that they have no financial or non-financial competing interests in the realization of this research.

Received: 31 January 2022 Accepted: 12 November 2022
Published online: 12 January 2023

References

1. Bouakouk MR, Abdelli A, Mokdad L (2020) Survey on the cloud-IoT paradigms: taxonomy and architectures. In: 2020 IEEE symposium on computers and communications (ISCC). IEEE, Rennes, pp 1–6
2. Atieh AT (2021) The next generation cloud technologies: a review on distributed cloud, fog and edge computing and their opportunities and challenges. Res Berg Rev Sci Technol 1:1–15
3. Mazzucca J Survey analysis: cloud adoption across vertical industries exhibits more similarities than differences. Gartner https://www.gartner.com/en/documents/2987617/survey-analysis-cloud-adoption-across-vertical-industrie. Accessed 28 Dec 2021
4. Cloud Native Computing Foundation Cloud Native Survey 2020. https://www.cncf.io/reports/#cloud-native-surveys. Accessed 5 Apr 2021
5. How leading industries are driving multi-cloud adoption | ITProPortal. https://www.itproportal.com/features/how-leading-industries-are-driving-multi-cloud-adoption/. Accessed 1 Jan 2022
6. Kratzke N, Quint P-C (2017) Understanding cloud-native applications after 10 years of cloud computing - a systematic mapping study. J Syst Softw 126:1–16. https://doi.org/10.1016/j.jss.2017.01.001
7. Priyadarsini K, Raj EFI, Begum AY, Shanmugasundaram V (2020) Comparing DevOps procedures from the context of a systems engineer. Mater Today: Proc S2214785320373491. https://doi.org/10.1016/j.matpr.2020.09.624
8. Alonso J, Stefanidis K, Orue-Echevarria L, Blasi L, Walker M, Escalante M, López MJ, Dutkowski S (2019) DECIDE: an extended DevOps framework for multi-cloud applications (PS33). In: Proceedings of the 2019 3rd international conference on cloud and big data computing. ACM, Oxford, pp 43–48
9. Asthana S, Megahed A, Iyoob I (2021) Multi-cloud solution Design for Migrating a portfolio of applications to the cloud. In: Hacid H, Outay F, Paik H, Alloum A, Petrocchi M, Bouadjenek MR, Beheshti A, Liu X, Maaradji A (eds) Service-oriented computing – ICSOC 2020 workshops. Springer International Publishing, Cham, pp 485–494
10. Vijayalakshmi A, Hridya (2022) Functionalities and approaches of multi-cloud environment. In: Nagarajan R, Raj P, Thirunavukarasu R (eds) Operationalizing multi-cloud environments. Springer International Publishing, Cham, pp 257–268
11. Rak M (2017) Security assurance of (multi-)cloud application with security SLA composition. In: Au MHA, Castiglione A, Choo K-KR, Palmieri F, Li K-C (eds) Green, pervasive, and cloud computing. Springer International Publishing, Cham, pp 786–799
12. Liberati A, Altman DG, Tetzlaff J, Mulrow C, Gøtzsche PC, Ioannidis JPA, Clarke M, Devereaux PJ, Kleijnen J, Moher D (2009) The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. J Clin Epidemiol 62:e1–e34. https://doi.org/10.1016/j.jclinepi.2009.06.006
13. El-Gazzar RF (2014) A literature review on cloud computing adoption issues in enterprises. In: Bergvall-Kåreborn B, Nielsen PA (eds) Creating value for all through IT. Springer, Berlin Heidelberg, pp 214–242
14. Ward JS, Barker A (2014) Observing the clouds: a survey and taxonomy of cloud monitoring. JoCCASA 3:24. https://doi.org/10.1186/s13677-014-0024-2

15. Chiregi M, Jafari Navimipour N (2018) Cloud computing and trust evaluation: a systematic literature review of the state-of-the-art mechanisms. J Electr Syst Inform Technol 5:608–622. https://doi.org/10.1016/j.jesit.2017.09.001
16. Sheikh A, Munro M, Budgen D (2019) Systematic literature review (SLR) of resource scheduling and security in cloud computing. IJACSA 10. https://doi.org/10.14569/IJACSA.2019.0100404
17. Petcu D (2013) Multi-cloud: expectations and current approaches (PS58). In: Proceedings of the 2013 international workshop on multi-cloud applications and federated clouds - MultiCloud '13. ACM Press, Prague, p 1
