Computer Science Review 56 (2025) 100696

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review Article

Cloud continuum testbeds and next-generation ICTs: Trends, challenges, and perspectives

Fran Casino [a,b,*], Peio Lopez-Iturri [c], Constantinos Patsakis [b,d]

[a] Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Spain
[b] Information Management Systems Institute, Athena Research Centre, Artemidos 6, Marousi 15125, Greece
[c] Department of Electric, Electronic and Communication Engineering, Public University of Navarre, 31006 Pamplona, Spain
[d] Department of Informatics, University of Piraeus, 80 Karaoli & Dimitriou str., 18534 Piraeus, Greece

ARTICLE INFO

Keywords:
Cloud
Simulation
Cloud testbeds
Cloud continuum
Edge computing
Fog computing

ABSTRACT

As society's dependence on Information and Communication Technologies (ICTs) grows, providing efficient and resourceful services entails many complexities that require, among others, scalable systems that are provided with intelligent and automated management. In parallel, the different components of cloud computing are continuously evolving to enhance their capabilities towards leveraging the next generation of ICTs. Due to the substantial investment in resources required to provide efficient services, suitable research and experimentation platforms to test and validate cloud technologies before releasing them into operational versions are crucial to delivering sound systems with sustainable cost/benefit ratios. In this article, we review the current state of the art by analysing cloud testbeds devoted to studying the capabilities of the cloud continuum. Instead of recalling a component-wise or architectural discussion of these systems, this article explores the full spectrum of the cloud continuum testbeds and their features, providing a taxonomy that can be practically used as an entry point to identify each testbed's scope. Moreover, we extract the challenges found in the literature to deliver a profound discussion, correlating the analysed testbeds and their features. Our findings highlight the main gaps and potential roadmaps to provide effective testbeds considering the next generation of ICTs.

Contents

* Correspondence to: Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Avinguda dels Països Catalans, 26, 43007 Tarragona, Spain.
E-mail addresses: franciscojose.casino@urv.cat (F. Casino), peio.lopez@unavarra.es (P. Lopez-Iturri), kpatsak@unipi.gr (C. Patsakis).

https://doi.org/10.1016/j.cosrev.2024.100696
Received 25 July 2024; Received in revised form 31 October 2024; Accepted 24 November 2024
Available online 6 December 2024

1. Introduction

The next generation of Information and Communication Technologies (ICTs) will be sustained – in its vast majority – by cloud-based platforms [1–3]. This means that the technological advancement and digitisation related to most of the services leveraged by the industry, governments, critical infrastructures, and other companies and end-users, will use cloud resources to provide ubiquitous and timely services in myriad heterogeneous contexts. Moreover, the growth of ubiquitous systems, sensors and smart contexts is forcing a paradigm change in how data are managed and processed, embracing the cloud continuum paradigm [4], in which multiple services and decentralisation levels coexist [5]. The statistics on the number of IoT-connected devices significantly differ between studies [6,7]; nonetheless, the minimum is more than 10 billion worldwide, which justifies some timely initiatives behind the adoption of edge and fog computing [8]. One of the main ideas behind this radical shift is that IoT sensors and data collected from disparate resources are processed on the edge. The latter implies that cloud resources are only used when deemed necessary (i.e., providing elastic resource management), minimising the overload of information flows generated by system endpoints and providing a scalable continuum of resources [9]. On the one hand, this setup reduces latency, costs, and bandwidth. On the other hand, computational resources are required to be installed and managed in the fog and on the edge; thus, the attack surface is increased. Moreover, due to local data preprocessing, some information may be lost and never reach the cloud, which requires further management.

Cyber-physical systems (CPS) refer to a new generation of systems with integrated computational and physical capabilities that can interact with humans in different ways [10]. Thus, CPS testbeds are platforms equipped with system monitoring tools, data analysis capabilities and commercial software [11], capable of simulating platforms in a hybrid (i.e., replicating physical components) or fully virtual environments. Such testbeds are used, among others, for testing and experimenting, as experiments with production systems with real components can incur costly procedures and safety risks [12]. For the sake of readability, this article uses the term “testbed” to refer to such systems.

Motivation and contribution: Given the scale, complexity, and commercial sensitivity of hyperscale computing environments, the opportunity for experimentation is limited and requires a substantial investment of resources in terms of both time and effort, creating an attractive line of research that also has lucrative commercial potential. In this regard, the need for suitable research platforms to test and validate the continuously evolving cloud services and technologies before releasing them into their commercial/functional versions is mandatory to increase the effectiveness of the solutions by resolving possible issues during the development phase, and therefore, guaranteeing the achievement of the desired outcomes at a much lower cost [13]. Moreover, these platforms are used as a back-end to realise simulations in a plethora of contexts, including the implementation of digital twins with diverse capabilities, such as the recreation of real-time working conditions and intelligent decision-making [14].

In this survey, we review the state of the art testbeds devoted to simulating and evaluating particular characteristics of the cloud continuum while providing a classification based on their characteristics and scope. Rather than recalling a component-wise or architectural discussion of these systems, as commonly seen in the literature, the analysis provided in this work aims to provide an entry point for researchers and practitioners to leverage a suitability analysis and further evaluation of the testbeds according to their specific needs. This is accomplished by a robust methodology, which allowed us to collect the current state of practice, including other review articles – as described in the next paragraph – allowing us to provide a unique global overview by recalling the multi-purpose testbeds analysed in them. To complement the latter, and provided such a unified background, we extract the common challenges and issues of state of the art to develop a profound discussion, with a particular interest in the features and enabling technologies that such testbeds should leverage and/or improve to face the next generation of ICTs.

The closer surveys to ours are those of Lynn et al. [15], and Byrne et al. [16], and Sharkh et al. [17]. The scope of these surveys differentiates from ours since they analysed cloud testbeds in terms of their technical components and capabilities, and/or their relevance in the state of the art, focusing on a subset of the cloud testbeds included in our article. Indeed, most of them focus on CloudSim and its variants. Sakellari et al. [18] proposed a taxonomy of research-oriented cloud testbeds, covering a subset of the taxonomy presented in this article. Other authors focused on IoT-based cloud testbeds [19,20], including edge and fog simulation [21,22]. Similarly, Bendechache et al. [23] analysed some tools to leverage resource allocation in the cloud continuum. Fakhfakh et al. [24] performed a taxonomy according to the technologies used in each cloud simulator, focusing on Cloudsim and its variants. Fog-based tesbed and simulation surveys and their challenges have also been discussed in [22,25,26], yet not covering other aspects of cloud computing. Finally, Berman et al. [27] highlighted some cloud testbed systems from the perspective of their research applicability in federated environments.

While the previous surveys have provided insights into specific areas targeting, e.g., cloud-only or fog-only infrastructures, they fail to address the growing complexity and interconnectedness of modern ICT systems that span multiple layers. As next-generation ICT systems are highly dependent on the seamless integration of cloud, edge, and fog computing for critical applications such as real-time data processing, low-latency communication, and scalable resource management, it is crucial to review existing testbeds and identify key challenges and gaps in simulating these environments together. This survey uniquely tackles the integration of cloud, fog, and edge computing environments and fills this gap by offering a novel classification of testbeds across the entire cloud continuum. The latter is enriched by showcasing the interrelation between them and the current gaps and challenges, providing a roadmap for future research.

The remainder of the article is organised as follows. In Section 2, we provide a background on cloud computing and its evolution. Section 3 details our research methodology. Then, Section 4 reviews the state of the art of cloud continuum testbeds and classifies them according to their scope. Relevant open issues, trends, and further research lines are discussed in Section 5. The article concludes in Section 6 by answering the research questions and providing some final remarks.

2. Evolution of cloud computing

The concept of cloud computing goes back to the origins of computing, when users used mainframes. At that time, users had to share the available computing system from their dummy terminals due to lack of resources. This resource sharing is practically at the core of modern cloud computing as users may seamlessly access rich computing environments, storage, and infrastructure via various devices that act as dummy devices of that time.

However, while the evolution of resource sharing in a mainframe was one key factor in developing the concept of the cloud, the creation

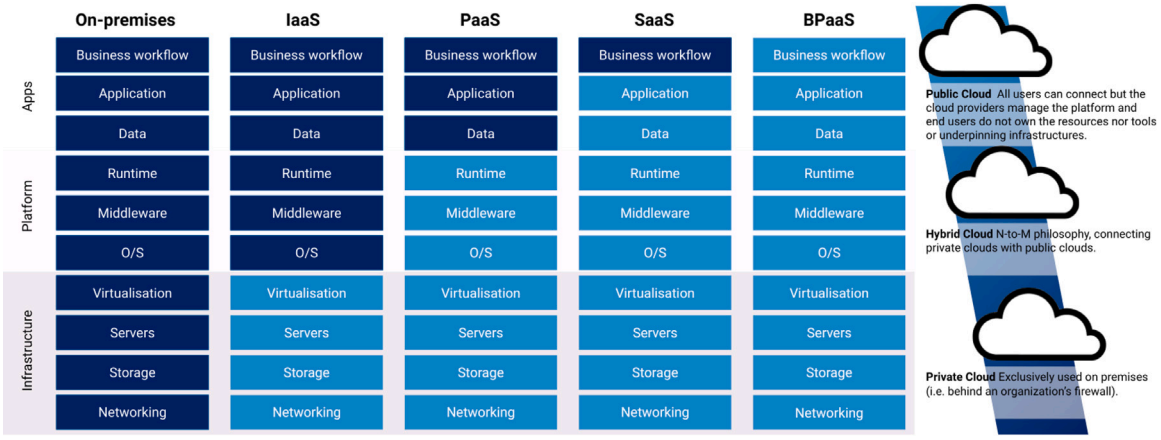


Fig. 1. Cloud services (left) and cloud platform models (right). Cloud services correspond to these available in a public cloud.

of virtual machines in the '70s was also a fundamental milestone. Thus, the primary steps towards sharing different computing resources and interfaces were enabled by hosting various virtual machines in a single physical environment. The latter enabled users to access remote computing environments regardless of where they were hosted. This way, virtualisation and containerisation [28] paved the way for managing computing resources more efficiently and on demand.

The issues related to migrating physical assets to the cloud require a proper suitability assessment according to each need since there are several models of cloud services, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Business Process as a Service (BPaaS). More recently, the Simulation as a Service (SMaaS) concept appeared. SMaaS operates at the application level, sometimes utilising specific hardware tailored to context-aware simulation scenarios [29]. Nevertheless, we consider that SMaaS, depending on its flavours, lies somewhere between SaaS and PaaS without having a clear distinction from them in most settings. Therefore, we omit it from the general classification. Each of the previous variants and concepts has different benefits and assumes a different level of migration, as seen in Fig. 1. The most common service is SaaS, which uses the Internet to deliver applications to its users that are managed by a third-party vendor. In the case of PaaS, all servers, storage, and networking can be managed by the enterprise or a third-party provider, while the developers can maintain the management of the applications. IaaS is used for accessing and monitoring computers, networking, storage, and other services. IaaS allows businesses to purchase resources on-demand and as needed instead of buying hardware outright. BPaaS is an extension of PaaS, which virtualises a whole business process, such as billing and payments. At its core, SMaaS is a cloud-based service designed for decision-making and training purposes. However, the technology faces several technical challenges, including discoverability and scalability [30].

3. Research methodology

Our review protocol is based on the five steps of Denyer and Tranfield [31] for a systematic literature review. More precisely, the steps are the following: (1) Define the scope of the review, (2) Define the research questions, (3) Search literature databases, (4) Apply inclusion and exclusion criteria, and (5) Synthesise and report the results of the literature analysis.

3.1. Defining the scope of the review

A systematic literature review relies on standardised processes for searching, screening, analysing, and synthesising the available literature in a systematic, transparent, and reproducible manner, thus assisting in the development of policy and decision-making [32]. Systematic reviews help build a reliable knowledge base by aggregating information from a wide range of relevant studies [32].

This paper focuses on cloud testbed systems and their particularities according to their features. Our approach relies on several predefined research questions pertinent to cloud testbed systems, which are aligned with the specific objectives of our survey (see Table 1). Based on these research questions, we performed a thorough analysis of the available literature and provided a classification of the most well-known cloud testbed systems.

3.2. Search strategy

As previously stated, our overall survey process is based on several predefined research questions relevant to the cloud testbeds literature. To this end, we performed a systematic literature search without time constraints in October 2024. The main search engines used were Web of Science (WoS) and Scopus, which were used to locate all scientific-related literature due to their multidisciplinary coverage and scope [33]. Google was used as a complementary source to locate further cloud testbed relevant data, mostly from non-research-oriented and commercial solutions (grey literature).

For the white literature, we queried WoS and Scopus using the following query:

```
TITLE-ABS-KEY ( cloud AND ( testbed OR simula-
tion ) ) AND ( LIMIT-TO ( LANGUAGE , ''English''
) ) AND ( LIMIT-TO ( DOCTYPE , ''re'' ) )
```

Note that we limited the search with the previous query so that additional studies can be found afterwards. It should be noted that the first bulk search query yielded 617 results. The database's various refinement features were used (fine-tuning of results following the context of specific articles, papers, subject area, etc.). When a study's abstract was unavailable, the full article was retrieved and evaluated for relevance. Moreover, we retrieved the full text of all relevant articles.

Due to the broad selection of articles, we discovered additional studies using the so-called backward and forward snowball effect, which involved searching the references of critical articles and reports for additional citations [34]. For instance, additional grey literature was discovered by manually searching the reference lists in several

Table 1
Summary of research questions and the corresponding sections devoted to answering them.

Research Question	Objective	Sections
RQ1: What is the current state of practice of cloud testbed systems?	The objective of this question is to discover the features offered by cloud testbed systems and in what contexts researchers and practitioners are devoting more effort so that we can identify the topics that require more support.	4
RQ2: What are the current challenges in cloud testbeds?	Since cloud testbeds offer different functionalities depending on their application context, the aim of this question is to extract the challenges from both local and global perspectives to provide a comprehensive overview.	4 and 5
RQ3: Is the current state of the art aligned with technological evolution in the cloud?	The intention of this question is to analyse whether the actual state of the art, in terms of, e.g., technologies, and simulation capabilities, is sufficient to cope with the next generation of cloud ecosystems. This can serve as a road map for tool and hardware development, more complex simulation environment definitions, and improved benchmarks.	2, 4 and 5
RQ4: What strategies and research directions should be used to deal with identified challenges?	According to the knowledge extracted from the state of the art, the aim of this question is to identify the pain points of the actual state of practice and provide fruitful strategies to overcome them.	5

reports since many cloud testbed solutions are only present in the form of grey literature. The latter were complemented with electronic searches using Google. In particular, different authors looked at the first 100 Google results for the query `cloud testbed systems` to find additional grey literature. Note that the scope of the Google query is to complement the research literature since the survey aims not to provide a report of all existing cloud testbed solutions, but to collect the most relevant ones. The latter also supports that Google may return different results for different users (i.e., the outcomes of the other searches were combined accordingly). Yet, we argue that the purpose and scope of the search are properly fulfilled. Following our methodology, 753 sources were initially selected (combining research and grey literature).

3.3. Apply inclusion and exclusion criteria

We evaluated the eligibility of the retrieved literature based on a set of inclusion/exclusion criteria. Initially, we excluded all non-English written papers from Scopus and WoS. The next step included screening the retrieved articles (title and abstract reading). For the remaining articles, we performed a full reading. It is worth noting that several articles were excluded during the last two steps (Title/Abstract screening and full paper reading). Our exclusion criteria aimed at fulfilling the scope of the survey; thus, we excluded application-based articles not presenting a novel cloud testbed system but only using or recalling it, except for literature review/survey articles, which in turn let us discover further relevant articles through the snowball effect. In addition, we excluded simulation contexts that did not strictly fall into a cloud context simulation (e.g., systems oriented to network-based simulation, which were included due to the use of particular keywords).

As summarised in Fig. 2, after collecting all relevant sources and applying our methodology, 142 research articles passed the title and abstract screening. From these, 29 were discarded after a full review, leaving 113 research articles relevant to the scope of our paper, which were complemented with 34 relevant sources extracted from the grey literature. In this sense, the articles selected in the methodology were used to cover the analysis and classification presented in Section 4. Note that in Section 5, we perform a discussion based on the information collected from these sources plus others according to each section and particular area, as we believe that advancing beyond the state of the art requires a multidisciplinary approach.

3.4. Content analysis and reporting

We adopted a thematic content analysis approach to derive research areas and common themes from the eligible literature. We used qualitative analysis software for the thematic content analysis of the selected literature (MAXQDA2022) [35]. Moreover, the findings were peer-reviewed by the authors. We applied various qualitative analysis methods, such as narrative synthesis, to classify the extracted data comprehensively, combining the findings from multiple studies in a qualitative manner. For example, we present multiple categorisations of the cloud testbed systems, and we analyse their challenges in a global manner according to their context of application to derive further discussion in Sections 4 and 5.

3.5. Bibliographic analysis

The bibliographic analysis includes 113 peer-reviewed research articles published between 2006 and 2024 (as of October). Of these research articles, 76 describe a specific testbed tool, while the other 37 articles analyse different features of one or more than one of these cloud testbeds. As a common practice, we omitted the grey literature in the year-wise analysis due to the difficulty of assessing the exact dates of each contribution or tool. As shown in Fig. 3, 2017, 2018 and 2019 received a relatively high number of publications, all of which were related to specific cloud testbed implementations. In the last five years, the number of review papers discussing cloud testbeds has increased, probably due to the maturity of novel technologies such as blockchain and the increased use of cloud systems in different contexts, with particular relevance of fog and edge, which require extended simulation capabilities. The latter is paired with the cloud adoption in the industry in terms of market size and volume [36–38].

4. Cloud simulation testbeds for next generation ICTs

Nowadays, the complexity of cloud environments is increasing with scale and heterogeneity, posing a challenge to the efficient management of cloud applications and data centre resources. The increasing ubiquity of social media, mobile, and cloud computing combined with the IoT and emerging paradigms such as edge and fog computing is exacerbating this complexity [15,16,39–42]. Following these drivers, this trend is amplified by increasing demands for dependability and real-time low latency communication, among other challenges [25,26,43]. Thus, it has driven the integration of telecommunications [44], software-defined networks [45] and cloud infrastructure (edge computing), and development and integration of applications that make greater use of the capabilities of end-user devices and appliances (fog computing) [19–23,46,47]. However, there is still a general inability to control and process the network environment and predict and control network conditions in hyper-scale computing environments considering a continuum flow of resources from the cloud core to the edge [15,16,48–50].

The research on cloud computing models primarily focuses on the IaaS paradigm. Nevertheless, other models that offer higher integration levels include PaaS, SaaS, and, more recently, SMaaS and BPaaS services in their frameworks [29,51]. The validation of the models, beyond their mathematical soundness and well-established privacy and security policies [52], is a critical part of their development [53] since there is the need to validate the capabilities of a

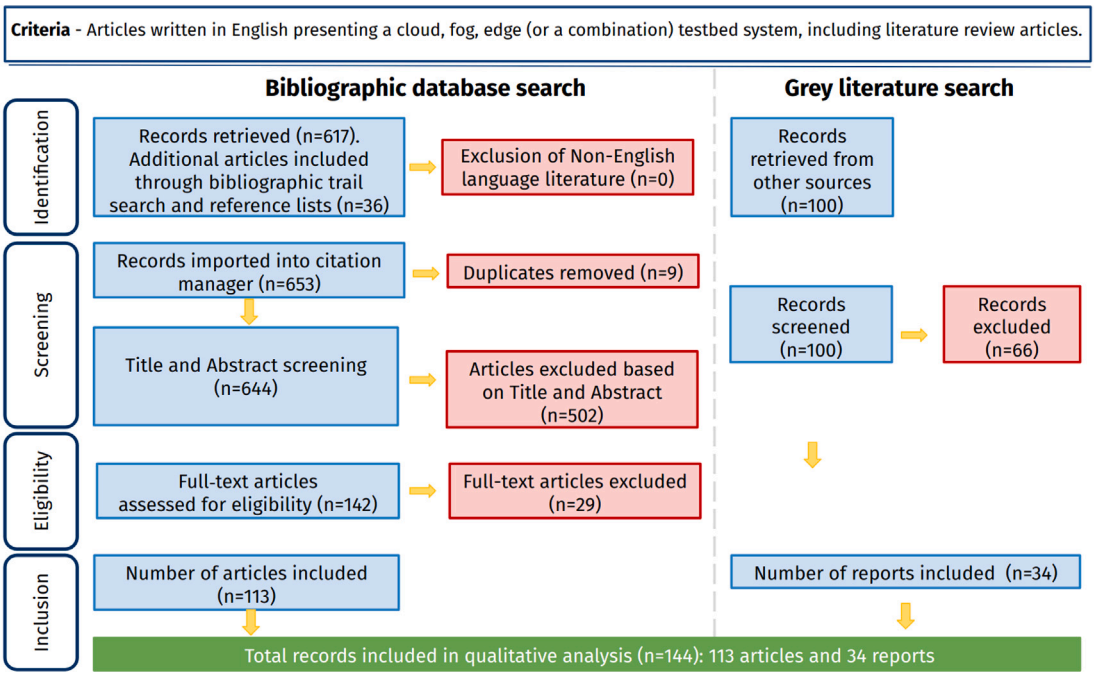


Fig. 2. Flowchart of the statistics for each step according to the inclusion criteria.

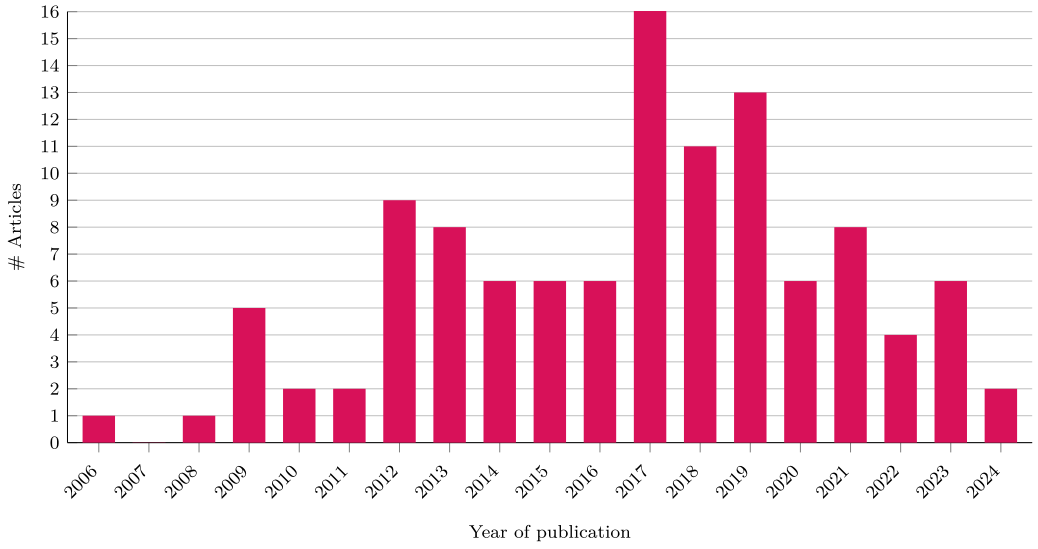


Fig. 3. Distribution of the selected research literature per year.

cloud system from their early stages to their final deployment, both in research and commercial contexts [17,51,54]. Several simulation platforms were conceived from networking simulators such as NS-2 [55], SIMCAN [56], and Simkit [57]. For example, GreenCloud [58] extends NS-2, iCanCloud [59] and secCloudSim [60] extend SIMCAN, and SPECI [61] extends Simkit.

In order to provide a comprehensive overview, we analysed all the testbeds retrieved using the methodology described in Section 3. For each testbed, we provide a summary description, and a classification based on several dimensions, namely the scope, the family, and the category of each testbed as seen in Table 2. We provide a description of each dimension in the following paragraphs.

The 'Scope' column in Table 2 classifies each testbed according to the computing infrastructure it primarily targets: cloud, edge, fog, or a combination of these. This categorisation clarifies the specific environments each testbed is designed for, providing a clearer distinction between the computational layers involved in resource management, data processing, and simulation. The rationale for assigning testbeds to these categories stems from the operational focus outlined in their documentation. For instance, testbeds like CloudSim [162], which focus on resource allocation within large-scale cloud infrastructures, are classified with the Cloud scope. In contrast, testbeds such as PureEdgeSim [165], which focus on distributed processing at the network's edge, are classified as Edge. Some testbeds, like iFogSim [163] and FogBus [161], manage resource orchestration and computation across both fog and cloud environments, combining more than one scope.

According to the analysed literature, we further classified cloud testbed systems into three families (i.e., note that some testbeds may fall into more than one family, yet we selected the most representative one in such cases for the sake of clarity), as can be seen in the 'Family' column of Table 2. First, we grouped cloud testbeds originating from the research, investigation and/or open-source perspective, often

Table 2
Main features and summarised description of the testbeds found in the literature (see [62–150]).

Legend:

Scope: ☁ Cloud, ▦ Fog, ∧ Edge

Family: ● Research and Investigation, ● CloudSim-Related Testbeds, ● Commercial Testbeds

Categories: **R**: Resource Allocation and Management, **P**: Privacy, **S**: Security, **E**: Energy and Performance, **C**: Communication and Networks, **D**: Data Acquisition and Storage

Testbed	Ref.	Scope	Family	Description	Categories
SIMCAN	[56]	☁	●	SIMCAN is a simulation tool for large-scale distributed systems, including storage and computational resources. SIMCAN has a modular design that eases the integration of different basic systems on a single architecture.	R,E,C
GreenCloud	[58]	☁	●	GreenCloud is a network simulation platform with a focus on energy efficiency in data centre networks. Built on the NS2 simulator, it models the energy consumption of servers, switches, and network links.	E,C
iCanCloud	[59]	☁	●	iCanCloud is a simulation framework for cloud architectures and applications, emphasising performance prediction and cost estimation, and allows simulation at different abstraction levels.	R,E,D
secCloudSim	[60]	☁	●	secCloudSim is a security-aware cloud simulation tool that extends ICanCloud to simulate security features and cyber attacks.	R,S,D
CloudSched	[151]	☁	●	CloudSched is an open-source simulation platform for cloud resource scheduling algorithms, focusing on virtual machine allocation and resource utilisation.	R,E
DCSim	[62]	☁	●	DCSim is a data centre simulation framework focusing on resource management and dynamic virtual machine scheduling policies.	R,E
GroudSim	[63]	☁	●	GroudSim is an event-based simulation framework for grid and cloud computing, focusing on job scheduling and resource management. It supports complex job dependencies and workflows.	R,E,C
SPECI	[61]	☁	●	SPECI is a simulation tool for analysing the performance and scalability of cloud infrastructures, focusing on emergent behaviours in data centres. It is useful for studying scalability issues in large-scale data centres.	E
CACTOSim	[152]	☁	●	CACTOSim is a simulation tool for cloud application performance and energy efficiency. As part of the CACTOS project, it models cloud applications and underlying infrastructure.	R,E
Castnet	[64]	☁	●	Castnet is a simulation platform for content distribution networks over cloud platforms, focusing on network performance and efficient content delivery.	C
CloudLightning	[153]	☁	●	CloudLightning is a simulation framework from an EU project, that focuses on the efficiency of heterogeneous cloud infrastructures, including resource management and scheduling.	R,E
OpenNebula	[154]	∧ ☁	●	OpenNebula is an open-source cloud and edge computing platform that simplifies data centre management and supports hybrid cloud deployments.	R,S
OpenQRM	[65]	☁	●	OpenQRM is an open-source data centre management and cloud computing platform. It provides tools for managing both virtual and physical resources in data centres.	R,S
DISSECT-CF	[155]	☁	●	DISSECT-CF is a discrete event-based simulation toolkit for cloud federations, focusing on energy consumption and resource sharing.	R,E
DISSECT-CF-Fog	[66]	▦☁	●	DISSECT-CF-Fog introduces capabilities for modelling fogs and their evaluation in terms of reliability, among the other options offered by DISSECT-CF.	R,E
DISSECT-CF-IoT	[67]	∧ ▦☁	●	DISSECT-CF-IoT enables the resources of DISSECT-CF and extends the capability of modelling IoT sensors.	R,E,C
OpenStack	[156]	☁	●	OpenStack is an open-source cloud computing platform for Infrastructure as a Service (IaaS), supporting public and private clouds with a modular architecture.	R,S
EmuFog	[157]	▦☁	●	EmuFog is a tool for the emulation of large-scale fog computing networks using container technologies. It automates the deployment of fog nodes within network topologies.	C
SCORE	[158]	☁	●	SCORE is a simulation tool for cloud resource and energy optimisation, designed to test energy-efficiency, security and scheduling strategies in cloud environments.	R,E
Eucalyptus	[68]	☁	●	Eucalyptus is an open-source software platform for building AWS-compatible private clouds, enabling hybrid cloud computing with AWS integration.	R,S
FogBed	[69]	▦	●	FogBed is an emulation tool for fog computing environments using container-based virtualisation. It uses Docker containers and it is suitable for testing real applications in fog scenarios.	R,E,C
FogNetSim++	[159]	▦	●	FogNetSim++ is a simulation tool for fog networking environments, focusing on network protocols and resource management.	R,E,C
SimIC	[70]	☁	●	SimIC is a simulation tool for inter-cloud computing systems, simulating interactions between multiple cloud providers resulting in efficient resource allocation management.	R,E,C
FogTorch	[71]	▦	●	FogTorch is a tool for analysing fog computing deployments based on service placement requirements.	R,E
FogTorchII	[72]	▦	●	FogTorchII is a tool for analysing fog computing deployments based on QoS requirements. It evaluates deployment configurations, considering factors such as latency and energy consumption.	R,E
STEP-ONE	[160]	☁	●	STEP-ONE is a simulation tool for edge-fog computing, simulating edge-fog processes based on the Opportunistic Network Environment simulator.	R,E
GDCSim	[73]	☁	●	GDCSim is a green data centre simulator focusing on energy consumption, simulating energy usage in data centres to study energy efficiency.	R,E
TCS ECP	[74]	☁	●	TCS ECP is an Enterprise Cloud Platform developed by Tata Consultancy Services, offering cloud services and solutions for enterprises.	R,S
xCAT	[75]	☁	●	xCAT is a scalable cluster management and provisioning tool used for managing large-scale clusters and data centres.	R
SpanEdge	[76]	∧ ☁	●	SpanEdge is a framework for processing data streams across edge and cloud resources, addressing latency-sensitive stream processing needs.	R,E,C
VirtFogSim	[77]	▦	●	VirtFogSim is a fog computing simulator with a focus on virtualisation, simulating virtualised fog environments.	R,E
YAFS	[78]	∧ ▦☁	●	YAFS is a simulation tool for large-scale fog computing scenarios, focusing on application placement and network dynamics while enabling highly customisable simulations.	R,C,E
piFogBed	[79]	▦	●	piFogBed is a physical testbed for the emulation of fog computing using Raspberry Pi devices, useful for realistic experimentation.	R,E
piFogBedII	[80]	▦	●	piFogBedII is an advanced physical testbed for fog computing using Raspberry Pi devices. It is an updated version of piFogBed, used for advanced fog computing experiments.	R,E
MockFog	[81]	▦	●	MockFog is an emulation platform for fog computing environments that uses containerisation technologies. It facilitates the testing of fog applications within a controlled environment.	R,E
MockFog2	[82]	▦	●	MockFog2 is an updated verson of MockFog platform for fog computing environments, also using containerisation, this time incorporating enhanced features for fog computing emulation.	R,E
FogBus	[161]	▦☁	●	FogBus is a middleware platform for integrating fog and cloud resources, designed to simulate IoT applications along with security and privacy configurations.	R,S,P,E,C
FogDirSim	[83]	▦	●	FogDirSim is a fog computing simulation environment that permits the comparison of different application management strategies within fog environments.	C
FogExplorer	[84]	▦	●	FogExplorer is a tool for modelling and simulation of fog computing architectures, analysing application deployment. It provides a graphical user interface for designing and evaluating fog scenarios.	R,E
Edge-Fog Cloud	[85]	∧ ▦☁	●	Edge-Fog Cloud is a simulation framework that combines edge, fog, and cloud computing layers to evaluate end-to-end scenarios. It addresses resource management across all layers.	R,E,C

(*continued on next page*)

presented and discussed in the research literature. Next, due to its popularity, we consider CloudSim [162] and its variants into another

Table 2 (*continued*).

DockerSim	[86]	☁	●	DockerSim is a simulation tool for container-based virtualisation in cloud environments, focusing on container orchestration and management.	R,S,E
Apache VCL	[87]	☁	●	Apache VCL is a cloud computing platform for provisioning resources used in academic environments. It supports reservation of resources and virtualisation, often employed in universities.	R,S
Grid5000	[88]	☁	●	Grid5000 is a large-scale grid and cloud computing testbed in France, used for research in parallel and distributed computing.	R,S,E,C
SimGrid	[89]	☁	●	SimGrid is a simulation framework for modelling and studying large-scale distributed computing systems with applications, enabling versatile configurations and metrics.	R,E,C
ENIGMA	[90]	∧ ⠿ ☁	●	ENIGMA, based on the SimGrid simulation tool, is capable of simulating Edge and Fog Computing environments, allowing the specification of different characteristics of the components and applications.	R,E,s
Chameleon	[91]	☁	●	Chameleon is a large-scale, reconfigurable testbed for cloud research that supports high-performance computing and cloud computing experiments.	R,S,E,C
Nimbus	[92]	☁	●	Nimbus is a cloud computing toolkit providing an implementation to manage virtual infrastructures with a web service interface.	R,S
Cloudlab	[93]	☁	●	CloudLab is a cloud computing research testbed designed for building customisable cloud environments, supporting different cloud architectures and applications for testing and benchmarking.	R,S,E,C
Okeanos	[94]	☁	●	Okeanos is a cloud service providing virtual computing resources in Greece. It offers Infrastructure as a Service (IaaS) primarily for academic and research institutions, facilitating scholarly activities with scalable computing resources.	R,S,C
Fed4fire	[95]	☁	●	Fed4FIRE is a federated testbed infrastructure for experimentation across wired, wireless, and cloud domains. It offers access to diverse testbeds across Europe, enabling comprehensive networking and cloud experimentation.	R,S,C
Fed4fire+	[95]	☁	●	Fed4FIRE+ is an enhanced version of the Fed4FIRE federated testbed, offering additional features for experimentation. It continues to provide access to diverse European testbeds for advanced networking research.	R,S,C
Open Cirrus	[96]	☁	●	Open Cirrus is a cloud computing testbed dedicated to open-source research. It allows the federation of resources, and focuses on fostering research and innovation.	R,S,C
Open Cloud Testbed	[97]	☁	●	Open Cloud Testbed is a platform for cloud computing research and experimentation that supports open-source cloud technologies. It provides access to OpenStack and other cloud software, facilitating research in cloud infrastructure and services.	R,S,E,C
FIT IoT-LAB	[98]	∧	●	FIT IoT-LAB is an IoT experimentation platform designed for large-scale wireless sensor network experiments. It provides thousands of nodes across several sites in France, supporting extensive networking research in IoT.	S,E,C
SAVI	[99]	∧ ☁	●	SAVI (Smart Applications on Virtual Infrastructure) is an edge computing testbed for cloud and edge computing research. It focuses on future internet application research, providing a platform for developing smart applications on virtual infrastructures.	R,S,E,C
Sphere	[100]	∧	●	Sphere is a project that offers research infrastructures with diverse resources relevant to cybersecurity and privacy research.	R,S,C,P
Abiquo	[101]	☁	●	Abiquo is a cloud management platform designed for hybrid cloud orchestration. It manages private, public, and hybrid cloud infrastructures, providing tools for efficient cloud integration and management.	R,S
Heroku	[102]	☁	●	Heroku is a cloud platform supporting multiple programming languages. It simplifies application deployment and scalability, allowing developers to deploy applications without managing underlying infrastructure.	R,S
Adtran Mosaic	[103]	☁	●	Adtran Mosaic offers network access solutions through software-defined access and cloud software for broadband networks, allowing virtualisation to enhance management.	R,S
IBM Cloud	[104]	☁	●	IBM Cloud is an enterprise cloud platform offering IaaS and PaaS with a focus on artificial intelligence and data analytics. It provides a range of cloud services, including IBM Watson AI, to support advanced business applications.	R, S, D, P, E
Alibaba Cloud	[105]	☁	●	Alibaba Cloud provides cloud computing services such as elastic computing, databases, storage, and CDN. As a leading cloud provider in China and the Asia-Pacific region, it offers robust resource management solutions.	R, S, D, P, E
Google Cloud	[106]	☁	●	Google Cloud is a scalable cloud platform offering services running on Google's internal infrastructure. It provides IaaS, PaaS, and serverless computing environments, supporting various cloud service models.	R, S, D, P, E
MetaNet Tplatform	[107]	☁	●	MetaNet Tplatform is a cloud services provider offering hybrid cloud solutions in South Korea. It delivers end-to-end hybrid cloud services, including IaaS, PaaS, and SaaS, to meet diverse business needs.	R,S
Tencent Cloud	[108]	☁	●	Tencent Cloud offers comprehensive cloud services, including compute, storage, databases, and AI services. As one of China's leading cloud providers, it provides a global infrastructure for various technological applications.	R, S, D, P, E
Amazon Web Services	[109]	☁	●	Amazon Web Services (AWS) provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, supporting a wide range of cloud-based solutions.	R, S, D, P, E
Microsoft Azure	[110]	☁	●	Microsoft Azure is a public cloud platform offering a comprehensive set of services for building, deploying, and managing applications. It supports a wide range of programming languages, tools, and frameworks, facilitating versatile application development.	R, S, D, P, E
Apache CloudStack	[111]	☁	●	Apache CloudStack is open-source cloud computing software for creating and managing IaaS cloud services. It supports hypervisors like KVM, VMware, and XenServer, enabling flexible cloud orchestration and management.	R,S
Salesforce Cloud	[112]	☁	●	Salesforce Cloud is a cloud-based customer relationship management (CRM) platform providing tools for customer service, marketing automation, and analytics.	R,S,P
Cisco Cloud	[113]	☁	●	Cisco Cloud delivers cloud solutions focusing on networking, security, and collaboration services. It offers multi-cloud solutions and cloud-managed networking, aiding organisations in managing networks across various cloud environments.	R,S
Rackspace Cloud	[114]	☁	●	Rackspace Cloud provides managed cloud computing services across applications, data, security and infrastructure, offering support to optimise cloud deployments.	R,S
Cloud Foundry	[115]	☁	●	Cloud Foundry is an open-source, multi-cloud application PaaS governed by the Cloud Foundry Foundation. It enables developers to deploy and scale applications without managing infrastructure, promoting efficient application development.	R,S
Oracle Cloud	[116]	☁	●	Oracle Cloud offers cloud services including SaaS, PaaS and IaaS. It provides integrated cloud applications and platform services, supporting businesses in deploying enterprise applications.	R, S, D, E
DataDog	[117]	☁	●	DataDog is a monitoring and analytics platform for cloud-scale applications. It provides performance metrics and event monitoring, offering real-time insights into application and infrastructure performance.	R,S
VMware Cloud	[118]	☁	●	VMware Cloud delivers cloud services for running, managing, connecting and protecting applications across clouds. It offers solutions for hybrid and multi-cloud environments, extending VMware infrastructure seamlessly to the cloud.	R,S
Digital Ocean	[119]	☁	●	DigitalOcean is a cloud infrastructure provider offering compute, storage, and networking resources to enable accessible application deployments.	R, S, D
SAP Cloud	[120]	☁	●	SAP Cloud is a cloud platform providing SaaS, PaaS and IaaS solutions with a focus on enterprise applications for businesses.	R, S, D, P
CloudSim	[162]	☁	●	CloudSim is a general-purpose cloud computing simulation framework that supports modelling of cloud infrastructures, virtual machine provisioning, and resource scheduling. It is widely used and extensible, serving as the basis for many other simulators such as iFogSim and NetworkCloudSim.	R,E
ElasticSim	[121]	☁	●	ElasticSim is a simulation tool for elastic cloud resource management, designed to evaluate techniques for auto-scaling web applications in cloud environments.	R,E
Cloud2Sim	[122]	☁	●	Cloud2Sim is a concurrent and distributed cloud simulation platform designed to simulate heterogeneity in computational clouds.	R,E
EMUSIM	[123]	☁	●	EMUSIM is a hybrid tool that integrates emulation and simulation for cloud applications, combining real application execution with simulation by using automated switching between the two modes.	R,E
CloudSimSDN	[124]	☁	●	CloudSimSDN is a simulation framework designed to model and simulate cloud computing environments integrated with SDN concepts.	R,C
CEPSim	[125]	☁	●	CEPSim is a simulation tool for complex event processing in cloud environments, designed to evaluate the performance of event processing systems over cloud infrastructures.	C
FederatedCloudSim	[126]	☁	●	FederatedCloudSim is a simulation tool for federated cloud environments, focusing on resource sharing across clouds. It models inter-cloud communication and data transfer costs.	R,E,S
FTCloudSim	[127]	☁	●	FTCloudSim is a fault-tolerant cloud simulation tool that simulates failures and recovery mechanisms. It extends CloudSim to evaluate fault tolerance strategies.	R,E,S
CDOSim	[128]	☁	●	CDOSim is a Cloud Deployment Option Simulator that evaluates the cost and performance of cloud deployment options, aiding in decision-making for cloud deployments.	R,S,D