18. Liaqat M, Chang V, Gani A, Hamid SHA, Toseef M, Shoaib U, Ali RL (2017) Federated cloud resource management: review and discussion. J Netw Comput Appl 77:87–105. https://doi.org/10.1016/j.jnca.2016.10.008
19. Tomarchio O, Calcaterra D, Modica GD (2020) Cloud resource orchestration in the multi-cloud landscape: a systematic review of existing frameworks. JoCCASA 9:49. https://doi.org/10.1186/s13677-020-00194-7
20. Lahmar F, Mezni H (2018) Multicloud service composition: a survey of current approaches and issues. J Softw Evol Proc 30:e1947. https://doi.org/10.1002/smr.1947
21. Vakili A, Navimipour NJ (2017) Comprehensive and systematic review of the service composition mechanisms in the cloud environments. J Netw Comput Appl 81:24–36. https://doi.org/10.1016/j.jnca.2017.01.005
22. Niknejad N, Ismail W, Ghani I, Nazari B, Bahari M, Hussin ARBC (2020) Understanding service-oriented architecture (SOA): a systematic literature review and directions for further investigation. Inform Syst 91:101491. https://doi.org/10.1016/j.is.2020.101491
23. Hamzehloui MS, Sahibuddin S, Salah K (2019) A systematic mapping study on microservices. In: Saeed F, Gazem N, Mohammed F, Busalim A (eds) Recent trends in data science and soft computing. Springer International Publishing, Cham, pp 1079–1090
24. Soldani J, Tamburri DA, Van Den Heuvel W-J (2018) The pains and gains of microservices: a systematic grey literature review. J Syst Softw 146:215–232. https://doi.org/10.1016/j.jss.2018.09.082
25. Chacón-Luna AE, Gutiérrez AM, Galindo JA, Benavides D (2020) Empirical software product line engineering: a systematic literature review. Inform Softw Technol 128:106389. https://doi.org/10.1016/j.infsof.2020.106389
26. Di Martino B, Esposito A (2016) Semantic techniques for multi-cloud applications portability and interoperability (PS64). Proc Comput Sci 97:104–113. https://doi.org/10.1016/j.procs.2016.08.285
27. Kitchenham B Guidelines for performing Systematic Literature Reviews in Software Engineering. 44
28. Orue-Echevarria L, Garcia JL, Banse C, Alonso J (2021) Medina: improving cloud services trustworthiness through continuous audit-based certification CEUR Workshop Proceedings
29. Siriweera A, Naruse K (2021) Survey on cloud robotics architecture and model-driven reference architecture for decentralized multicloud heterogeneous-robotics platform (PS83). IEEE Access 9:40521–40539. https://doi.org/10.1109/ACCESS.2021.3064192
30. Kritikos K, Plexousakis D (2015) Multi-cloud application design through cloud service composition (PS21). In: 2015 IEEE 8th international conference on cloud computing. IEEE, New York, pp 686–693
31. Soltani B, Ghenai A, Zeghib N (2018) Towards distributed containerized Serverless architecture in multi cloud environment (PS54). Proc Comput Sci 134:121–128. https://doi.org/10.1016/j.procs.2018.07.152
32. Varghese B, Buyya R (2018) Next generation cloud computing: new trends and research directions (PS60). Fut Gener Comput Syst 79:849–861. https://doi.org/10.1016/j.future.2017.09.020
33. Gao M, Chen M, Liu A, Ip WH, Yung KL (2020) Optimization of microservice composition based on artificial immune algorithm considering fuzziness and user preference (PS79). IEEE Access 8:26385–26404. https://doi.org/10.1109/ACCESS.2020.2971379
34. Miglierina M, Gibilisco GP, Ardagna D, Nitto ED (2013) Model based control for multi-cloud applications (PS36). In: 2013 5th international workshop on modeling in software engineering (MiSE), pp 37–43
35. Ren Y, Leng Y, Qi J, Sharma PK, Wang J, Almakhadmeh Z, Tolba A (2021) Multiple cloud storage mechanism based on blockchain in smart homes (PS86). Fut Gener Comput Syst 115:304–313. https://doi.org/10.1016/j.future.2020.09.019
36. Pérez J, Díaz J, Garcia-Martin J, Tabuenca B (2020) Systematic literature reviews in software engineering—enhancement of the study selection process using Cohen's kappa statistic. J Syst Softw 168:110657. https://doi.org/10.1016/j.jss.2020.110657