(*continued on next page*)

Table 2 (*continued*).

iFogSim	[163]	⁞⁞ ☁	●	iFogSim is a simulation tool for fog and edge computing environments that extends CloudSim. It models latency and network congestion and it is widely used for fog computing research.	R,E,S,P
IOTsim	[129]	☁	●	IOTsim is a simulation tool for IoT applications within cloud environments, designed to evaluate IoT data processing and resource allocation in clouds.	R,E
CloudAnalyist	[130]	☁	●	CloudAnalyst is a simulation tool built on top of CloudSim, designed specifically to model and analyse large-scale cloud computing environments with a focus on the performance of applications deployed in geographically distributed data centres.	R,E
CloudExp	[131]	☁	●	CloudExp is a cloud computing experimentation framework that provides a flexible environment for conducting cloud experiments.	R,E
MR-CloudSim	[132]	☁	●	MR-CloudSim is an extension of CloudSim for MapReduce applications, simulating data processing tasks by modelling MapReduce job execution in cloud data centres.	R,E
CloudReports	[133]	☁	●	CloudReports is a user-friendly cloud simulation tool that emphasises reporting and visualisation. It is well-suited for educational purposes and provides graphical outputs.	R,E
MultiRE-CloudSIm	[134]	☁	●	MultiRE-CloudSim is an extended version of the CloudSim simulation framework that is designed to model and simulate multi-region cloud computing environments.	R,E
NetworkCloudSim	[135]	☁	●	NetworkCloudSim is a network-aware cloud simulation tool that extends CloudSim with network topologies and bandwidth sharing. It is useful for applications sensitive to network performance.	C
CloudSimEx	[136]	☁	●	CloudSimEx builds on the basic CloudSim framework by offering more advanced tools for modelling, simulating, and evaluating cloud resource management, scheduling, and virtual machine provisioning strategies in cloud data centres	R,E
DartCSim	[137]	☁	●	DartCSim is an enhanced cloud simulation system that offers better performance and hides implementation details, allowing users to configure all the data of the simulation environment with a visual interface.	R,E
PriDynSim	[138]	☁	●	PriDynSim is an I/O scheduling cloud simulation tool that models dynamic I/O behaviour in cloud data centres.	R,E
DartCSim+	[139]	☁	●	DartCSim+ is an advanced data centre simulator with power and network models, simulating energy consumption and network performance in data centres with improved accuracy.	R,E
TeachCloud	[140]	☁	●	TeachCloud is an educational cloud computing simulation toolkit, an extension of CloudSim designed for academic teaching purposes.	C
DynamicCloudSim	[141]	☁	●	DynamicCloudSim is an extension of CloudSim for dynamic simulation scenarios, supporting dynamic workloads and resource variation during simulation runtime.	R,E
UCloud	[142]	☁	●	UCloud is a cloud computing platform designed to provide scalable and flexible infrastructure as a service (IaaS). By implementing a hybrid cloud model, it focuses on performance and cost reduction.	R,E
EdgeCloudSim	[164]	∧ ☁	●	EdgeCloudSim is a simulation tool for edge computing scenarios that includes mobility models, network modelling, and edge server simulation. It is an extension of CloudSim useful for mobile edge computing studies.	R,C,E
WorkflowSim	[143]	☁	●	WorkflowSim is an extension of CloudSim for workflow simulations, adding support for modelling workflow execution and scheduling in cloud environments.	R
EdgeNetworkCloudSim	[144]	∧ ☁	●	EdgeNetworkCloudSim simulates both edge and cloud environments with detailed network modelling, combining features of EdgeCloudSim and NetworkCloudSim.	R,C
FogWorkflowSim	[145]	⁞⁞	●	FogWorkflowSim is a simulation tool for workflow management in fog computing environments. It extends WorkflowSim and evaluates the performance of workflow scheduling algorithms.	R,E
MobFogSim	[146]	⁞⁞ ☁	●	MobFogSim is a simulation tool focusing on mobility in fog computing, considering user mobility patterns and evaluating Quality of Service (QoS) in mobile fog environments.	R,E
MyiFogSim	[147]	⁞⁞	●	MyiFogSim is an extension of iFogSim with additional features, enhancing it with new capabilities for fog computing research.	R,E,S, P
PFogSim	[148]	⁞⁞	●	PFogSim is a simulator for performance evaluation in pure fog computing environments, focusing on fog-only scenarios without cloud interaction.	R,E
PureEdgeSim	[165]	∧	●	PureEdgeSim is a simulation tool for edge computing environments that includes mobility and network models. It models energy consumption and network latency, supporting custom scenarios.	R,E
MDCSim	[149]	☁	●	MDCSim is a multi-tier data centre network simulation tool that focuses on performance and scalability. It models data centre components including servers, switches, and network topology.	R,E,C
RECAP	[150]	☁	●	RECAP is a simulation tool for cloud, edge, and fog computing that optimises application deployment and simulates large-scale network scenarios.	R,E

group. Finally, commercial cloud systems, oriented to companies and businesses and mainly service provision for profit, are summarised in the last group. Regarding the research and investigation testbeds group, several testbed software frameworks have been developed to set up and manage a private cloud, covering different service layers. These frameworks enable fine-grained outcomes and resource control since the software can be designed to solve a specific problem and the set of physical resources assigned to it. The main trade-off of these solutions is that they usually cannot reproduce realistic functionalities due to reduced computing resources compared to large-scale platforms. Therefore, further experiments in real-world scenarios are required depending on the research context or product. As already discussed, one needs access to a hardware infrastructure and a software framework to set up a cloud environment for experimental purposes. Multiple research centres, businesses and academics support the testbeds discussed in this section. This practice is therefore translated into a service commonly known as testing-as-a-service (TaaS) [166] and is widely adopted due to its attractive features, delivering automated application testing services. TaaS enables the proper testing of diverse technologies such as large-scale tests compared with local testbeds, reproducible experimentation based on realistic user and machine behaviour, the dynamic resource allocation from local resources to distributed large-scale cloud platforms, the seamless integration of complex distributed systems and tools to the broader community, and, thus, a transition model to provide successful research and experimentation outcomes [167]. The majority of the testbeds of this group aim to simulate advanced resource allocation, virtualisation and orchestration of the cloud. In this regard, more efforts should be devoted to IoT-oriented testbeds, which should enable the simulation of Industry 4.0 frameworks and their corresponding metrics [49].

Cloud simulation systems usually instantiate machines and simulate multiple resources, including network, traffic profiles, virtual machines and even federated clouds. These methods can simulate and monitor the properties above and other features, such as energy consumption. The most common simulation method for cloud systems is Discrete Event Simulation (DES) [15], where every system change is modelled as an event. Since CloudSim [162] is the most widely-used platform [23], DES is the most popular modelling technique, also paired with the timeliness of its release. Nevertheless, CloudSim-based testbeds are able to cover simulate multiple aspects of cloud, fog, and edge, showcasing their diversity. Similarly to CloudSim, other examples of DES simulation platforms are DISSECT-CF [155], SCORE [158], STEP-ONE [160], FogNetSim++ [159], and CloudLightning Simulator [153]. Nevertheless, there is a lack of cloud testbeds focusing on the novel cloud continuum paradigm [4]. While simulation offers several advantages, especially in terms of scalability and experiment reproducibility, it is still based on assumptions and simplifications that could only partially represent an actual cloud [18,168].

Finally, the resource potential offered by commercial solutions is at another level, yet it is often used to simulate the performance in the latest stage of development. Clearly, the objective of this survey is not to perform a market analysis or capture all existing cloud commercial solutions. Thus, we selected the most representative according to our research methodology and their adoption [37,38], thus many commercial solutions are not included.

The last dimension (last column in Table 2) relies on a set of key operational categories, namely, Resource Allocation and Management, Privacy, Security, Energy and Performance, Communication and Networks, and Data Acquisition and Storage. The Resource Allocation and Management category was applied to testbeds that explicitly manage

resource scheduling, task management, workload distribution, or resource provisioning in cloud, edge, or fog environments. For example, platforms like CloudSim [162], iCanCloud [59], and OpenNebula [154] have integrated mechanisms for managing virtual machines (VMs), containers, or distributed workloads, making them central to resource management. The Privacy category was assigned to platforms that explicitly handle user data protection, data privacy concerns, or compliance with privacy regulations. Testbeds like FogBus [161] and iFogSim [163] were categorised under privacy due to their proximity to end-user data in fog and edge computing environments, where sensitive information is processed closer to the user. The Security category was applied to testbeds that either simulate security features or focus on securing cloud and distributed computing environments. Platforms like secCloudSim [60] and OpenStack [156] implement mechanisms to ensure data integrity, secure resource management, and access control. As a further example, platforms without a direct focus on security, like GreenCloud [58], were excluded from this category. The Energy and Performance category included tools that focus on optimising the energy consumption of cloud or distributed infrastructures or that emphasise performance optimisation. Testbeds like GreenCloud [58] and CACTOSim [152] focus on improving energy efficiency within data centres or cloud environments. Other platforms like CloudSched [151] focus on performance optimisation and were also included in this category. The Communication and Networks category was applied to platforms that explicitly simulate or manage network communication or interactions between cloud, edge, or fog environments. Testbeds such as FogNetSim++ [159] and EmuFog [157] fall under this category because they emphasise network simulation and communication between distributed nodes. Finally, the Data Acquisition and Storage category includes testbeds focusing on data management, storage solutions, or handling large datasets in distributed environments. For instance, iCanCloud [59] and secCloudSim [60] manage data storage systems and support secure data handling.

The goal of this comprehensive categorisation, along with the rest of dimensions was to align the testbeds with the computing infrastructure components they are designed to simulate or manage, ensuring a clear understanding of the scope and capabilities of each testbed. Moreover, Section 5 discusses the same subset of categories, allowing the reader to map each testbed in Table 2 with the current state of knowledge, gaps, and challenges to establish a connection across them.

5. Discussion and the road ahead

To identify which features would be desirable to enhance in Cloud testbed systems, we split the analysis into different sections, highlighting the benefits of each technology and the importance of their integration in cloud testbeds, as depicted in Fig. 4. Furthermore, we discuss qualitative aspects of evaluating testbed systems, which require particular attention.

5.1. Communication and connectivity

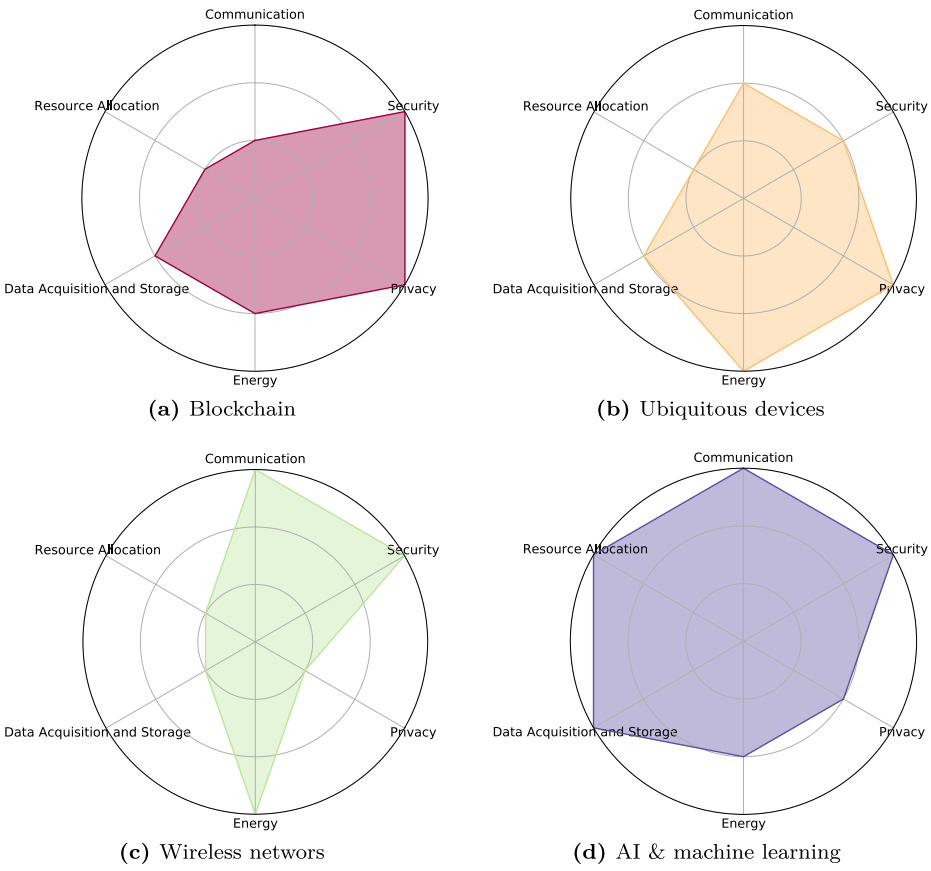
The connectivity and the assessment of wireless communications among the components/devices of a cloud-based system are key factors to guarantee operational performance. However, in most cases, they are overlooked in general solutions proposed in the literature and by cloud testbed systems in particular. For instance, although some tools for networking simulation could be used to leverage current testbeds [20], including IoT systems [41], they lack the proper simulation of novel communication technologies and ubiquitous device capabilities. For instance, some examples of wireless security testbeds can be found in the literature [169], yet there is a gap in terms of actually computing and simulating wireless propagation behaviours. IoT devices are usually connected via wireless communications, and the inherent properties of the wireless channel make the radio propagation assessment and subsequent radio planning very complex. This complexity is given mainly due to the site-specific nature of the behaviour of the propagating waves, which is determined by the obstacles, their material's electric properties (i.e., dielectric constant and conductivity) and the interaction of the electromagnetic waves with these objects. Thus, different contexts lead to different electromagnetic propagation phenomena such as reflection, refraction, diffraction and scattering.

Typically, the deployed devices create a Wireless Sensor Network (WSN) or an IoT-based network capable of containing thousands of devices, depending on the specific application and subject to the underlying wireless technology. Should the wireless network be deployed without a proper radio planning analysis, the collected information by the nodes might never reach the gateway or the edge nodes. In general, it is often assumed that the nodes deployed in a real environment will work correctly, but that is not always true, even more in complex radio-electric environments such as Vehicle to Everything communications [170], Industry 4.0 (e.g., due to the presence of volumetric and metallic obstacles, electromagnetic noise), Smart Farming (e.g., due to near-ground or underground communication, presence of high-density vegetation) or Urban scenarios (e.g., due to high density of obstacles such as buildings, presence of human beings, the coexistence of other wireless systems), to name a few. Therefore, radio propagation estimation methods for different wireless communication systems in cloud testbeds would be beneficial when evaluating the wireless communication alternatives deployed in specific environments. Accurate results of the overall performance of the wireless network would help practitioners select the most suitable wireless communication solution, including the wireless technology (e.g., LoRaWAN, WiFi, ZigBee), its parameters (e.g., transmitted power, antenna types, spreading factors in case of LoRaWAN) and issues related to the network deployment (e.g., location of nodes and gateways, coverage-capacity assessment, number of nodes to be deployed, latency, nodes' energy consumption, SNR and interference analysis).

The development of wireless communication techniques has increased in recent years while new protocols have been created to meet the new requirements for WSNs and the IoT paradigm leading to the adoption of mature technologies such as Bluetooth [171], RFID [172], ZigBee [173], Ultra Wide Band (UWB) [174] or LoRaWAN [175]. Nevertheless, the list of available wireless communication technologies is far greater. More recently, new technologies have been introduced in a continuous effort to improve the capabilities of the precedents (e.g., enhance range and data rate, and decrease the latency and energy consumption). In this group, we can classify the promising Bluetooth 5 LE (Low Energy) [171], 5G communication systems [176], Near Field Magnetic Induction (NFMI) systems [177], Mioty [178] or WiFi HaLow (IEEE 802.11ah) [179]. Other relevant technologies include networks based on 6G systems [180], new protocols such as WiFi 7 (IEEE 802.11be) [181], and millimetre wave communication systems, in general, [182].

This range of wireless communication technology possibilities leads to increasingly complex radio planning tasks. Thus, including radio propagation analysis tools in cloud testbeds becomes challenging. The empirical or statistical models are the most direct and easily implementable propagation models, based on measurements and using a set of equations derived (from a regression) from those extensive field measurements. Once obtained, they are simple and efficient if employed for the analysis in environments with the same characteristics as those where the original measurements were made [183]. However, the main drawback of empirical models is that the accuracy falls drastically when used for different types of environments. For example, using a macrocell model for indoor pico-cells. Some examples of empirical models are Okumura, Hata and COST 231 models.

In contrast to empirical models, deterministic radio propagation methods exhibit increased accuracy since they consider site-specific features (i.e., all the elements within the scenario are taken into account, their size and their material's electromagnetic properties) based on numerical calculations: They solve Maxwell's equations to calculate



(a) Blockchain (b) Ubiquitous devices

(c) Wireless networs (d) AI & machine learning

Fig. 4. Relation between different enabling technologies and their relevance considering each discussed topic.

the full electromagnetic propagation behaviour, taking into account all phenomena (i.e. refraction, reflection, scattering and diffraction) [183]. Some examples are the Ray-Tracing method [184], the Method of Moments (MoM) [185] and the Finite-Difference Time-Domain (FDTD) method [186]. The major disadvantage of the deterministic methods is the large computational overhead that could be prohibitive for some large complex environments. For these cases, Ray Tracing and Ray Launching methods offer a good trade-off between accuracy and calculation time, providing accurate RF power distribution estimations [183, 187]. Above all, the 3D or volumetric tools offer results for the whole volume of the scenario under analysis [188].

Finally, it is worth noting that beyond the tools for radio propagation analysis, other technologies impact connectivity and communication, such as machine learning and blockchain. For example, in edge and fog computing, it is crucial to reduce communication overhead. In this regard, machine learning, particularly distributed and federated learning approaches, can prevent sending data to the cloud if it can be processed in edge of fog devices. More concretely, computation and data-sharing across different edge devices are crucial to establishing an effective ML-edge distributed system [189]. Novel networking paradigms that are 'computation-aware' are highly desirable for building such data-sharing distributed systems. 5G networks, which provide Ultra-Reliable Low-Latency Communication (URLLC) services, are a promising field to integrate with edge computing. 5G should help to establish more control over the network resources for supporting on-demand interconnections across different edge devices. The adoption of software-defined networks and network function virtualisation and its integration in Cloud testbeds systems to include 5G networks and control distributed ML settings is a clear example of an appealing research area for future ML researchers [44]. On the other hand, Blockchain could boost the privacy and security of the growing number of personal wireless devices and the generated personal data [190], for spectrum sensing and medium access regulation [191], and identifying fraudulent users in wireless networks [192]. Additionally, Wireless Blockchains will provide decentralised services to current wireless systems, which are centralised (causing data monopoly, such as 5G) and easy to be attacked [193]. Wireless Blockchains and their transactions, consensus protocol messages and new blocks face the same characteristics of all wireless communications: limited resources (e.g. energy consumption), higher interference levels and path loss, which could impact very negatively on the performance of a Wireless Blockchain, especially if the consensus protocol is affected. Thus, these key issues are being analysed and studied to facilitate large-scale deployments of Blockchain-based wireless networks [194].

5.2. Security and privacy

Cloud outage [195–197] and unauthorised access [198] are not rare phenomena. Yet, cloud vulnerabilities are typically not issued CVEs as they are not linked to a specific element but are caused by misconfigurations. As a result, customers have little insight into the actual security of deployed clouds. Some initiatives, such as the Open Cloud Vulnerability and Security Issue Database (OCVSID) [199] have shed some light on this aspect; nevertheless, due to the criticality of cloud infrastructures, it is necessary to push the security aspect further and having cloud security testbeds available for researchers and practitioners is an ideal way to identify and patch security issues before they become an actual problem.

To understand the risk exposure, we examined the reports from OCVSID and categorised the various published vulnerabilities for services such as AWS, Google Cloud, and Azure into multiple categories, see Table 3. Fig. 5 shows the distribution of reports per severity. It must be highlighted that many of these vulnerabilities classify into more than one category, but the denoted number refers to the number of reports.

Table 3
Classification of vulnerabilities reported in the Open Cloud Vulnerability and Security Issues Database.

Vulnerability	#	Vulnerability	#
Privilege escalation	21	Lack of audit trail	5
Unauthorised access	17	CSRF	4
Stored data/metadata exfiltration	13	XSS	3
Remote code execution	12	Request smuggling	3
Credential/data/code leak	11	Malicious images/dockers/packages	4
Policy override	10	SQL injection	2
Sandbox/terminal/container escape	9	Other	8
Cryptographic primitives	5		

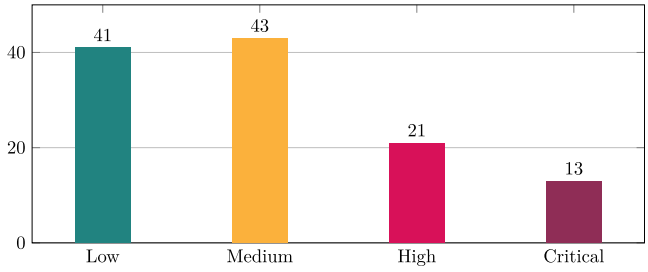


Fig. 5. Classification of vulnerabilities reported in the Open Cloud Vulnerability and Security Issues Database per severity.

The latter justifies the difference in the numbers reported in Table 3 and Fig. 5. Practically, one of these attacks may apply to more than one service or imply more than one attack on a service, and we differentiate the data stored on the cloud from possibly other user data stored by the service, credentials, and metadata. It is clear that cloud services often suffer from privilege escalation attacks, unauthorised access, and data leaks, although they were developed to avoid these attacks. Even if one considers the rest of the attacks, it is easy to understand that the exposure is not significantly different from other information systems, e.g., remote code execution, data leakage, and escape from isolated environments (e.g. sandbox, container). Moreover, issues with cryptographic primitives are very relevant in the cloud context. However, the impact of such attacks is some orders of magnitude bigger than traditional information systems, as the underlying information can be on the scale of hundreds of terabytes.

Considering the state of practice of cloud security, we should revisit the role of security in cloud testbeds. Currently, the bulk of research is focused on the use cloud for security testing or simulating attack scenarios and providing cyber range capabilities [200–206] as the cloud offers an on-demand isolated infrastructure to test various attacks and monitoring malware [207–210]. This results from the convenience of the cloud of preventing further infection, always being available, and dynamically allocating resources. The latter has pushed most malware analysis sandboxes to cloud infrastructures. While several existing testbeds have inherent security measures, the state of the practice illustrates that testbeds focused on security must be developed so that practitioners and researchers can test and validate these infrastructures. In the literature, there are some such testbeds [211,212]; however, more targeted development and broader scenarios must be considered. Using tools and methods such as [213–216] and DevSecOps approaches must be fostered to enable easy and seamless integration and automated testing of security features and policies. Especially the fostering of DevSecOps can provide more guarantees that baseline security measures have been tested before the deployment to production while also having further security monitoring measures and procedures to timely detect and mitigate attacks once the cloud infrastructure is deployed. In fact, according to a recent report [217], only 50% of IT decision-makers across industries perform some application security testing procedure during the DevOps process. The most common such procedures are software analysis scanning solutions, dynamic analysis methodologies and third-party penetration testing. While chief information officers (CIO) and other decision-makers seem to be very aware of the benefits of fostering DevSecOps [218], they are rather slow in this shift as they report several obstacles including: (i) lack of "automated, integrated" security testing tools, (ii) inconsistent approaches, (iii) the fact that security testing "slows things down", (iv) the large number of false positive results, and (v) developer resistance to adopting new methodologies and technologies. Incorporating technologies and procedures in testbeds to prevent vulnerabilities and exploits starting from the development till the production phase is critical [54]. Thus, an important research path arises towards adopting sound and automated methodologies to test the security of the cloud and providing services in the aforementioned categories.

Beyond the above, one should also consider the shift towards zero-trust security [219]. In essence, up to recently, organisations have abided by the perimeter security model. What is within the perimeter is secure and trusted; all the attacks come from outside. However, once an adversary gets a foothold at a host of an organisation, all traffic is treated as legitimate and can lead to full compromise. The zero trust model tries to eliminate such risks by segmenting the network, ensuring that only legitimate traffic is allowed after being authenticated while all traffic is logged and inspected, conforming to the least access privilege policy. Despite the technical difficulties in implementing zero trust in one organisation, implementing it in a cloud environment is an even bigger challenge. The reason is that the cloud is beyond the organisation's premises and its actual perimeter. As a result, there are obvious constraints in implementing such a policy. Evidently, fostering zero trust models in cloud testbeds is a definite need and would enable organisations to boost their security significantly [220,221]. Note that while organisations shift their infrastructure to the cloud, they have many employees and subcontractors working remotely and using external applications with their own outgoing and incoming connections. Nevertheless, the fact that much of this traffic is expected does not often trigger any alert. Thus, the zero trust model can fill in many gaps in the security of most organisations, respecting their current workflows. Cloud-wise, while we acknowledge that many companies provide consulting services to foster this approach, given the aforementioned issues, having some cloud testbeds to assess the fitness and efficiency of such technologies and architectures would be greatly beneficial.

Some of the countermeasures to enforce such trusted environments rely on various access technologies, including, but not limited to VPN access, software-defined perimeter, proxies (inbound, cloud access security broker), and virtualised firewall, to mention a few. The result of this is very fragmented security architectures in which it is difficult to be sure which policies are in place to protect any given data in the cloud at any given time. Despite the legal issues that this may raise [222], this situation puts at stake the very foundations of organisations, which nowadays is their data.

This landscape motivated NIST's publication regarding Zero Trust architectures [223] which devotes a section to multicloud enterprises, highlighting that "*relying on the enterprise perimeter for security becomes a liability*". The use of this security model aims to bring the following business benefits; (a) network visibility improvements, breach, detection, and vulnerability management, (b) to stop malware propagation, (c) to reduce both capital and operational expenditures on security, (d)

to increases data awareness and insight, (f) prevents data exfiltration into the hands of malicious actors.

In addition to security, cloud platforms are no longer only serving resources (i.e. IaaS), but they are also providing services at the application and development level, as discussed in Section 1. Such services are integrated into a myriad of end users, requiring the management of hundreds or thousands of applications, which need a careful development strategy to resolve problems in a scalable way. In this context, some novel development paradigms like FleetOps [224] focus on the efficient planning, management and use of containers (e.g. Dockers, Kubernetes) to guarantee rapid development without requiring huge teams behind the process. Such strategies can be integrated from the planning phase and integrated into the PaaS layer to enhance the management of an application or a website infrastructure by eliminating several core sinks such as manual development/deployment/testing, heterogeneous technology stacks, or the disparate security updates/checks of the underlying technologies.

Finally, of specific interest for cloud testbeds is the privacy perspective. Currently, there are several proposals on how to store, retrieve content, and perform computations on data in a privacy-preserving manner [225–231] mainly exploiting homomorphic encryption and other cryptographic primitives. However, despite their necessity, the available testbeds are very rare in the literature [232]. Given that security and privacy issues in the underlying schemes can gravely impact the users' data, the availability of privacy-focused cloud testbeds to experiment with these mechanisms is crucial to cope with current challenges and regulations [233,234]. Moreover, the upcoming adoption of secure post-quantum cryptographic primitives will require further testing to assess their fitness for handling sensitive user data at scale.

For more on cloud security and privacy, the interested reader may refer to [231,235–240].

5.3. Energy and performance

Energy consumption, related to both data processing and wireless communication of the deployed devices, is a critical aspect that should be taken into consideration when resource allocation is being analysed and planned. In fact, improving the overall energy consumption of the network will directly affect the network lifetime and the general cost of the system.

Following that idea, different energy-saving techniques for IoT nodes [241] and energy efficiency for WSNs have been broadly studied in recent years, covering diverse areas such as energy-efficient routing protocols for WSNs [242,243], MAC (Medium Access Protocol) protocols for energy consumption enhancement [244], optimised clustering algorithms [245] and energy-efficient data transmission in the integration of WSNs and cloud computing [246].

As can be seen, many of the presented studies come from the research and development of protocols for WSNs, as these networks are, in many cases, the base for the Internet of Things. But nowadays, searching for sustainable cities and societies leads researchers to study new techniques and next-generation IoT devices. Thus, research topics within the frame of the design of sustainable green communication networks such as Energy Harvesting, (ultra-)low-power Wireless Connectivity or Sustainable Eco-Friendly Manufacturing have been gaining importance [247,248]. In addition to enabling wireless communication technologies for the so-called Green IoT [249], Radio Resource Management (RRM) has gained a lot of attention mainly due to the development of Artificial Intelligence (AI) techniques applied to radio designs such as next-generation 5G or 6G networks [250,251]. Although AI heralds a step-change in RRM and wireless networks, its high energy consumption requirements present a challenge in terms of energy efficiency and management [252].

At this point, Software Defined Networks (SDN) play a key role. SDNs can be leveraged to enhance the efficiency of cloud computing, in areas such as communication overhead, performance, virtualisation, and also energy consumption. These software-defined environments, merged with the centralised processing of cloud-based systems, can lead to green and flexible Cloud-Radio Access Networks (C-RAN). Due to the innovation of migrating baseband processing functionalities to the cloud, C-RAN solutions are anticipated to drastically reduce energy consumption and become a prospective architecture for 5G and greener next-generation networks [253].

Among future networks, it is worth mentioning dynamic and heterogeneous WSNs and IoT networks, where Vehicular Ad-hoc Networks (VANET) and flying Unmanned Aerial Vehicles (UAV)-based Internet of Drones (IoD) networks present specific and complex challenges in terms of energy management due to their intrinsic dynamism and continuous re-organisation of the network [254,255]. Finally, we want to mention the fast-growing quantum-based applications, specifically quantum-based WSNs, which have not been thoroughly studied yet [256], but surely will cause a great impact in every area of wireless communications.

As seen, wireless communication systems combined with Cloud capabilities present a very complex frame where many different wireless communication technologies, network topologies, applications and interdisciplinary solutions can be found. Therefore, including these aspects in cloud testbeds to analyse and assess energy efficiency is very challenging. But a task that should be carried out due to the huge importance that energy management and consumption reduction have gained nowadays in a world where green and eco-friendly solutions must be deployed in the near future.

5.4. Data processing and storage

The humongous amount of data generated by ubiquitous devices, including IoT devices and sensors [257,258] is estimated to keep growing. Therefore, optimising data collection and processing in constrained devices is mandatory [259,260]. However, according to the application scenario, such optimisation must be applied carefully. For instance, vehicle systems generate large amounts of data that need to be processed in real-time [258]. In this regard, bandwidth constraints prevent continuous communications with the cloud, and thus, edge computing is becoming an integral part of autonomous vehicle systems. Due to the critical impact of system failures in this context, cloud testbeds that aim at simulating networking, communication and AI-based data processing policies of vehicular networks (e.g. reducing the number of necessary communications and applying AI-based methods to reduce the amount of data required to make decisions) have to be tested to ensure security and performance [50].

In the recent years, edge computing has been increasingly used to deploy machine learning based intelligent systems in resource-constrained environments [260,261]. However, most AI models, such as deep learning, require training large datasets. This conflicts with resource-constrained IoT devices, which may generate continuous sources of data, but their limited storage and power make them unsuitable for training tasks [260,262]. In this regard, federated learning is a promising line, which enables distributed aggregation of local models and privacy-preserving mechanisms [263]. These can be combined with AI-based data storage policies to discard unnecessary data and minimise communications with the cloud [262,264].

One of the most relevant contexts which needs further simulation is smart cities [265]. The continuous digitisation of urban areas is enabling a myriad of context applications such as pedestrian security monitoring, crowd analysis, traffic surveillance, secure emergency response, and weather monitoring, to name a few [266]. The scalability of such systems depends on the capabilities of the devices in several dimensions, such as storage, energy, and processing power. Moreover, the cloud computation resources behind them and the communication overhead must be carefully assessed. Notably, smart cities combine heterogeneous sources of information, which require careful processing

to leverage learning models according to different applications [265–267]. Moreover, given the challenges to be faced by future mega-cities, current approaches could be enhanced with cognitive models to exploit human-machine collective intelligence [268]. Therefore, cloud testbeds should accommodate use case scenarios and capabilities to mimic orchestration between fog, edge and cloud by collecting these data from different sources and applying data management policies to reduce communication overhead.

Recently, systems that combine components such as AI, IoT, and blockchain are proliferating [269]. Blockchain provides interesting features to enhance the next-generation cloud, such as integrity and auditability [270]. Moreover, the use of encryption provides extended security, privacy, and robustness to edge and fog computing frameworks. However, these features come with a cost due to their computation and communication overhead. Next generation testbeds should manage the latter by allowing the integration of blockchain systems in their simulation scenarios.

Blockchain is also used to extend current business networks by enabling collaboration opportunities and enhancing the trust of such transactions [271]. For instance, blockchain is currently used to enforce quality of service policies in the context of the cloud [272]. Smart contracts combined with monitoring systems can ensure that the resources allocated by a cloud provider and their performance are guaranteed, avoiding, e.g. computing resources saving policies the cloud provider applies.

5.5. Resource allocation management

Given the extended and successful use of AI and machine learning to solve optimisation problems considering different sets of challenging features and multiple sources of heterogeneous information, researchers and practitioners have recently started adopting such tools to optimise the functionalities of cloud platforms on their core level [273]. Cloud resource allocation management entails the study of the behaviour of several dimensions of the cloud architecture. For instance, resource management includes the dynamic allocation of containers (i.e. computing resources) to prevent bottlenecks, the seamlessly distributed allocation of resources to optimise the performance/scalability of the platform, and the monitoring of the lifecycle of the hardware, preventing deterioration of the systems due to overloads and scheduling the proper maintenance tasks. The use of ML enables the automation of the aforementioned tasks according to predefined rules. Moreover, due to the learning capabilities of deep learning and ML models, we can optimise and prevent managerial issues [274,275]. This guarantees the elastic provision of services according to the statistics monitored and collected, enabling the application of seamless cloud-to-edge managerial policies, which could adapt their traffic size and computing power in real-time to unpredictable amounts of requests [49,276].

Resource allocation management in cloud environments is a well-studied problem [25,277], including coordinating the cloud's physical and virtual resources. Traditionally, it is tackled by static policies that have two shortcomings [273]. First, they are tuned offline based on relatively few benchmark workloads. For example, threshold-based policies typically involve hand-tuned thresholds that must be used for widely different workloads. Second, static policies require reactive actions and may incur unnecessary overheads and customer impact. To deal with these problems, intelligent cloud resource management is introduced as a significant shift to automatically manage and coordinate all aspects of cloud assets, especially resource utilisation. For instance, scheduling strategies based on heuristic and meta-heuristic techniques can be employed in fog-based environments to release and request resources [278].

In general, submitting containers to virtual machines (VMs) and VMs to physical machines is an NP-hard combinatorial problem. The problem can be formulated as an optimisation problem, where the objective is to minimise power consumption and increase resource utilisation of a cloud data centre. Moreover, depending on the VM placement strategy, we mainly differentiate it into static and dynamic. A static VM placement algorithm maps a set of VMs, the number of which and the corresponding configuration is known, to a set of fully empty physical machines. Static and dynamic placement can be considered a vector bin-packing problem [279]. However, the former is preferred in current installations because extensive dynamic placement may cause overhead due to the time consumed by the migration process [280,281]. Nonetheless, the actual load of a system relates to the running applications, and for VMs, the actual memory and processing consumption are constantly changing. Obviously, a static memory and processing allocation policy will lead to a waste of resources.