37. Petersen K, Vakkalanka S, Kuzniarz L (2015) Guidelines for conducting systematic mapping studies in software engineering: an update. Inform Softw Technol 64:1–18. https://doi.org/10.1016/j.infsof.2015.03.007
38. Kitchenham BA, Budgen D, Brereton OP (2010) The value of mapping studies – a participant-observer case study
39. Assis MRM, Bittencourt LF (2020) MultiCloud tournament: a cloud federation approach to prevent free-riders by encouraging resource sharing (PS31). J Netw Comput Appl 166:102694. https://doi.org/10.1016/j.jnca.2020.102694
40. Brogi A, Carrasco J, Cubo J, D'Andria F, Di Nitto E, Guerriero M, Pérez D, Pimentel E, Soldani J (2016) SeaClouds: an open reference architecture for multi-cloud governance (PS56)
41. Mell PM, Grance T (2011) The NIST definition of cloud computing. National Institute of Standards and Technology, Gaithersburg
42. Felderer M, Travassos GH (2020) Contemporary empirical methods in software engineering. Springer Nature
43. Tacconelli E (2010) Systematic reviews: CRD's guidance for undertaking reviews in health care. Lancet Infect Dis 10:226. https://doi.org/10.1016/S1473-3099(10)70065-7
44. Baby K, Vysala A (2015) Multicloud architecture for augmenting security in clouds (PS48). In: 2015 global conference on communication technologies (GCCT). IEEE, Thuckalay, pp 474–478
45. Ferrer AJ, Pérez DG, González RS (2016) Multi-cloud platform-as-a-service model, functionalities and approaches (PS18). Proc Comput Sci 97:63–72. https://doi.org/10.1016/j.procs.2016.08.281
46. Guillén J, Miranda J, Murillo JM, Canal C (2013) Developing migratable multicloud applications based on MDE and adaptation techniques (PS35). In: Proceedings of the second Nordic symposium on Cloud Computing & Internet Technologies - NordiCloud '13. ACM Press, Oslo, pp 30–37
47. Komu M, Sethi M, Mallavarapu R, Oirola H, Khan R, Tarkoma S (2012) Secure networking for virtual Machines in the Cloud (PS45). In: 2012 IEEE international conference on cluster computing workshops. IEEE, Beijing, pp 88–96
48. Nitto ED, da Silva MAA, Ardagna D, Casale G, Craciun CD, Ferry N, Muntes V, Solberg A (2013) Supporting the development and operation of multi-cloud applications: the MODAClouds approach (PS16). In: 2013 15th international symposium on symbolic and numeric algorithms for scientific computing. IEEE, Timisoara, pp 417–423
49. Perera S, Kumarasiri R, Kamburugamuva S, Fernando S, Weerawarana S, Fremantle P (2012) Cloud services gateway: a tool for exposing private services to the public cloud with fine-grained control (PS4). In: 2012 IEEE 26th international parallel and distributed processing symposium workshops PhD forum, pp 2237–2246
50. Raj P, Raman A (2018) The hybrid cloud: the journey toward hybrid IT (PS1). In: Raj P, Raman A (eds) Software-defined cloud centers: operational and management technologies and tools. Springer International Publishing, Cham, pp 91–110
51. Tricomi G, Panarello A, Merlino G, Longo F, Bruneo D, Puliafito A (2017) Orchestrated multi-cloud application deployment in OpenStack with TOSCA (PS22). In: 2017 IEEE international conference on smart computing (SMARTCOMP), pp 1–6
52. Vijayanand KS, Mala T (2014) A framework for preserving data security in hybrid cloud environment using trusted multiple cloud service providers (PS41). In: 2014 sixth international conference on advanced computing (ICoAC). IEEE, Chennai, pp 14–18
53. Csorba MJ, Meling H, Heegaard PE (2011) A bio-inspired method for distributed deployment of services (PS13). New Gen Comput 29:185–222. https://doi.org/10.1007/s00354-010-0104-x
54. Ferry N, Chauvel F, Rossini A, Morin B, Solberg A (2013) Managing multi-cloud systems with CloudMF (PS12). In: Proceedings of the second Nordic symposium on Cloud Computing & Internet Technologies - NordiCloud '13. ACM Press, Oslo, pp 38–45
55. Kallergis D, Garofalaki Z, Katsikogiannis G, Douligeris C (2020) CAPO-DAZ: a containerised authorisation and policy-driven architecture using microservices (PS20). Ad Hoc Networks 104:102153. https://doi.org/10.1016/j.adhoc.2020.102153