The fact that applications live on the cloud practically means that the infrastructure must dynamically change depending on the workload [282]. To this end, IBM, Google, Amazon, Microsoft, and other providers offer cloud services that dynamically scale to cater to their customers' instant needs [283]. Notably, this scaling is primarily performed over configurations that remain static. For example, the client reserves a specific amount of CPU or memory resources that account for the spikes in traffic, storage, and processing needs. The dynamic scaling often results in significant service costs since such spikes are not usually estimated correctly by the users and result in many issues in service provisioning [282,284]. The recent outages and service disruptions due to the high demand during the COVID-19 worldwide crisis indicate that many cloud service providers are not yet ready to provide their services to such a scale [285,286]. Moreover, they indicate the high dependence of Europe on other countries for ICT infrastructures, as showcased by recent innovation actions such as GAIA-X [287]. However, while the infrastructure scales, the same does not apply to the applications. Considering that the application should always exhibit the same behaviour, regardless of the workload, means that we do not exploit our applications' full potential and scalability. For instance, one may prioritise specific tasks when the workload is exceptionally high or use another set of algorithms to address the increased needs. As running edge applications involves the coordination of edge nodes, computing resources, storage resources, and application services, applications have to be continuously manually managed to adjust resources to the fluctuating demand and face transient failures due to the heterogeneous and unreliable nature of edge nodes, posing a challenge [40,46,160,288]. In this regard, to make our applications elastic and context-aware, the infrastructure must be provided with the necessary intelligence to optimally adapt to the changing environment [23,40].

One way to balance the resources is to predict changes by recognising patterns and making the corresponding allocation seamless. To this end, public cloud providers are leveraging ML-based resource management in production [289], and optimisations based on Evolutionary Computing (EC) [290,291]. For example, Google uses, among others, neural networks to optimise fan speeds and other energy knobs [292]. In academia, researchers have proposed using collaborative filtering in scheduling containers for reduced in-server performance interference [293]. Others suggested using reinforcement learning to adjust the resources allocated to co-located VMs [294]. Furthermore, several proposed ML-informed dynamic policies can naturally adapt to actual production workloads [295–297], so each server can learn different thresholds for its resource management.

Despite these prior efforts and opportunities, it is unclear how best to integrate ML into cloud resource management. Previous approaches differ in multiple dimensions. For instance, the ML approach may generate either actual resource management decisions or just predictions regarding the workload or infrastructure. In some cases, the ML is deeply integrated with the resource manager; in others, it is entirely separate.

Going beyond cloud data centres, the emerging edge computing paradigm aims to fill the gap between centralised cloud infrastructures and data produced at the network edge. Nonetheless, many applications

cannot be sustained by solely using edge resources or sending all the data to the cloud [269]. They instead require a fluid integration of resources at the edge, the core, and along the data path to support dynamic and data-driven application workflows; that is, they need to leverage a computing continuum [4,298]. Continuum computing aims to realise a fluid ecosystem where distributed resources and services are programmatically aggregated on-demand to support emerging data-driven application workflows. In this context, Deep Reinforcement Learning (DRL) [295,299–303] outstands among the state of the art methods proposed in the literature for intelligently managing and orchestrating resources across the compute continuum [304,305]. Due to its excellent ability of autonomic and efficient learning, DRL not only handles the uncertainties of workload demands on resources but also deals with complex and dynamic environments [301,306]. This can be achieved since DRL algorithms can start from zero knowledge and gradually achieve human-level control capability over a specific environment to achieve some objective (reward). As such, a DRL-based computing resource management paradigm does not require prior knowledge of the network dynamics and the specificities of each deployed application. DRL agent-based models are capable of autonomously acquiring a holistic view of the computing environment and the data flows within deployed services by learning to make appropriate control decisions for optimising the service performance and cloud/edge resource efficiency [299,307]. Finally, blockchain systems and their integration into cloud systems are receiving increasing attention towards cloud continuum systems, IoT and resource allocation management [308–312], establishing a promising research line.

In conclusion, it is crucial to test different resource allocation strategies according to specific contexts (e.g., disparate cloud continuum setups and underlying technologies) in testbeds to ensure their performance, given their core impact on the whole cloud ecosystem.

5.6. Benchmarking of cloud testbeds and harmonisation

In general, a rigorous methodology needs to be followed to evaluate the performance of a cloud system [51,313], which often uses mathematical models adopted to a set of features, metrics, and characteristics [273,314]. A proper study of such metrics [164,313] is crucial to establish reproducible and comparable outcomes for each service offered and the monitored features [315].

Notably, each testbed enables different services and simulation capabilities. Thus, each service level will require different configurations and dynamism to accommodate different setups [51]. Moreover, use cases must be adequately defined to test several aspects according to the application context, e.g., vehicular, healthcare, finance, and supply chain, since requirements vary. For instance, some cases require advanced local data processing to minimise network overhead, or in others, data protection plays a critical role. Based on the number of sensors and hardware that a system may require, the ability to emulate them along with their energy consumption, processing power, and networking capabilities is crucial, especially in the case of IoT-enabled cloud contexts such as fog and edge.

Another critical research objective is to develop standards and frameworks towards interoperability between different cloud software [26] so that researchers and practitioners can use federated resources [316], resulting in a smooth integration of high-performance computing environments. Overall, a sound cloud testbed design should give application developers greater control over the network, computing power, data infrastructures and services, and seamless access to continuous service environments. While this path is being explored via multicloud solutions [317–319], we argue that there is still a road ahead in this direction. In parallel, the increasing complexity of cyber–physical systems requires the integration between simulations offering different features [11,40,48]. For instance, the Internet of Simulation (IoS) [320] allows the connection and integration of simulations, resulting in large co-simulations, overcoming the difficulty of developing large-scale monolithic simulations.

As previously discussed, there is an obvious need for improving cybersecurity. The types and number of cyberattacks and cybercrimes are constantly growing and causing significant damage to our economy and society, as has been demonstrated many times. Several measures are contemplated to overcome this [321–324], such as the necessity of rules and standards governing the cybersecurity of all connected devices, services, processes and software and a regulator with the necessary resources and capacity to enforce the rules. Moreover, a huge increase in stakeholder awareness of the need for enhanced cybersecurity is also needed since prevention measures are less costly than dealing with the consequences of cyberattacks and cybercrimes currently being experienced [222,325,326]. According to each product, its particularities, and its domain, different definitions and certifications are needed, strengthening the need for harmonisation.

Finally, the definition of sound policies to manage resources and security is a mandatory requirement to realise "everything-as-a-service" provisioning since virtual resources need to be automatically adapted from machine to machine (M2M), including cloud and edge assets, and end-user requirements. In this regard, management and security are tight together since the system's resources can be changed dynamically when a security threat is detected, significantly reducing the impact of attacks. Moreover, the platform can react in a preventive manner by enabling management policies that distribute the load balance in a way that, even if under attack, minimise the required time to reach a stable status again.

6. Concluding remarks

Cloud testbeds provide a myriad of components and simulation scenarios, e.g., to enable real-time applications and services simulations, reduce delays throughout product testing procedures, and enhance certification procedures [53]. Thus, cloud testbeds are a crucial component in achieving the next generation of ICTs, and advancement in multiple sectors is tied to different constraints and technological requirements.

Due to the challenges discussed in Section 5, adopting cloud computing from SMEs and the public administration does not meet the expectations [327]. It has significantly improved from the 25% (for SMEs) reported in 2018 [328], mainly due to the shift of many services, including email and productivity suites on the cloud, and was given a further boost during the recent lockdown. However, cloud infrastructures and services, e.g. AI and big data analytics, are yet to be widely adopted. The latter could be attributed to the lack of trust in the cloud providers and their services as they operate beyond their control. Note that their core assets and the collected and generated data must be outsourced for storage and processing. Therefore, to guarantee mandatory features such as performance, scalability, availability, security and privacy, cloud platforms require the proper application of managerial – in terms of resources and allocation – and security – in terms of prevention, detection and mitigation of threats – policies. The research questions posed in Section 3 summarise the main aim of our research, namely providing a comprehensive review of cloud continuum testbeds, focusing on their role in simulating and evaluating cloud, edge, and fog environments for next-generation ICT systems, and identifying challenges and gaps where research should be focused. We discuss them in order as follows:

***RQ1**: What is the current state of practice of cloud testbed systems?*

The current state of the art reflects a broad set of testbeds supplying different research and industrial needs, addressing the growing complexity of cloud environments. In particular, cloud testbeds like CloudSim and iFogSim have become integral in modelling and simulating cloud infrastructures, resource allocation, and network behaviour. Section 4 provides a detailed classification of these systems based on their operational scope, distinguishing between cloud, fog, and edge computing environments. Nevertheless, while these testbeds have advanced to incorporate modular and scalable features, challenges remain in fully integrating emerging technologies like edge computing and IoT into existing frameworks. The analysis of such testbeds indicates that they are designed to simulate different aspects of cloud environments, from data centre performance to energy efficiency. However, some areas, such as security, have not received much attention, except for commercial platforms. Moreover, gaps in coverage, particularly concerning the cloud continuum, need to be addressed. Therefore, there is room for improvement to accommodate the next generation of ICTs.

***RQ2**: What are the current challenges in cloud testbeds?*

The challenges cloud testbeds face range from technical limitations in handling large-scale distributed environments to gaps in addressing emerging trends such as the cloud continuum. These challenges are exacerbated by the need for low-latency communication and efficient resource allocation across diverse network topologies. Moreover, Section 5 highlights that many systems struggle to provide accurate, real-time simulations of large, dynamic networks. Incorporating real-time systems and IoT devices into cloud testbeds introduces additional complications, such as ensuring seamless integration and scalability while procuring adequate levels of privacy and security. Addressing these challenges requires further refinement in simulation frameworks and the development of more robust models capable of simulating and benchmarking next-generation cloud ecosystems so that real deployments can be made with guarantees.

***RQ3**: Is the current state of the art aligned with technological evolution in the cloud?*

The alignment of cloud testbeds with technological evolution in cloud computing is partial, as existing platforms have made significant advancements but still lag in several critical areas. Section 2 provides an overview of the technological advancements in cloud computing, such as the shift towards virtualisation, containerisation, and the increased role of edge computing. While several testbeds have incorporated some of these advancements, their capacity to fully simulate the complexities of next-generation cloud architectures remains limited. Sections 4 and 5 further highlight that the state of the art is not fully equipped to integrate AI-driven cloud orchestration, real-time decision-making, and advanced resource management at the edge and fog layers. The rapid pace of technological development, especially in distributed and federated cloud environments, has outpaced the capabilities of numerous existing testbeds. Therefore, while there is a general alignment, there is a need for more advanced testbeds that can better cope with the demands of modern cloud infrastructures.

***RQ4**: What strategies and research directions should be used to deal with identified challenges?*

To address the challenges identified in cloud testbeds, future research should focus on several key areas, including enhancing modularity, improving interoperability between cloud, edge, and fog environments, and fostering the development of AI-driven cloud management frameworks. More concretely, Section 5 thoroughly discusses these strategies, suggesting that testbeds need to adopt more modular designs that can be easily adapted to new technologies as they emerge. Additionally, improving the interoperability of cloud testbeds with fog and edge systems is crucial to managing the increasing volume and diversity of cloud workloads. In parallel, integrating more sophisticated benchmarks and performance evaluation tools into testbeds is mandatory to ensure they can accurately simulate the behaviour of large-scale, distributed environments. Finally, embracing machine learning and AI in cloud orchestration and resource management is a promising path, allowing for more efficient and scalable solutions in next-generation ICT systems. We foresee that these strategies will enable cloud testbeds to evolve alongside the cloud continuum and meet the demands of modern cloud infrastructures.

In terms of future trends, recent enabling technologies such as blockchain, with features like decentralisation and immutability, add, among others, trustworthiness and transparency to cloud computing solutions. Although its relatively recent adoption, blockchain has been integrated into many cloud architectures [310,329]. Nevertheless, each cloud solution may differ, and the suitability of blockchain has to be assessed according to the corresponding specifications and requirements. Thus, the incorporation of blockchain in cloud testbeds is a promising line of research and mandatory to test aspects such as efficiency, costs, data privacy issues due to immutability, the use and selection of the proper consensus mechanisms [330–332], and the control of the whole ecosystem and its scalability, taking into account further aspects of blockchain architectures [333,334]. Other novel paradigms enabling cognitive intelligence and dynamic, distributed learning approaches, combined with the advent of advanced human-machine interactions, require further ethical, technological, and security assessments before deploying them into production systems due to the potentially concerning criticality of such advancements. Therefore, cloud testbeds enable a seamless and scalable integration of technologies and services to benefit society as a whole. We sustain that our topic-based analysis, along with the discussion on the current challenges and future trends, reflects with high fidelity the current state of practice and provides a fruitful ground for research in the coming years.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported by the European Commission under the Horizon Europe Programme, as part of the projects SAFEHORIZON (Grant Agreement no. 101168562), LAZARUS (Grant Agreement no. 101070303) and HEROES (Grant Agreement no. 101021801). This work was also supported by the European Union's Internal Security Fund as part of the ALUNA project (Grant Agreement no. 101084929). This work was also supported by the COST Action GoodBrother, Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living, (CA 19121). This work was partially supported by Ministerio de Ciencia, Innovación *y* Universidades, Gobierno de España (Agencia Estatal de Investigación, Fondo Europeo de Desarrollo Regional -FEDER-, European Union) under the research grant PID2021-127409OB-C33 CONDOR. Fran Casino was supported by the Spanish Ministry of Science and Innovation under the "Ramón *y* Cajal" programme (RYC2023-044857-I), and by AGAUR with the project ASCLEPIUS (2021SGR-00111).

The content of this article does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

Data availability

Data will be made available on request.

References

[1] European Commission, 2022, https://digital-strategy.ec.europa.eu/en/policies/cloud-computing.

[2] European Commission, European industrial technology roadmap for the next generation cloud-edge offering, 2021, https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf.

[3] Ericsson, The future of cloud computing: Highly distributed with heterogeneous hardware, 2020, https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/the-future-of-cloud-computing.

[4] A. Al-Dulaimy, M. Jansen, B. Johansson, A. Trivedi, A. Iosup, M. Ashjaei, A. Galletta, D. Kimovski, R. Prodan, K. Tserpes, et al., The computing continuum: From IoT to the cloud, Internet of Things 27 (2024) 101272.

[5] S. Moreschini, F. Pecorelli, X. Li, S. Naz, D. Hästbacka, D. Taibi, Cloud continuum: The definition, IEEE Access 10 (2022) 131876–131886.

[6] G.D. Maayan, The IoT rundown for 2020: Stats, risks, and solutions, 2020, https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx.

[7] B. Jovanovic, Internet of things statistics for 2023 - taking things apart, 2023, https://dataprot.net/statistics/iot-statistics/.

[8] J. Liang, F. Liu, S. Li, Z. Cai, A comparative research on open source edge computing systems, in: Artificial Intelligence and Security: 5th International Conference, ICAIS 2019, New York, NY, USA, July 26-28, 2019, Proceedings, Part II, Springer-Verlag, Berlin, Heidelberg, 2019, pp. 157–170.

[9] D. Balouek-Thomert, E.G. Renart, A.R. Zamani, A. Simonet, M. Parashar, Towards a computing continuum: Enabling edge-to-cloud integration for data-driven workflows, Int. J. High Perform. Comput. Appl. 33 (6) (2019) 1159–1174.

[10] R. Baheti, H. Gill, Cyber-physical systems, Impact Control. Technol. 12 (1) (2011) 161–166.

[11] O. Salunkhe, M. Gopalakrishnan, A. Skoogh, Å. Fasth-Berglund, Cyber-physical production testbed: literature review and concept development, Procedia Manuf. 25 (2018) 2–9.

[12] C. Siaterlis, B. Genge, Cyber-physical testbeds, Commun. ACM 57 (6) (2014) 64–73.

[13] X.F. Liu, et al., Cyber-physical manufacturing cloud: Architecture, virtualization, communication, and testbed, J. Manuf. Syst. 43 (2017) 352–364.

[14] K.Y.H. Lim, P. Zheng, C.-H. Chen, A state-of-the-art survey of digital twin: techniques, engineering product lifecycle management and business innovation perspectives, J. Intell. Manuf. 31 (2020) 1313–1337.

[15] T. Lynn, et al., A preliminary systematic review of computer science literature on cloud computing research using open source simulation platforms, in: Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017), ScitePress, 2017.

[16] J. Byrne, et al., A review of cloud computing simulation platforms and related environments, in: International Conference on Cloud Computing and Services Science, 2, SCITEPRESS, 2017, pp. 679–691.

[17] M.A. Sharkh, A. Kanso, A. Shami, P. Öhlén, Building a cloud on earth: A study of cloud computing data center simulators, Comput. Netw. 108 (2016) 78–96.

[18] G. Sakellari, G. Loukas, A survey of mathematical models, simulation approaches and testbeds used for research in cloud computing, Simul. Model. Pract. Theory 39 (2013) 92–103.

[19] A. Singh, A. Payal, S. Bharti, A walkthrough of the emerging IoT paradigm: Visualizing inside functionalities, key features, and open issues, J. Netw. Comput. Appl. 143 (2019) 111–151.

[20] E.E. Abel, M.S. Abd Latiff, The utilization of algorithms for cloud internet of things application domains: a review, Front. Comput. Sci. 15 (3) (2021) 1–27.

[21] M. Ashouri, et al., Quality attributes in edge computing for the internet of things: A systematic mapping study, Internet of Things 13 (2021) 100346.

[22] S. Svorobej, P. Takako Endo, M. Bendechache, C. Filelis-Papadopoulos, K.M. Giannoutakis, G.A. Gravvanis, D. Tzovaras, J. Byrne, T. Lynn, Simulating fog and edge computing scenarios: An overview and research challenges, Future Internet 11 (3) (2019) 55.

[23] M. Bendechache, S. Svorobej, P. Takako Endo, T. Lynn, Simulating resource management across the cloud-to-thing continuum: A survey and future directions, Future Internet 12 (6) (2020) 95.

[24] F. Fakhfakh, H.H. Kacem, A.H. Kacem, An evaluative review and research challenges of the simulation in cloud environment, Int. J. Softw. Innov. 5 (4) (2017) 59–73.

[25] S. Patel, R. Patel, A comprehensive analysis of computing paradigms leading to fog computing: simulation tools, applications, and use cases, J. Comput. Inf. Syst. 63 (6) (2023) 1495–1516.

[26] M. Gill, D. Singh, A comprehensive study of simulation frameworks and research directions in fog computing, Comp. Sci. Rev. 40 (2021) 100391.

[27] M. Berman, et al., Future internets escape the simulator, Commun. ACM 58 (6) (2015) 78–89.

[28] R. Queiroz, T. Cruz, J. Mendes, P. Sousa, P. Simões, Container-based virtualization for real-time industrial systems—A systematic review, ACM Comput. Surv. 56 (3) (2023) 1–38.

[29] W. de Paula Ferreira, F. Armellini, L.A. De Santa-Eulalia, Simulation in industry 4.0: A state-of-the-art review, Comput. Ind. Eng. 149 (2020) 106868.

[30] M. Shahin, M.A. Babar, M.A. Chauhan, Architectural design space for modelling and simulation as a service: a review, J. Syst. Softw. 170 (2020) 110752.

[31] D. Denyer, D. Tranfield, Producing a systematic review, Sage Handb. Organ. Res. Method. (2009) 671–689.

[32] D. Tranfield, D. Denyer, P. Smart, Towards a methodology for developing evidence-informed management knowledge by means of systematic review, Br. J. Manage. 14 (3) (2003) 207–222, http://dx.doi.org/10.1111/1467-8551.00375.

[33] R. Pranckutė, Web of science (WoS) and scopus: The titans of bibliographic information in today's academic world, Publications 9 (1) (2021) 12.

[34] J. Vom Brocke, et al., Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research, Commun. Assoc. Inf. Syst. 37 (1) (2015) 9.

[35] maxqda, https://www.maxqda.com/, accessed on 04.04.2024.

[36] A. Khayer, et al., The adoption of cloud computing in small and medium enterprises: A developing country perspective, VINE J. Inf. Knowl. Manage. Syst. (2020).

[37] Zdnet, https://www.zdnet.com/article/the-top-cloud-providers-of-2021-aws-microsoft-azure-google-cloud-hybrid-saas/, accessed on 04.04.2024.

[38] Itproportal, https://www.itproportal.com/guides/best-cloud-computing-services/, accessed on 04.04.2024.

[39] D. Rodriguez, D. Gomez, D. Alvarez, S. Rivera, A review of parallel heterogeneous computing algorithms in power systems, Algorithms 14 (10) (2021) 275.

[40] X. Zhou, X. Gou, T. Huang, S. Yang, Review on testing of cyber physical systems: Methods and testbeds, IEEE Access 6 (2018) 52179–52194.

[41] S. Zhu, S. Yang, X. Gou, Y. Xu, T. Zhang, Y. Wan, Survey of testing methods and testbed development concerning internet of things, Wirel. Pers. Commun. 123 (1) (2022) 165–194.

[42] M. Nikravan, M.H. Kashani, A review on trust management in fog/edge computing: Techniques, trends, and challenges, J. Netw. Comput. Appl. (2022) 103402.

[43] M. Zolghadri, P. Asghari, S.E. Dashti, A. Hedayati, Resource allocation in fog–cloud environments: State of the art, J. Netw. Comput. Appl. 227 (2024) 103891.

[44] A. Esmaeily, K. Kralevska, Small-scale 5G testbeds for network slicing deployment: A systematic review, Wirel. Commun. Mob. Comput. 2021 (2021).

[45] J. Son, R. Buyya, A taxonomy of software-defined networking (SDN)-enabled cloud computing, ACM Comput. Surv. 51 (3) (2018) 1–36.

[46] A.A. Alli, M.M. Alam, The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications, Internet of Things 9 (2020) 100177.

[47] P. Gupta, R. Sharma, S. Gupta, Simulators for fog computing and information processing, Proc. Nat. Acad. Sci. India Sect. A (2024) 1–11.

[48] D.W. McKee, et al., Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems, CAAI Trans. Intell. Technol. 3 (2) (2018) 75–82.

[49] Z.J.K. Abadi, N. Mansouri, M. Khalouie, Task scheduling in fog environment—Challenges, tools & methodologies: A review, Comp. Sci. Rev. 48 (2023) 100550.

[50] B. Ahmed, A.W. Malik, T. Hafeez, N. Ahmed, Services and simulation frameworks for vehicular cloud computing: a contemporary survey, EURASIP J. Wireless Commun. Networking 2019 (1) (2019) 1–21.

[51] N. Thakur, A. Singh, A. Sangal, Cloud services selection: A systematic review and future research directions, Comp. Sci. Rev. 46 (2022) 100514.

[52] R. Masood, M.A. Shibli, Y. Ghazi, A. Kanwal, A. Ali, Cloud authorization: exploring techniques and approach towards effective access control framework, Front. Comput. Sci. 9 (2) (2015) 297–321.

[53] R.M. Fujimoto, Research challenges in parallel and distributed simulation, ACM Trans. Model. Comput. Simul. (TOMACS) 26 (4) (2016) 1–29.

[54] M. Younas, D.N. Jawawi, I. Ghani, T. Fries, R. Kazmi, Agile development in the cloud computing environment: A systematic review, Inf. Softw. Technol. 103 (2018) 142–158.

[55] M.H. Rehmani, Y. Saleem, Network simulator NS-2, in: Encyclopedia of Information Science and Technology, Third Edition, IGI Global, 2015, pp. 6249–6258.

[56] A. Núñez, et al., SIMCAN: A flexible, scalable and expandable simulation platform for modelling and simulating distributed architectures and applications, Simul. Model. Pract. Theory 20 (1) (2012) 12–32.

[57] A. Buss, Component based simulation modeling with simkit, in: Proceedings of the Winter Simulation Conference, 1, IEEE, 2002, pp. 243–249.

[58] D. Kliazovich, P. Bouvry, S.U. Khan, GreenCloud: a packet-level simulator of energy-aware cloud computing data centers, J. Supercomput. 62 (3) (2012) 1263–1283.

[59] A. Núñez, et al., ICanCloud: A flexible and scalable cloud infrastructure simulator, J. Grid Comput. 10 (1) (2012) 185–209.

[60] U.U. Rehman, et al., Seccloudsim: Secure cloud simulator, in: 2014 12th International Conference on Frontiers of Information Technology, IEEE, 2014, pp. 208–213.

[61] I. Sriram, SPECI, a simulation tool exploring cloud-scale data centres, in: IEEE International Conference on Cloud Computing, Springer, 2009, pp. 381–392.

[62] M. Tighe, G. Keller, M. Bauer, H. Lutfiyya, Dcsim: A data centre simulation tool for evaluating dynamic virtualized resource management, in: 2012 8th International Conference on Network and Service Management (Cnsm) and 2012 Workshop on Systems Virtualiztion Management (Svm), IEEE, 2012, pp. 385–392.

[63] S. Ostermann, K. Plankensteiner, R. Prodan, T. Fahringer, Groudsim: An event-based simulation framework for computational grids and clouds, in: European Conference on Parallel Processing, Springer, 2010, pp. 305–313.

[64] H. Daga, H. Yoon, K. Bhardwaj, H. Gupta, A. Gavrilovska, From back-of-the-envelope to informed estimation of edge computing benefits in minutes using castnet, in: 2019 IEEE International Conference on Fog Computing (ICFC), IEEE, 2019, pp. 165–174.

[65] OpenQRM, OpenQRM, https://openqrm-enterprise.com/, accessed on 04.04.2024.

[66] A. Markus, A. Kertesz, Investigating IoT application behaviour in simulated fog environments, in: Cloud Computing and Services Science: 10th International Conference, CLOSER 2020, Prague, Czech Republic, May 7–9, 2020, Revised Selected Papers 10, Springer, 2021, pp. 258–276.

[67] A. Markus, A. Kertesz, G. Kecskemeti, Cost-aware iot extension of dissect-cf, Future Internet 9 (3) (2017) 47.

[68] Eucalyptus, Eucalyptus, https://www.eucalyptus.cloud/, Accessed on 04.04.2024.

[69] A. Coutinho, F. Greve, C. Prazeres, J. Cardoso, Fogbed: A rapid-prototyping emulation environment for fog computing, in: 2018 IEEE International Conference on Communications (ICC), IEEE, 2018, pp. 1–7.

[70] S. Sotiriadis, N. Bessis, N. Antonopoulos, A. Anjum, Simic: Designing a new inter-cloud simulation platform for integrating large-scale resource management, in: 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA), IEEE, 2013, pp. 90–97.

[71] A. Brogi, S. Forti, Qos-aware deployment of IoT applications through the fog, IEEE Internet Things J. 4 (5) (2017) 1185–1192.

[72] A. Brogi, S. Forti, A. Ibrahim, How to best deploy your fog applications, probably, in: 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC), IEEE, 2017, pp. 105–114.

[73] S.K. Gupta, et al., GDCSim: A tool for analyzing green data center design and resource management techniques, in: 2011 International Green Computing Conference and Workshops, 2011, pp. 1–8, http://dx.doi.org/10.1109/IGCC.2011.6008612.

[74] T. Platform, TCS Enterprise Cloud Platform, https://www.tcs.com/content/dam/tcs/pdf/Services/cloud-infrastructure/solutions/tcs-enterprise-cloud-paas.pdf, accessed on 04.04.2024.

[75] xCAT, xCAT, https://xcat.org/, accessed on 04.04.2024.

[76] H.P. Sajjad, K. Danniswara, A. Al-Shishtawy, V. Vlassov, Spanedge: Towards unifying stream processing over central and near-the-edge data centers, in: 2016 IEEE/ACM Symposium on Edge Computing (SEC), IEEE, 2016, pp. 168–178.

[77] M. Scarpiniti, E. Baccarelli, A. Momenzadeh, VirtFogSim: A parallel toolbox for dynamic energy-delay performance testing and optimization of 5G mobile-fog-cloud virtualized platforms, Appl. Sci. 9 (6) (2019) 1160.

[78] I. Lera, C. Guerrero, C. Juiz, YAFS: A simulator for IoT scenarios in fog computing, IEEE Access 7 (2019) 91745–91758.

[79] Q. Xu, J. Zhang, PiFogBed: a fog computing testbed based on raspberry pi, in: 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC), IEEE, 2019, pp. 1–8.

[80] Q. Xu, J. Zhang, B. Togookhuu, Support mobile fog computing test in piFogBedII, Sensors 20 (7) (2020) 1900.

[81] J. Hasenburg, M. Grambow, E. Grünewald, S. Huk, D. Bermbach, Mockfog: Emulating fog computing infrastructure in the cloud, in: 2019 IEEE International Conference on Fog Computing (ICFC), IEEE, 2019, pp. 144–152.

[82] J. Hasenburg, M. Grambow, D. Bermbach, MockFog 2.0: Automated execution of fog application experiments in the cloud, IEEE Trans. Cloud Comput. 11 (1) (2023) 58–70, http://dx.doi.org/10.1109/TCC.2021.3074988.

[83] S. Forti, A. Pagiaro, A. Brogi, Simulating fogdirector application management, Simul. Model. Pract. Theory 101 (2020) 102021.

[84] J. Hasenburg, S. Werner, D. Bermbach, FogExplorer, in: Proceedings of the 19th International Middleware Conference (Posters), 2018, pp. 1–2.

[85] N. Mohan, J. Kangasharju, Edge-fog cloud: A distributed cloud for internet of things computations, in: 2016 Cloudification of the Internet of Things (CIoT), IEEE, 2016, pp. 1–6.

[86] Z. Nikdel, B. Gao, S.W. Neville, DockerSim: Full-stack simulation of container-based Software-as-a-Service (SaaS) cloud deployments and environments, in: 2017 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM), IEEE, 2017, pp. 1–6.

[87] apache, https://vcl.apache.org/, accessed on 04.04.2024.

[88] R. Bolze, et al., Grid'5000: a large scale and highly reconfigurable experimental grid testbed, Int. J. High Perform. Comput. Appl. 20 (4) (2006) 481–494.

[89] H. Casanova, A. Giersch, A. Legrand, M. Quinson, F. Suter, Versatile, scalable, and accurate simulation of distributed applications and platforms, J. Parallel Distrib. Comput. 74 (10) (2014) 2899–2917.

[90] E. Del-Pozo-Puñal, F. García-Carballeira, D. Camarmas-Alonso, A scalable simulator for cloud, fog and edge computing platforms with mobility support, Future Gener. Comput. Syst. 144 (2023) 117–130.

[91] chameleoncloud, https://www.chameleoncloud.org/, accessed on 04.04.2024.

[92] N. Project, Nimbus Project, https://www.nimbusproject.org/, accessed on 04.04.2024.

[93] cloudlab, https://www.cloudlab.us/, accessed on 04.04.2024.

[94] V. Koukis, C. Venetsanopoulos, N. Koziris, ˜ okeanos: Building a cloud, cluster by cluster, IEEE Internet Comput. 17 (3) (2013) 67–71.

[95] fed4fire, https://www.fed4fire.eu/, accessed on 04.04.2024.

[96] R.H. Campbell, et al., Open cirrus™ cloud computing testbed: Federated data centers for open source systems and services research, HotCloud 9 (2009) 1–1.

[97] R. Grossman, Y. Gu, M. Sabala, C. Bennet, J. Seidman, J. Mambratti, The open cloud testbed: A wide area testbed for cloud computing utilizing high performance network services, 2009, arXiv preprint arXiv:0907.4810.

[98] iot lab, https://www.iot-lab.info, accessed on 04.04.2024.

[99] J.-M. Kang, H. Bannazadeh, A. Leon-Garcia, Savi testbed: Control and management of converged virtual ict resources, in: 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), IEEE, 2013, pp. 664–667.

[100] S. project, Security and Privacy Heterogeneous Environment for Reproducible Experimentation, https://sphere-project.net/, accessed on 04.04.2024.

[101] Abiquo, Abiquo, https://www.abiquo.com/, accessed on 04.04.2024.

[102] heroku, https://www.heroku.com/, accessed on 04.04.2024.

[103] A.M.C. Platform, Adtran Mosaic Cloud Platform, https://adtran.com/web/page/portal/Adtran/group/4560, accessed on 04.04.2024.

[104] I. Cloud, IBM Cloud, https://www.ibm.com/cloud, accessed on 04.04.2024.

[105] A. Cloud, Alibaba Cloud, https://eu.alibabacloud.com/en, accessed on 04.04.2024.

[106] G. Cloud, Google Cloud, https://cloud.google.com/, accessed on 04.04.2024.

[107] M. Tplatform, Metanet Tplatform, http://metanettplatform.com/, accessed on 04.04.2024.

[108] T. Cloud, Tencent Cloud, https://intl.cloud.tencent.com/, accessed on 04.04.2024.

[109] A. web services, Amazon Web Services, https://aws.amazon.com/, accessed on 04.04.2024.

[110] M. Azure, Microsoft Azure, https://azure.microsoft.com/, accessed on 04.04.2024.

[111] A. Cloudstack, Apache Cloudstack, https://cloudstack.apache.org/, accessed on 04.04.2024.

[112] Salesforce, Salesforce, https://www.salesforce.com/, accessed on 04.04.2024.

[113] C. Cloud, Cisco Cloud, https://www.cisco.com/c/en/us/solutions/cloud/index.html, accessed on 04.04.2024.

[114] rackspace, https://www.rackspace.com/, accessed on 04.04.2024.

[115] cloudfoundry, https://www.cloudfoundry.org/, accessed on 04.04.2024.

[116] O. Cloud, Oracle Cloud, https://www.oracle.com/cloud/, accessed on 04.04.2024.

[117] DataDog, DataDog, https://www.datadoghq.com/, accessed on 04.04.2024.

[118] W. Cloud, VMware Cloud, https://www.vmware.com/, accessed on 04.04.2024.

[119] D. Ocean, Digital Ocean, https://www.digitalocean.com/, accessed on 04.04.2024.

[120] S. Cloud, SAP Cloud, https://www.sap.com/products/cloud-platform.html, accessed on 04.04.2024.

[121] Z. Cai, Q. Li, X. Li, Elasticsim: A toolkit for simulating workflows with cloud resource runtime auto-scaling and stochastic task execution times, J. Grid Comput. 15 (2) (2017) 257–272.

[122] P. Kathiravelu, L. Veiga, Concurrent and distributed CloudSim simulations, in: 2014 IEEE 22nd International Symposium on Modelling, Analysis Simulation of Computer and Telecommunication Systems, 2014, pp. 490–493, http://dx.doi.org/10.1109/MASCOTS.2014.70.

[123] R.N. Calheiros, M.A. Netto, C.A. De Rose, R. Buyya, EMUSIM: an integrated emulation and simulation environment for modeling, evaluation, and validation of performance of cloud computing applications, Softw. - Pract. Exp. 43 (5) (2013) 595–612.

[124] J. Son, A.V. Dastjerdi, R.N. Calheiros, X. Ji, Y. Yoon, R. Buyya, Cloudsimsdn: Modeling and simulation of software-defined cloud data centers, in: 2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, IEEE, 2015, pp. 475–484.

[125] W.A. Higashino, M.A. Capretz, L.F. Bittencourt, CEPSim: Modelling and simulation of complex event processing systems in cloud environments, Future Gener. Comput. Syst. 65 (2016) 122–139.

[126] A. Kohne, M. Spohr, L. Nagel, O. Spinczyk, FederatedCloudSim: a SLA-aware federated cloud simulation framework, in: Proceedings of the 2nd International Workshop on CrossCloud Systems, 2014, pp. 1–5.

[127] A. Zhou, S. Wang, Q. Sun, H. Zou, F. Yang, FtCloudSim: A simulation tool for cloud service reliability enhancement mechanisms, in: Proceedings Demo & Poster Track of ACM/IFIP/USENIX International Middleware Conference, 2013, pp. 1–2.

[128] F. Fittkau, S. Frey, W. Hasselbring, Cdosim: Simulating cloud deployment options for software migration support, in: 2012 IEEE 6th International Workshop on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA), IEEE, 2012, pp. 37–46.

[129] X. Zeng, et al., IoTSim: A cloud based simulator for analysing IoT applications, 2016, arXiv preprint arXiv:1602.06488.

[130] B. Wickremasinghe, R.N. Calheiros, R. Buyya, Cloudanalyst: A cloudsim-based visual modeller for analysing cloud computing environments and applications, in: 2010 24th IEEE International Conference on Advanced Information Networking and Applications, IEEE, 2010, pp. 446–452.

[131] Y. Jararweh, et al., CloudExp: A comprehensive cloud computing experimental framework, Simul. Model. Pract. Theory 49 (2014) 180–192.

[132] J. Jung, H. Kim, MR-CloudSim: Designing and implementing MapReduce computing model on CloudSim, in: 2012 International Conference on ICT Convergence (ICTC), IEEE, 2012, pp. 504–509.

[133] T.T. Sá, et al., CloudReports: An extensible simulation tool for energy-aware cloud computing environments, in: Cloud Computing, Springer, 2014, pp. 127–142.

[134] W. Lin, S. Xu, L. He, J. Li, Multi-resource scheduling and power simulation for cloud computing, Inform. Sci. 397 (2017) 168–186.

[135] S.K. Garg, R. Buyya, Networkcloudsim: Modelling parallel applications in cloud simulations, in: 2011 Fourth IEEE International Conference on Utility and Cloud Computing, IEEE, 2011, pp. 105–113.

[136] CLoudSimEx, https://github.com/Cloudslab/CloudSimEx, accessed on 04.04.2024.

[137] X. Li, X. Jiang, P. Huang, K. Ye, DartCSim: An enhanced user-friendly cloud simulation system based on CloudSim with better performance, in: 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, 1, IEEE, 2012, pp. 392–396.

[138] N. Jain, N. Grozev, J. Lakshmi, R. Buyya, PriDynSim a simulator for dynamic priority based I/O scheduling for cloud applications, in: 2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), IEEE, 2015, pp. 8–15.

[139] X. Li, X. Jiang, K. Ye, P. Huang, DartCSim+: Enhanced cloudsim with the power and network models integrated, in: 2013 IEEE Sixth International Conference on Cloud Computing, IEEE, 2013, pp. 644–651.

[140] Y. Jararweh, et al., Teachcloud: a cloud computing educational toolkit, Int. J. Cloud Comput. 12 (2–3) (2013) 237–257.

[141] M. Bux, U. Leser, Dynamiccloudsim: Simulating heterogeneity in computational clouds, Future Gener. Comput. Syst. 46 (2015) 85–99.