56. Mulfari D, Fazio M, Celesti A, Villari M, Puliafito A (2016) Design of an IoT cloud system for container virtualization on smart objects (PS7). In: Celesti A, Leitner P (eds) Advances in service-oriented and cloud computing. Springer International Publishing, Cham, pp 33–47
57. Casola V, De Benedictis A, Rak M, Villano U (2018) Security-by-design in multi-cloud applications: an optimization approach (PS51). Inform Sci 454–455:344–362. https://doi.org/10.1016/j.ins.2018.04.081
58. Chituc C-M (2015) Towards a methodology for trade-off analysis in a multi-cloud environment considering monitored QoS metrics and economic performance assessment results (PS77). In: 2015 IEEE 7th international conference on cloud computing technology and science (CloudCom). IEEE, Vancouver, pp 479–482
59. Ciavotta M, Ardagna D, Gibilisco GP (2017) A mixed integer linear programming optimization approach for multi-cloud capacity allocation (PS74). J Syst Softw 123:64–78. https://doi.org/10.1016/j.jss.2016.10.001
60. Demchenko Y, Turkmen F, Slawik M, Laat C d (2017) Defining Intercloud security framework and architecture components for multi-cloud data intensive applications (PS59). In: 2017 17th IEEE/ACM international symposium on cluster, cloud and grid computing (CCGRID). IEEE, Madrid, pp 945–952
61. Elgedawy I (2015) SULTAN: a composite data consistency approach for SaaS multi-cloud deployment (PS10). In: 2015 IEEE/ACM 8th international conference on utility and cloud computing (UCC), pp 122–131
62. Huang J, Sharaf M, Huang C-T (2012) A hierarchical framework for secure and scalable EHR sharing and access control in multi-cloud (PS25). In: 2012 41st international conference on parallel processing workshops. IEEE, Pittsburgh, pp 279–287
63. Jakóbczyk MT (2020) Cloud-native architecture (PS62). In: Practical Oracle cloud infrastructure. Apress, Berkeley, pp 487–551
64. Kritikos K, Skrzypek P (2019) Are cloud Modelling languages ready for multi-cloud? (PS66). In: Proceedings of the 12th IEEE/ACM international conference on utility and cloud computing companion - UCC '19 companion. ACM Press, Auckland, pp 51–58
65. Kumar SNV, Meenakshi R (2017) Securing multi-cloud by auditing (PS42). In: 2017 third international conference on sensing, signal processing and security (ICSSS). IEEE, Chennai, pp 253–258
66. Leite AF, Alves V, Rodrigues GN, Tadonki C, Eisenbeis C, Melo ACMA d (2017) Dohko: an autonomic system for provision, configuration, and management of inter-cloud environments based on a software product line engineering method (PS68). Cluster Computing 20:1951–1976. https://doi.org/10.1007/s10586-017-0897-1
67. Oprescu A, Antonescu A, Demchenko Y, Laat C (2013) ICOMF: towards a multi-cloud ecosystem for dynamic resource composition and scaling (PS15). In: 2013 IEEE 5th international conference on cloud computing technology and science, pp 49–55
68. Razaque A, Nadimpalli SSV, Vommina S, Atukuri DK, Reddy DN, Anne P, Vegi D, Malllapu VS (2016) Secure data sharing in multi-clouds (PS80). In: 2016 international conference on electrical, electronics, and optimization techniques (ICEEOT). IEEE, Chennai, pp 1909–1913
69. Somoskői B, Spahr S, Rios E, Ripolles O, Dominiak J, Cserveny T, Bálint P, Matthews P, Iturbe E, Muntés-Mulero V (2019) Airline application security in the digital economy: tackling security challenges for distributed applications in Lufthansa systems (PS46). In: Urbach N, Röglinger M (eds) Digitalization cases. Springer International Publishing, Cham, pp 35–58
70. Sukmana MIH, Torkura KA, Graupner H, Cheng F, Meinel C (2019) Unified cloud access control model for cloud storage broker (PS23). In: 2019 international conference on information networking (ICOIN). IEEE, Kuala Lumpur, pp 60–65
71. Yang L, Humayed A, Li F (2016) A multi-cloud based privacy-preserving data publishing scheme for the internet of things (PS63). In: Proceedings of the 32nd annual conference on computer security applications. ACM, Los Angeles, pp 30–39
72. Yasrab R, Gu N (2016) Multi-cloud PaaS architecture (MCPA): a solution to cloud lock-in (PS32). In: 2016 3rd international conference on information science and control engineering (ICISCE). IEEE, Beijing, pp 473–477
73. Zhou S, Chen G, Huang G, Shi J, Kong T (2020) Research on multi-authority CP-ABE access control model in multicloud (PS44). China Commun 17:220–233. https://doi.org/10.23919/JCC.2020.08.018
74. Buzachis A, Fazio M, Celesti A, Villari M (2019) Osmotic flow deployment leveraging FaaS capabilities (PS69). In: Montella R, Ciaramella A, Fortino G, Guerrieri A, Liotta A (eds) Internet and distributed computing systems. Springer International Publishing, Cham, pp 391–401
75. Ferrer AJ, Hernández F, Tordsson J, Elmroth E, Ali-Eldin A, Zsigri C, Sirvent R, Guitart J, Badia RM, Djemame K, Ziegler W, Dimitrakos T, Nair SK, Kousiouris G, Konstanteli K, Varvarigou T, Hudzia B, Kipp A, Wesner S, Corrales M, Forgó N, Sharif T, Sheridan C (2012) OPTIMIS: a holistic approach to cloud service provisioning (PS30). Futur Gen Comput Syst 28:66–77. https://doi.org/10.1016/j.future.2011.05.022
76. Petcu D (2014) Consuming resources and services from multiple clouds: from terminology to Cloudware support (PS82). J Grid Computing 12:321–345. https://doi.org/10.1007/s10723-013-9290-3
77. Jofre J, Velayos C, Landi G, Giertych M, Hume AC, Francis G, Vico Oton A (2014) Federation of the BonFIRE multi-cloud infrastructure with networking facilities (PS38). Comput Netw 61:184–196. https://doi.org/10.1016/j.bjp.2013.11.012
78. Li Q, Wang Z, Li W, Cao Z, Du R, Luo H (2013) Model-based services convergence and multi-clouds integration (PS39). Comput Indust 64:813–832. https://doi.org/10.1016/j.compind.2013.05.003
79. Patel R, Dahiya D (2015) Aggregation of cloud providers: a review of opportunities and challenges (PS43). In: International conference on computing. Communication & Automation. IEEE, Greater Noida, pp 620–626
80. Rios E, Mallouli W, Rak M, Casola V, Ortiz AM (2016) SLA-driven monitoring of multi-cloud application components using the MUSA framework (PS40). In: 2016 IEEE 36th international conference on distributed computing systems workshops (ICDCSW). IEEE, Nara, pp 55–60
81. Xhagjika V, Navarro L, Vlassov V (2015) Enhancing real-time applications by means of multi-tier cloud federations (PS53). In: 2015 IEEE 7th international conference on cloud computing technology and science (CloudCom). IEEE, Vancouver, pp 397–404
82. Wahab OA, Bentahar J, Otrok H, Mourad A (2018) Towards trustworthy multi-cloud services communities: a trust-based hedonic coalitional game (PS52). IEEE Transact Services Comput 11:184–201. https://doi.org/10.1109/TSC.2016.2549019
83. Chondamrongkul N, Temdee P (2013) Multi-cloud computing platform support with model-driven application runtime framework (PS14). In: 2013 13th international symposium on communications and information technologies (ISCIT). IEEE, Surat Thani, pp 715–719
84. Casale G, Artač M, van den Heuvel W-J, van Hoorn A, Jakovits P, Leymann F, Long M, Papanikolaou V, Presenza D, Russo A, Srirama SN, Tamburri DA, Wurster M, Zhu L (2020) RADON: rational decomposition and orchestration for serverless computing (PS67). SICS Softw-Inensiv Cyber-Phys Syst 35:77–87. https://doi.org/10.1007/s00450-019-00413-w
85. Ferry N, Chauvel F, Song H, Rossini A, Lushpenko M, Solberg A (2018) CloudMF: model-driven Management of Multi-Cloud Applications (PS11). ACM Transact Inter Technol 18:1–24. https://doi.org/10.1145/3125621
86. He B, Wang J, Zhou J, Li L, Zhou W, Zhu L, Zhai M (2019) The design and implementation of multi-cloud based distributed storage platform with random linear coding (PS76). In: 2019 IEEE 21st international conference on high performance computing and communications; IEEE 17th international conference on Smart City; IEEE 5th international conference on data science and systems (HPCC/SmartCity/DSS). IEEE, Zhangjiajie, pp 1233–1240