[142] M.H. Sqalli, et al., Ucloud: A simulated hybrid cloud for a university environment, in: 2012 IEEE 1st International Conference on Cloud Networking (CLOUDNET), 2012, pp. 170–172, http://dx.doi.org/10.1109/CloudNet.2012.6483678.

[143] W. Chen, E. Deelman, Workflowsim: A toolkit for simulating scientific workflows in distributed environments, in: 2012 IEEE 8th International Conference on E-Science, IEEE, 2012, pp. 1–8.

[144] M. Seufert, B.K. Kwam, F. Wamser, P. Tran-Gia, Edgenetworkcloudsim: Placement of service chains in edge clouds using networkcloudsim, in: 2017 IEEE Conference on Network Softwarization (NetSoft), IEEE, 2017, pp. 1–6.

[145] X. Liu, L. Fan, J. Xu, X. Li, L. Gong, J. Grundy, Y. Yang, FogWorkflowSim: An automated simulation toolkit for workflow performance evaluation in fog computing, in: 2019 34th IEEE/ACM International Conference on Automated Software Engineering (ASE), IEEE, 2019, pp. 1114–1117.

[146] C. Puliafito, D.M. Gonçalves, M.M. Lopes, L.L. Martins, E. Madeira, E. Mingozzi, O. Rana, L.F. Bittencourt, MobFogSim: Simulation of mobility and migration for fog computing, Simul. Model. Pract. Theory 101 (2020) 102062.

[147] M.M. Lopes, W.A. Higashino, M.A. Capretz, L.F. Bittencourt, Myifogsim: A simulator for virtual machine migration in fog computing, in: Companion Proceedings of The10th International Conference on Utility and Cloud Computing, 2017, pp. 47–52.

[148] Q. Wang, Pfogsim: A Simulator for Evaluating Dynamic and Layered Fog Computing Environments (Ph.D. thesis), Auburn University, 2019.

[149] S.-H. Lim, et al., MDCSim: A multi-tier data center simulation, platform, in: 2009 IEEE International Conference on Cluster Computing and Workshops, IEEE, 2009, pp. 1–9.

[150] M.C. Silva Filho, R.L. Oliveira, C.C. Monteiro, P.R. Inácio, M.M. Freire, CloudSim plus: a cloud computing simulation framework pursuing software engineering principles for improved modularity, extensibility and correctness, in: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), IEEE, 2017, pp. 400–406.

[151] W. Tian, et al., A toolkit for modeling and simulation of real-time virtual machine allocation in a cloud data center, IEEE Trans. Autom. Sci. Eng. 12 (1) (2013) 153–161.

[152] cactosim, https://cordis.europa.eu/project/id/610711, accessed on 04.04.2024.

[153] C.K. Filelis-Papadopoulos, G.A. Gravvanis, P.E. Kyziropoulos, A framework for simulating large scale cloud infrastructures, Future Gener. Comput. Syst. 79 (2018) 703–714.

[154] OpenNebula, Opennebula, https://opennebula.io/, accessed on 04.04.2024.

[155] G. Kecskemeti, DISSECT-CF: a simulator to foster energy-aware scheduling in infrastructure clouds, Simul. Model. Pract. Theory 58 (2015) 188–218.

[156] openstack, OpenStack, https://www.openstack.org/, accessed on 04.04.2024.

[157] R. Mayer, L. Graser, H. Gupta, E. Saurez, U. Ramachandran, Emufog: Extensible and scalable emulation of large-scale fog computing infrastructures, in: 2017 IEEE Fog World Congress (FWC), IEEE, 2017, pp. 1–6.

[158] D. Fernández-Cerero, et al., Security supportive energy-aware scheduling and energy policies for cloud environments, J. Parallel Distrib. Comput. 119 (2018) 191–202.

[159] T. Qayyum, et al., FogNetSim++: A toolkit for modeling and simulation of distributed fog environment, IEEE Access 6 (2018) 63570–63583.

[160] J. Mass, S.N. Srirama, C. Chang, STEP-ONE: simulated testbed for edge-fog processes based on the opportunistic network environment simulator, J. Syst. Softw. 166 (2020) 110587.

[161] S. Tuli, R. Mahmud, S. Tuli, R. Buyya, Fogbus: A blockchain-based lightweight framework for edge and fog computing, J. Syst. Softw. 154 (2019) 22–36.

[162] R. Buyya, R. Ranjan, R.N. Calheiros, Modeling and simulation of scalable cloud computing environments and the CloudSim toolkit: Challenges and opportunities, in: 2009 International Conference on High Performance Computing & Simulation, IEEE, 2009, pp. 1–11.

[163] H. Gupta, A. Vahid Dastjerdi, S.K. Ghosh, R. Buyya, IFogSim: A toolkit for modeling and simulation of resource management techniques in the internet of things, edge and fog computing environments, Softw. - Pract. Exp. 47 (9) (2017) 1275–1296.

[164] C. Sonmez, A. Ozgovde, C. Ersoy, Edgecloudsim: An environment for performance evaluation of edge computing systems, Trans. Emerg. Telecommun. Technol. 29 (11) (2018) e3493.

[165] C. Mechalikh, H. Taktak, F. Moussa, PureEdgeSim: A simulation toolkit for performance evaluation of cloud, fog, and pure edge computing environments, in: 2019 International Conference on High Performance Computing & Simulation (HPCS), IEEE, 2019, pp. 700–707.

[166] S. Jain, D.K. Srivastava, Testing as a service (TaaS) on cloud: needs and challenges, Int. J. Adv. Res. Comput. Sci. Technol. 2 (2) (2014) 335–340.

[167] A. Ibrahim, V. Ford, Observations, evaluations, and recommendations for DETERLab from an educational perspective, J. Cybersecur. Educ. Res. Pract. 2021 (1) (2021).

[168] Q. Duan, Cloud service performance evaluation: status, challenges, and opportunities–a survey from the system modeling perspective, Digit. Commun. Netw. 3 (2) (2017) 101–111.

[169] V. Kampourakis, V. Gkioulos, S. Katsikas, A systematic literature review on wireless security testbeds in the cyber-physical realm, Comput. Secur. (2023) 103383.

[170] P.V. Wadatkar, R.G. Garroppo, G. Nencioni, 5G-MEC testbeds for V2X applications, Future Internet 15 (5) (2023) 175.

[171] Bluetooth, Bluetooth, https://www.bluetooth.com/, accessed on 04.04.2024.

[172] IEEE, IEEE Standard for Low-Rate Wireless Networks, IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015), 2020, pp. 1–800, http://dx.doi.org/10.1109/IEEESTD.2020.9144691.

[173] C.S. Alliance, Connectivity Standards Alliance, https://csa-iot.org/, accessed on 04.04.2024.

[174] U. Alliance, UWB Alliance, https://uwballiance.org/, accessed on 04.04.2024.

[175] L. Alliance, LoRa Alliance, https://lora-alliance.org/, accessed on 04.04.2024.

[176] ETSI, ETSI, https://www.etsi.org/technologies/mobile/5g, accessed on 04.04.2024.

[177] A. Pal, K. Kant, NFMI: Connectivity for short-range IoT applications, Computer 52 (2) (2019) 63–67, http://dx.doi.org/10.1109/MC.2019.2892862.

[178] M. Alliance, Mioty Alliance, https://mioty-alliance.com/, accessed on 04.04.2024.

[179] W. Alliance, WiFi Alliance, https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-halow, accessed on 04.04.2024.

[180] J. Kaur, M.A. Khan, Sixth generation (6G) wireless technology: An overview, vision, challenges and use cases, in: 2022 IEEE Region 10 Symposium (TENSYMP), 2022, pp. 1–6, http://dx.doi.org/10.1109/TENSYMP54529.2022.9864388.

[181] E. Khorov, I. Levitsky, I.F. Akyildiz, Current status and directions of IEEE 802.11be, the future wi-fi 7, IEEE Access 8 (2020) 88664–88688, http://dx.doi.org/10.1109/ACCESS.2020.2993448.

[182] A.A. Madankar, A. Khobragade, A review paper on milli-meter wave communications, in: 2022 6th International Conference on Electronics, Communication and Aerospace Technology, 2022, pp. 194–201, http://dx.doi.org/10.1109/ICECA55336.2022.10009475.

[183] M. Iskander, Z. Yun, Propagation prediction models for wireless communication systems, IEEE Trans. Microw. Theory Tech. 50 (3) (2002) 662–673, http://dx.doi.org/10.1109/22.989951.

[184] C.F. Yang, A ray-tracing method for modeling indoor wave propa- gation and penetration, IEEE Trans. Antennas and Propagation 46 (6) (1998) 907–919.

[185] Z. Sandor, L. Nagy, Z. Szabo, T. Csaba, 3D ray launching and moment method for indoor radio propagation purposes, in: 8th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 1, 1997, pp. 130–134.

[186] J.W. Schuster, R.J. Luebbers, Comparison of GTD and FDTD predictions for UHF radio wave propagation in a simple outdoor urban environment, in: IEEE Antennas Propag. Soc. Int. Symp., 3, 1997, pp. 2022–2025.

[187] A.W. Reza, M.S. Sarker, K. Dimyati, A novel integrated mathematical approach of ray-tracing and genetic algorithm for optimizing indoor wireless coverage, Prog. Electromagn. Res. -Pier 110 (2010) 147–162.

[188] L. Azpilicueta, P. López-Iturri, E. Aguirre, F. Falcone, Characterisation of radio wave propagation in complex indoor environments with and accurate ray launching and UTD method, in: 2016 10th European Conference on Antennas and Propagation (EuCAP), 2016, pp. 1–4, http://dx.doi.org/10.1109/EuCAP.2016.7481193.

[189] Z. Chang, S. Liu, X. Xiong, Z. Cai, G. Tu, A survey of recent advances in edge-computing-powered artificial Intelligence of Things, IEEE Internet Things J. (2021).

[190] T. Singh, R. Vaid, A. Sharma, Security issues in blockchain integrated WSN: Challenges and concerns, in: 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), 2022, pp. 1–5, http://dx.doi.org/10.1109/ICSES55317.2022.9914006.

[191] A.Z. Abyaneh, N. Zorba, B. Hamdaoui, IEEE 802.11ax based medium access design for wireless IoT-blockchain networks, in: GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1–6, http://dx.doi.org/10.1109/GLOBECOM42002.2020.9348079.

[192] V. Roopa, H. Shekhar Pradhan, Blockchain based spectrum sensing for secured cognitive radio wireless networks, in: 2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT), 2022, pp. 553–559, http://dx.doi.org/10.1109/CSNT54456.2022.9787585.

[193] Y. Zhou, et al., Blockchain for 5G advanced wireless networks, in: 2022 International Wireless Communications and Mobile Computing (IWCMC), 2022, pp. 1306–1310, http://dx.doi.org/10.1109/IWCMC55113.2022.9825182.

[194] S. Lee, J. Lee, Wireless blockchains: Trade-offs and future challenges, in: 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), 2022, pp. 2195–2197, http://dx.doi.org/10.1109/ICTC55196.2022.9952875.

[195] A. Sharma, Microsoft cloud outage hits users around the world, 2023, https://www.reuters.com/article/microsoft-outages-idTRNIKBN2U40BQ.

[196] Google, Incident affecting google cloud networking, cloud load balancing, traffic director, virtual private cloud (VPC), 2022, https://status.cloud.google.com/incidents/LuGcJVjNTeC5Sb9pSJ9o.

[197] K. Johnson, S. Rhea, Cloudflare outage on june 21, 2022, 2023, https://blog.cloudflare.com/cloudflare-incident-on-january-24th-2023/.

[198] E. Gabay, Attachme: critical OCI vulnerability allows unauthorized access to customer cloud storage volumes, 2022, https://www.wiz.io/blog/attachme-oracle-cloud-vulnerability-allows-unauthorized-cross-tenant-volume-access.

[199] T.O.C. Vulnerability, S.I. Database, The Open Cloud Vulnerability and Security Issue Database, https://www.cloudvulndb.org/, accessed on 04.04.2024.

[200] D. Kouril, et al., Cloud-based testbed for simulation of cyber attacks, in: 2014 IEEE Network Operations and Management Symposium (NOMS), IEEE, 2014, pp. 1–6.

[201] T. Jirsík, M. Husák, P. Celeda, Z. Eichler, Cloud-based security research testbed: A DDoS use case, in: 2014 IEEE Network Operations and Management Symposium (NOMS), IEEE, 2014, pp. 1–2.

[202] A. Tekeoglu, A.c. Tosun, A testbed for security and privacy analysis of IoT devices, in: 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), IEEE, 2016, pp. 343–348.

[203] M. Frank, M. Leitner, T. Pahi, Design considerations for cyber security testbeds: A case study on a cyber security testbed for education, in: 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), IEEE, 2017, pp. 38–46.

[204] A. Dhanapal, P. Nithyanandam, An OpenStack based cloud testbed framework for evaluating HTTP flooding attacks, Wirel. Netw. 27 (8) (2021) 5491–5501.

[205] M.M. Yamin, B. Katt, V. Gkioulos, Cyber ranges and security testbeds: Scenarios, functions, tools and architecture, Comput. Secur. 88 (2020) 101636.

[206] M. Conti, D. Donadel, F. Turrin, A survey on industrial control system testbeds and datasets for security research, IEEE Commun. Surv. Tutor. 23 (4) (2021) 2248–2294.

[207] L. Martignoni, R. Paleari, D. Bruschi, A framework for behavior-based malware analysis in the cloud, in: Information Systems Security: 5th International Conference, ICISS 2009 Kolkata, India, December 14-18, 2009 Proceedings 5, Springer, 2009, pp. 178–192.

[208] X. Wang, Y. Yang, Y. Zeng, Accurate mobile malware detection and classification in the cloud, SpringerPlus 4 (1) (2015) 1–23.

[209] H. Zhang, et al., Scanme mobile: a cloud-based android malware analysis service, ACM SIGAPP Appl. Comput. Rev. 16 (1) (2016) 36–49.

[210] D. Deyannis, E. Papadogiannaki, G. Kalivianakis, G. Vasiliadis, S. Ioannidis, Trustav: Practical and privacy preserving malware analysis in the cloud, in: Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy, CODASPY '20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 39–48.

[211] F. Minna, F. Massacci, An open-source cloud testbed for security experimentation, in: 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid), IEEE, 2022, pp. 756–759.

[212] A. Chowdhary, et al., Science DMZ: SDN based secured cloud testbed, in: 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2017, pp. 1–2, http://dx.doi.org/10.1109/NFV-SDN.2017.8169868.

[213] P. Kamongi, S. Kotikela, K. Kavi, M. Gomathisankaran, A. Singhal, Vulcan: Vulnerability assessment framework for cloud computing, in: 2013 IEEE 7th International Conference on Software Security and Reliability, IEEE, 2013, pp. 218–226.

[214] G. Zhu, Y. Yin, R. Cai, K. Li, Detecting virtualization specific vulnerabilities in cloud computing environment, in: 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), IEEE, 2017, pp. 743–748.

[215] S. An, et al., Cloudsafe: A tool for an automated security analysis for cloud computing, in: 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2019, pp. 602–609.

[216] S. Kautish, R. A, A. Vidyarthi, SDMTA: Attack detection and mitigation mechanism for DDoS vulnerabilities in hybrid cloud environment, IEEE Trans. Ind. Inform. 18 (9) (2022) 6455–6463, http://dx.doi.org/10.1109/TII.2022.3146290.

[217] P. Institute, Bridging the digital transformation divide: Leaders must balance security & growth, 2018, https://www.ibm.com/account/reg/us-en/signup?formid=urx-30589.

[218] S. Manepalli, Building end-to-end AWS DevSecOps CI/CD pipeline with open source SCA, SAST and DAST tools, 2021, https://aws.amazon.com/es/blogs/devops/building-end-to-end-aws-devsecops-ci-cd-pipeline-with-open-source-sca-sast-and-dast-tools/.

[219] J. Kindervag, et al., Build security into your network's dna: The zero trust network architecture, Forrester Res. Inc. 27 (2010).

[220] S. Mehraj, M.T. Banday, Establishing a zero trust strategy in cloud computing environment, in: 2020 International Conference on Computer Communication and Informatics (ICCCI), IEEE, 2020, pp. 1–6.

[221] L. Ferretti, F. Magnanini, M. Andreolini, M. Colajanni, Survivable zero trust for cloud computing environments, Comput. Secur. 110 (2021) 102419.

[222] F. Casino, et al., SoK: cross-border criminal investigations and digital evidence, J. Cybersec. 8 (1) (2022) tyac014.

[223] S. Rose, O. Borchert, A. Mitchell, S. Connelly, Zero trust architecture NIST special publication 888-207, NIST (2020).

[224] C. Yates, DevOps isn't enough — your team needs to embrace FleetOps, 2020, https://thenextweb.com/news/devops-isnt-enough-your-team-needs-to-embrace-fleetops.

[225] K. Zhang, X. Zhou, Y. Chen, X. Wang, Y. Ruan, Sedic: Privacy-aware data intensive computing on hybrid clouds, in: Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS '11, Association for Computing Machinery, New York, NY, USA, 2011, pp. 515–526, http://dx.doi.org/10.1145/2046707.2046767.

[226] Z. Zhou, H. Zhang, X. Du, P. Li, X. Yu, Prometheus: Privacy-aware data retrieval on hybrid cloud, in: 2013 Proceedings IEEE INFOCOM, IEEE, 2013, pp. 2643–2651.

[227] E. Stefanov, E. Shi, Oblivistore: High performance oblivious cloud storage, in: 2013 IEEE Symposium on Security and Privacy, IEEE, 2013, pp. 253–267.

[228] X. Zhang, L.T. Yang, C. Liu, J. Chen, A scalable two-phase top-down specialization approach for data anonymization using mapreduce on cloud, IEEE Trans. Parallel Distrib. Syst. 25 (2) (2013) 363–373.

[229] W. Wang, L. Chen, Q. Zhang, Outsourcing high-dimensional healthcare data to cloud with personalized privacy preservation, Comput. Netw. 88 (2015) 136–148.

[230] M. Shen, B. Ma, L. Zhu, X. Du, K. Xu, Secure phrase search for intelligent processing of encrypted data in cloud-based IoT, IEEE Internet Things J. 6 (2) (2018) 1998–2008.

[231] T. Kanwal, A. Anjum, S.U. Malik, A. Khan, M.A. Khan, Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud, Comput. Stand. Interfaces 78 (2021) 103522.

[232] J. Gardiner, et al., Building a privacy testbed: Use cases and design considerations, in: Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021, Revised Selected Papers, Springer, 2022, pp. 185–193.

[233] E. Politou, E. Alepis, C. Patsakis, Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions, J. Cybersec. 4 (1) (2018) tyy001.

[234] E. Politou, F. Casino, E. Alepis, C. Patsakis, Blockchain mutability: Challenges and proposed solutions, IEEE Trans. Emerg. Top. Comput. (2019).

[235] R. Kumar, R. Goyal, On cloud security requirements, threats, vulnerabilities and countermeasures: A survey, Comp. Sci. Rev. 33 (2019) 1–48.

[236] K. Kritikos, K. Magoutis, M. Papoutsakis, S. Ioannidis, A survey on vulnerability assessment tools and databases for cloud-based web applications, Array 3 (2019) 100011.

[237] J.B. Hong, et al., Systematic identification of threats in the cloud: A survey, Comput. Netw. 150 (2019) 46–69.