87. Kritikos K, Kirkham T, Kryza B, Massonet P (2017) Towards a security-enhanced PaaS platform for multi-cloud applications (PS50). Fut Gener Comput Syst 67:206–226. https://doi.org/10.1016/j.future.2016.10.008
88. Kritikos K, Kirkham T, Kryza B, Massonet P (2018) Reprint of "towards a security-enhanced PaaS platform for multi-cloud applications" (PS73). Future Gener Comput Syst 78:155–175. https://doi.org/10.1016/j.future.2016.11.014
89. Quinton C, Haderer N, Rouvoy R, Duchien L (2013) Towards multi-cloud configurations using feature models and ontologies (PS47). In: Proceedings of the 2013 international workshop on multi-cloud applications and federated clouds - MultiCloud '13. ACM Press, Prague, p 21
90. Movahedisefat MR, Reza Farshchi SM, Mohammadpur D (2014) Emerging security challenges in cloud computing, from infrastructure-based security to proposed provisioned cloud infrastructure (PS9). In: Emerging trends in ICT security. Elsevier, pp 379–393
91. Casola V, De Benedictis A, Rak M, Rios E (2016) Security-by-design in clouds: a security-SLA driven methodology to build secure cloud applications (PS19). Proc Comput Sci 97:53–62. https://doi.org/10.1016/j.procs.2016.08.280

92. Kritikos K, Kirkham T, Kryza B, Massonet P (2015) Security enforcement for multi-cloud platforms – the case of PaaSage (PS72). Proc Comput Sci 68:103–115. https://doi.org/10.1016/j.procs.2015.09.227
93. Wei H, Rodriguez JS, Garcia ON-T (2021) Deployment management and topology discovery of microservice applications in the multicloud environment (PS88). J Grid Computing 19:1. https://doi.org/10.1007/s10723-021-09539-1
94. Zou C, Deng H, Qiu Q (2013) Design and implementation of hybrid cloud computing architecture based on cloud bus (PS70). In: 2013 IEEE 9th international conference on Mobile ad-hoc and sensor networks. IEEE, Dalian, pp 289–293
95. Shyamasundar RK, Kumar NVN, Rajarajan M (2016) Information-flow control for building security and privacy preserving hybrid clouds (PS81). In: 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on Smart City; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS). IEEE, Sydney, pp 1410–1417
96. Celesti A, Fazio M, Galletta A, Carnevale L, Wan J, Villari M (2019) An approach for the secure management of hybrid cloud–edge environments (PS8). Futur Gener Comput Syst 90:1–19. https://doi.org/10.1016/j.future.2018.06.043
97. da Silva MAA, Ardagna D, Ferry N, Perez JF (2014) Model-driven Design of Cloud Applications with quality-of-service guarantees: the MODAClouds approach, MICAS tutorial (PS37). In: 2014 16th international symposium on symbolic and numeric algorithms for scientific computing. IEEE, Romania, pp 3–10
98. Heilig L, Lalla-Ruiz E, Voß S (2020) Modeling and solving cloud service purchasing in multi-cloud environments (PS49). Expert Syst Appl 147:113165. https://doi.org/10.1016/j.eswa.2019.113165
99. Capitani D, di Vimercati S, Foresti S, Livraga G, Piuri V, Samarati P (2021) Security-aware data allocation in multicloud scenarios (PS84). IEEE Transact Depend Secure Comput 1–1. https://doi.org/10.1109/TDSC.2019.2953068
100. Wang L, Ramasamy HV, Karve A, Harper RE (2017) Providing resiliency to orchestration and automation Engines in Hybrid Cloud (PS78). In: 2017 47th annual IEEE/IFIP international conference on dependable systems and networks workshops (DSN-W). IEEE, Denver, pp 125–128
101. Hybrid Cloud Placement Algorithm (PS17). In: IEEE Conference Publication
102. Georgios C, Evangelia F, Christos M, Maria N (2021) Exploring cost-efficient bundling in a multi-cloud environment (PS85). Simul Modell Pract Theory 111:102338. https://doi.org/10.1016/j.simpat.2021.102338
103. Kaviani N, Wohlstadter E, Lea R (2012) MANTICORE: a framework for partitioning software services for hybrid cloud (PS5). In: 4th IEEE international conference on cloud computing technology and science proceedings. IEEE, Taipei, pp 333–340
104. Woo SS, Mirkovic J (2014) Optimal application allocation on multiple public clouds (PS28). Comput Netw 68:138–148. https://doi.org/10.1016/j.comnet.2013.12.001
105. Jamshidi P, Pahl C, Chinenyeze S, Liu X (2015) Cloud migration patterns: a multi-cloud service architecture perspective (PS27). In: Toumani F, Pernici B, Grigori D, Benslimane D, Mendling J, Ben Hadj-Alouane N, Blake B, Perrin O, Saleh Moustafa I, Bhiri S (eds) Service-oriented computing - ICSOC 2014 workshops. Springer International Publishing, Cham, pp 6–19
106. Almeida A, Dantas F, Cavalcante E, Batista T (2014) A branch-and-bound algorithm for autonomic adaptation of multi-cloud applications (PS6). In: 2014 14th IEEE/ACM international symposium on cluster, cloud and grid computing, pp 315–323
107. Alshammari MM, Alwan AA, Nordin A, Al-Shaikhli IF (2017) Disaster recovery in single-cloud and multi-cloud environments: issues and challenges (PS75). In: 2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS). IEEE, Salmabad, pp 1–7
108. Agarwal V, Kaushal AK, Chouhan L (2020) A survey on cloud computing security issues and cryptographic techniques (PS3). In: Shukla RK, Agrawal J, Sharma S, Chaudhari NS, Shukla KK (eds) Social networking and computational intelligence. Springer Singapore, Singapore, pp 119–134
109. Bhardwaj A, Mangat V, Vig R, Halder S, Conti M (2021) Distributed denial of service attacks in cloud: state-of-the-art of scientific and commercial solutions (PS87). Comput Sci Rev 39:100332. https://doi.org/10.1016/j.cosrev.2020.100332
110. Galletta A, Celesti A, Tusa F, Fazio M, Bramanti P, Villari M (2017) Big MRI data dissemination and retrieval in a multi-cloud hospital storage system (PS34). In: Proceedings of the 2017 international conference on digital health. ACM, London, pp 162–166
111. Wang L, Yang Z, Song X (2020) SHAMC: a secure and highly available database system in multi-cloud environment (PS57). Fut Gener Comput Syst 105:873–883. https://doi.org/10.1016/j.future.2017.07.011
112. Preserving Data Confidentiality Using Multi-cloud Architecture (PS2). https://www.sciencedirect.com/science/article/pii/S1877050915005360. Accessed 28 Feb 2021
113. Afolaranmi SO, Ferrer BR, Martinez Lastra JL (2018) A framework for evaluating security in multi-cloud environments (PS26). In: IECON 2018 - 44th annual conference of the IEEE industrial electronics society. IEEE, Washington, DC, pp 3059–3066
114. Javadi B, Abawajy J, Buyya R (2012) Failure-aware resource provisioning for hybrid cloud infrastructure (PS71). J Parallel Distrib Comput 72:1318–1331. https://doi.org/10.1016/j.jpdc.2012.06.012
115. OASIS OASIS Cloud Application Management for Platforms (CAMP). https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=camp
116. OASIS OASIS topology and orchestration specification for cloud applications (TOSCA). In: OASIS topology and orchestration specification for cloud applications (TOSCA) https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca
117. Distributed Management Task Force, Inc. (DMTF) (2012) Cloud infrastructure management Interface (CIMI) model and RESTful HTTP-based protocol
118. EUCS – cloud services scheme. In: ENISA https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme. Accessed 26 Sep 2022
119. EUR-Lex-32019R0881-EN-EUR-Lex. https://eur-lex.europa.eu/eli/reg/2019/881/oj. Accessed 26 Sep 2022
120. Balalaie A, Heydarnoori A, Jamshidi P (2016) Migrating to cloud-native architectures using microservices: an experience report. In: Celesti A, Leitner P (eds) Advances in service-oriented and cloud computing. Springer International Publishing, Cham, pp 201–215
121. Fehling C, Leymann F, Retter R, Schupeck W, Arbitter P (2014) Cloud application architecture patterns. In: Cloud computing patterns: fundamentals to design, build, and manage cloud applications. Springer Vienna, Vienna, pp 151–238

Publisher's Note