[238] H. Tabrizchi, M. Kuchaki Rafsanjani, A survey on security challenges in cloud computing: issues, threats, and solutions, J. Supercomput. 76 (12) (2020) 9493–9532.

[239] R. El Sibai, N. Gemayel, J. Bou Abdo, J. Demerjian, A survey on access control mechanisms for cloud computing, Trans. Emerg. Telecommun. Technol. 31 (2) (2020) e3720.

[240] F.K. Parast, et al., Cloud computing security: A survey of service-based models, Comput. Secur. 114 (2022) 102580.

[241] A.S.H. Abdul-Qawy, N.M.S. Almurisi, S. Tadisetty, Classification of energy saving techniques for IoT-based heterogeneous wireless nodes, Procedia Comput. Sci. 171 (2020) 2590–2599, Third International Conference on Computing and Network Communications (CoCoNet'19).

[242] P. Maratha, K. Gupta, A comprehensive and systematized review of energy-efficient routing protocols in wireless sensor networks, Int. J. Comput. Appl. 44 (1) (2022) 83–100.

[243] M. Shafiq, et al., Systematic literature review on energy efficient routing schemes in WSN – A survey, Mob. Netw. Appl. 25 (2020) 882–895, http://dx.doi.org/10.1007/s11036-020-01523-5.

[244] A.S. Sadeq, et al., Conceptual framework for future WSN-MAC protocol to achieve energy consumption enhancement, Sensors 22 (6) (2022).

[245] D. Wohwe Sambo, et al., Optimized clustering algorithms for large wireless sensor networks: A review, Sensors 19 (2) (2019).

[246] M.F. Khan, R.K. Dwivedi, R. Kumar, Energy efficient data transmission in sensor cloud : A review, in: 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 308–313, http://dx.doi.org/10.1109/ICOEI.2019.8862759.

[247] H. Rahmani, et al., Next-generation IoT devices: Sustainable eco-friendly manufacturing, energy harvesting, and wireless connectivity, IEEE J. Microw. 3 (1) (2023) 237–255, http://dx.doi.org/10.1109/JMW.2022.3228683.

[248] I.A. Alimi, et al., Towards a sustainable green design for next-generation networks, Wirel. Pers. Commun. 121 (2021) 1123–1138.

[249] F.K. Shaikh, S. Zeadally, E. Exposito, Enabling technologies for green internet of things, IEEE Syst. J. 11 (2) (2017) 983–994, http://dx.doi.org/10.1109/JSYST.2015.2415194.

[250] A. Mughees, M. Tahir, M.A. Sheikh, A. Ahad, Towards energy efficient 5G networks using machine learning: Taxonomy, research challenges, and future research directions, IEEE Access 8 (2020) 187498–187522, http://dx.doi.org/10.1109/ACCESS.2020.3029903.

[251] D. López-Pérez, et al., A survey on 5G radio access network energy efficiency: Massive MIMO, lean carrier design, sleep modes, and machine learning, IEEE Commun. Surv. Tutor. 24 (1) (2022) 653–697, http://dx.doi.org/10.1109/COMST.2022.3142532.

[252] Z. Du, Y. Deng, W. Guo, A. Nallanathan, Q. Wu, Green deep reinforcement learning for radio resource management: Architecture, algorithm compression, and challenges, IEEE Veh. Technol. Mag. 16 (1) (2021) 29–39, http://dx.doi.org/10.1109/MVT.2020.3015184.

[253] J. Tang, R. Wen, T.Q.S. Quek, M. Peng, Fully exploiting cloud computing to achieve a green and flexible C-RAN, IEEE Commun. Mag. 55 (11) (2017) 40–46, http://dx.doi.org/10.1109/MCOM.2017.1600922.

[254] M. Abrar, et al., Energy efficient UAV-enabled mobile edge computing for IoT devices: A review, IEEE Access 9 (2021) 127779–127798, http://dx.doi.org/10.1109/ACCESS.2021.3112104.

[255] C. Ge, S. Qin, Digital twin intelligent transportation system (DT-ITS)—A systematic review, IET Intell. Transp. Syst. (2024).

[256] M.E. Rivero-Angeles, Quantum-based wireless sensor networks: A review and open questions, Int. J. Distrib. Sens. Netw. 17 (10) (2021).

[257] W. Xu, et al., Internet of vehicles in big data era, IEEE/CAA J. Autom. Sin. 5 (1) (2017) 19–35.

[258] J. Zhang, K.B. Letaief, Mobile edge intelligence and computing for the internet of vehicles, Proc. IEEE 108 (2) (2019) 246–261.

[259] M. Samir, et al., UAV trajectory planning for data collection from time-constrained IoT devices, IEEE Trans. Wireless Commun. 19 (1) (2019) 34–46.

[260] M.S. Murshed, et al., Machine learning at the network edge: A survey, ACM Comput. Surv. 54 (8) (2021) 1–37.

[261] N.S. Sworna, et al., Towards development of IoT-ML driven healthcare systems: A survey, J. Netw. Comput. Appl. (2021) 103244.

[262] N.A. Sulieman, L. Ricciardi Celsi, W. Li, A. Zomaya, M. Villari, Edge-oriented computing: A survey on research and use cases, Energies 15 (2) (2022) 452.

[263] D.C. Nguyen, et al., Federated learning for internet of things: A comprehensive survey, IEEE Commun. Surv. Tutor. (2021).

[264] A. Imteaj, et al., A survey on federated learning for resource-constrained iot devices, IEEE Internet Things J. 9 (1) (2021) 1–24.

[265] V. Kumar, S. Gunner, T. Spyridopoulos, A. Vafeas, J. Pope, P. Yadav, G. Oikonomou, T. Tryfonas, Challenges in the design and implementation of iot testbeds in smart-cities: A systematic review, 2023, arXiv preprint arXiv:2302.11009.

[266] Z. Zheng, Y. Zhou, Y. Sun, Z. Wang, B. Liu, K. Li, Applications of federated learning in smart cities: Recent advances, taxonomy, and open challenges, Connect. Sci. 34 (1) (2022) 1–28.

[267] J.C. Jiang, B. Kantarci, S. Oktug, T. Soyata, Federated learning in smart city sensing: Challenges and opportunities, Sensors 20 (21) (2020) 6230.

[268] J. Machin, E. Batista, A. Martínez-Ballesté, A. Solanas, Privacy and security in cognitive cities: A systematic review, Appl. Sci. 11 (10) (2021) 4471.

[269] S.S. Gill, et al., Transformative effects of IoT, blockchain and artificial intelligence on cloud computing: Evolution, vision, trends and open challenges, Internet of Things 8 (2019) 100118.

[270] J. Leng, M. Zhou, J.L. Zhao, Y. Huang, Y. Bian, Blockchain security: A survey of techniques and research directions, IEEE Trans. Serv. Comput. 15 (4) (2022) 2490–2510, http://dx.doi.org/10.1109/TSC.2020.3038641.

[271] W. Viriyasitavat, L.D. Xu, G. Dhiman, Z. Bi, Blockchain-as-a-service for business process management: Survey and challenges, IEEE Trans. Serv. Comput. (2022) 1–14, http://dx.doi.org/10.1109/TSC.2022.3199232.

[272] H. Zhou, et al., A blockchain based witness model for trustworthy cloud service level agreement enforcement, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, IEEE, 2019, pp. 1567–1575.

[273] R. Bianchini, et al., Toward ml-centric cloud platforms, Commun. ACM 63 (2) (2020) 50–59.

[274] S.H. Mohamed, T.E. El-Gorashi, J.M. Elmirghani, A survey of big data machine learning applications optimization in cloud data centers and networks, 2019, arXiv preprint arXiv:1910.00731.

[275] Z. Jalali Khalil Abadi, N. Mansouri, M.M. Javidi, Deep reinforcement learning-based scheduling in distributed systems: A critical review, Knowl. Inf. Syst. (2024) 1–74.

[276] I. John, A. Sreekantan, S. Bhatnagar, Efficient adaptive resource provisioning for cloud applications using reinforcement learning, in: 2019 IEEE 4th International Workshops on Foundations and Applications of Self* Systems (FAS* W), IEEE, 2019, pp. 271–272.

[277] Q. Zhang, et al., Dynamic heterogeneity-aware resource provisioning in the cloud, IEEE transactions on cloud computing 2 (1) (2014) 14–28.

[278] P. Nand, et al., Assessment of various scheduling and load balancing algorithms in integrated cloud-fog environment, Recent Adv. Comput. Sci. Commun. (Formerly: Recent Patents on Computer Science) 16 (2) (2023) 44–60.

[279] W. Song, et al., Adaptive resource provisioning for the cloud using online bin packing, IEEE Trans. Comput. 63 (11) (2013) 2647–2660.

[280] Z. Tang, Y. Mo, K. Li, K. Li, Dynamic forecast scheduling algorithm for virtual machine placement in cloud computing environment, J. Supercomput. 70 (3) (2014) 1279–1296.

[281] H. Zhao, J. Wang, F. Liu, Q. Wang, W. Zhang, Q. Zheng, Power-aware and performance-guaranteed virtual machine placement in the cloud, IEEE Trans. Parallel Distrib. Syst. 29 (6) (2018) 1385–1400.

[282] M. Masdari, A. Khoshnevis, A survey and classification of the workload forecasting methods in cloud computing, Cluster Comput. 23 (4) (2020) 2399–2424.

[283] M. Shahrad, et al., Serverless in the wild: Characterizing and optimizing the serverless workload at a large cloud provider, in: 2020 {USENIX} Annual Technical Conference ({*USENIX*}{*ATC*} 20), 2020, pp. 205–218.

[284] J. Kumar, A.K. Singh, Workload prediction in cloud using artificial neural network and adaptive differential evolution, Future Gener. Comput. Syst. 81 (2018) 41–52.

[285] Z.R. Alashhab, et al., Impact of coronavirus pandemic crisis on technologies and cloud computing applications, J. Electron. Sci. Technol. 19 (1) (2021) 100059.

[286] S. Mandal, D.A. Khan, A study of security threats in cloud: Passive impact of COVID-19 pandemic, in: 2020 International Conference on Smart Electronics and Communication (ICOSEC), IEEE, 2020, pp. 837–842.

[287] Gaia-x, https://www.gaia-x.eu/, accessed on 04.04.2024.

[288] R. Rezapour, P. Asghari, H.H.S. Javadi, S. Ghanbari, Security in fog computing: A systematic review on issues, challenges and solutions, Comp. Sci. Rev. 41 (2021) 100421.

[289] E. Cortez, A. Bonde, A. Muzio, M. Russinovich, M. Fontoura, R. Bianchini, Resource central: Understanding and predicting workloads for improved resource management in large cloud platforms, in: Proceedings of the 26th Symposium on Operating Systems Principles, 2017, pp. 153–167.

[290] T. Shi, H. Ma, G. Chen, A genetic-based approach to location-aware cloud service brokering in multi-cloud environment, in: 2019 IEEE International Conference on Services Computing (SCC), IEEE, 2019, pp. 146–153.

[291] W. Tang, Q. Wu, Evolutionary computation, in: Condition Monitoring and Assessment of Power Transformers using Computational Intelligence, Springer, 2011, pp. 15–36.

[292] J. Gao, Machine learning applications for data center optimization, Google White Paper (2014).

[293] S. Chen, C. Delimitrou, J.F. Martínez, Parties: Qos-aware resource partitioning for multiple interactive services, in: Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems, 2019, pp. 107–120.

[294] J. Rao, X. Bu, C.-Z. Xu, L. Wang, G. Yin, Vconf: a reinforcement learning approach to virtual machines auto-configuration, in: Proceedings of the 6th International Conference on Autonomic Computing, 2009, pp. 137–146.

[295] H. Mao, et al., Resource management with deep reinforcement learning, in: Proceedings of the 15th ACM Workshop on Hot Topics in Networks, 2016, pp. 50–56.
[296] T. Khan, W. Tian, R. Buyya, Machine learning (ML)-centric resource management in cloud computing: A review and future directions, 2021, arXiv: 2105.05079.
[297] A. Boudi, M. Bagaa, P. Pöyhönen, T. Taleb, H. Flinck, AI-based resource management in beyond 5G cloud native environment, IEEE Netw. 35 (2) (2021) 128–135, http://dx.doi.org/10.1109/MNET.011.2000392.
[298] M. AbdelBaky, et al., Computing in the continuum: Combining pervasive devices and services to support data-driven applications, in: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2017, pp. 1815–1824.
[299] W. Guo, et al., Cloud resource scheduling with deep reinforcement learning and imitation learning, IEEE Internet Things J. 8 (5) (2021) 3576–3586, http://dx.doi.org/10.1109/JIOT.2020.3025015.
[300] M. Cheng, J. Li, S. Nazarian, DRL-cloud: Deep reinforcement learning-based resource provisioning and task scheduling for cloud service providers, in: 2018 23rd Asia and South Pacific Design Automation Conference (ASP-DAC), 2018, pp. 129–134, http://dx.doi.org/10.1109/ASPDAC.2018.8297294.
[301] T. Dong, F. Xue, C. Xiao, J. Zhang, Deep reinforcement learning for dynamic workflow scheduling in cloud environment, in: 2021 IEEE International Conference on Services Computing (SCC), 2021, pp. 107–115, http://dx.doi.org/10.1109/SCC53864.2021.00023.
[302] Y. Huang, et al., Deep adversarial imitation reinforcement learning for QoS-aware cloud job scheduling, IEEE Syst. J. (2021) 1–11, http://dx.doi.org/10.1109/JSYST.2021.3122126.
[303] G. Zhou, W. Tian, R. Buyya, Deep reinforcement learning-based methods for resource scheduling in cloud computing: A review and future directions, 2021, arXiv:2105.04086.
[304] S. Ilager, R. Buyya, Energy and thermal-aware resource management of cloud data centres: A taxonomy and future directions, 2021, arXiv:2107.02342.
[305] S. Tuli, et al., HUNTER: AI based holistic resource management for sustainable cloud computing, J. Syst. Softw. 184 (2022) 111124.
[306] Y. Zhang, J. Yao, H. Guan, Intelligent cloud resource management with deep reinforcement learning, IEEE Cloud Comput. 4 (6) (2017) 60–69.
[307] D. Zeng, L. Gu, S. Pan, J. Cai, S. Guo, Resource management at the network edge: A deep reinforcement learning approach, IEEE Netw. 33 (3) (2019) 26–33.
[308] Y. He, et al., Blockchain-based edge computing resource allocation in IoT: A deep reinforcement learning approach, IEEE Internet Things J. 8 (4) (2021) 2226–2237, http://dx.doi.org/10.1109/JIOT.2020.3035437.
[309] C. Xu, K. Wang, M. Guo, Intelligent resource management in blockchain-based cloud datacenters, IEEE Cloud Comput. 4 (6) (2017) 50–59, http://dx.doi.org/10.1109/MCC.2018.1081060.
[310] K. Gai, J. Guo, L. Zhu, S. Yu, Blockchain meets cloud computing: A survey, IEEE Commun. Surv. Tutor. 22 (3) (2020) 2009–2030, http://dx.doi.org/10.1109/COMST.2020.2989392.
[311] H. Wang, et al., Blockchain-based resource allocation model in fog computing, Appl. Sci. 9 (24) (2019) http://dx.doi.org/10.3390/app9245538.
[312] Y. Jiao, et al., Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks, IEEE Trans. Parallel Distrib. Syst. 30 (9) (2019) 1975–1989, http://dx.doi.org/10.1109/TPDS.2019.2900238.
[313] Z. Li, L. O'brien, H. Zhang, R. Cai, On a catalogue of metrics for evaluating commercial cloud services, in: 2012 ACM/IEEE 13th International Conference on Grid Computing, IEEE, 2012, pp. 164–173.
[314] R. Han, L.K. John, J. Zhan, Benchmarking big data systems: A review, IEEE Trans. Serv. Comput. 11 (3) (2018) 580–597, http://dx.doi.org/10.1109/TSC.2017.2730882.
[315] S. Maheshwari, et al., Scalability and performance evaluation of edge cloud systems for latency constrained applications, in: 2018 IEEE/ACM Symposium on Edge Computing (SEC), IEEE, 2018, pp. 286–299.
[316] D. Saxena, R. Gupta, A.K. Singh, A survey and comparative study on multi-cloud architectures: emerging issues and challenges for cloud federation, 2021, arXiv preprint arXiv:2108.12831.
[317] C. Ramalingam, P. Mohan, Addressing semantics standards for cloud portability and interoperability in multi cloud environment, Symmetry 13 (2) (2021) 317.
[318] B. Rajeshwari, M. Dakshayini, H. Guruprasad, Workload balancing in a multi-cloud environment: Challenges and research directions, in: Operationalizing Multi-Cloud Environments, Springer, 2022, pp. 129–144.
[319] V. Bucur, L.-C. Miclea, Multi-cloud resource management techniques for cyber-physical systems, Sensors 21 (24) (2021) 8364.
[320] D.W. McKee, et al., The internet of simulation, a specialisation of the internet of things with simulation and workflow as a service (sim/wfaas), in: 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE), IEEE, 2017, pp. 47–56.
[321] European Commission, EU Cyber Resilience Act, 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en.
[322] L. Project, et al., Response of the EU-funded projects CC-DRIVER, CYBERSPACE, COPKIT, HEROES, INSPECTr, LOCARD, RAYUELA, ROXANNE, and TRACE as well as Trilateral Research and Coventry University to the EC consultation on a proposed Cyber Resilience Act, 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services/F3263826_en.
[323] M. Negreiro, The NIS2 directive, a high common level of cybersecurity in the EU, Eur. Parliam. Res. Serv. Eur. Parliam. PE 689 (2021).
[324] U. Congress, S.3600 - Strengthening American Cybersecurity Act of 2022, 2022, https://www.congress.gov/bill/117th-congress/senate-bill/3600/text.
[325] E.U.A. for Cybersecurity, ENISA Threat Landscape 2022, 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.
[326] F. Casino, et al., Research trends, challenges, and emerging topics in digital forensics: A review of reviews, IEEE Access (2022).
[327] European Commission, https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe, accessed on 04.04.2024.
[328] Eurostat, https://ec.europa.eu/eurostat/statistics-explained/pdfscache/37043.pdf, accessed on 04.04.2024.
[329] M.R. Dorsala, V. Sastry, S. Chapram, Blockchain-based solutions for cloud computing: A survey, J. Netw. Comput. Appl. 196 (2021) 103246.
[330] F. Casino, T.K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues, Telemat. Inform. 36 (2019) 55–81.
[331] S.M.H. Bamakan, et al., A survey of blockchain consensus algorithms performance evaluation criteria, Expert Syst. Appl. 154 (2020) 113385.
[332] L.M. Bach, B. Mihaljevic, M. Zagar, Comparative analysis of blockchain consensus algorithms, in: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, 2018, pp. 1545–1550.
[333] R. Qin, et al., Economic issues in bitcoin mining and blockchain research, in: 2018 IEEE Intelligent Vehicles Symposium, IV, IEEE, 2018, pp. 268–273.
[334] P. Ciaian, d. Kancs, M. Rajcaniova, Interdependencies between mining costs, mining rewards and blockchain security, 2021, arXiv preprint arXiv:2102.08107.

Fran Casino is a postdoctoral researcher at the Department of Computer Engineering and Mathematics at Rovira i Virgili University, Spain, and Athena Research Center, Greece. He obtained his B.Sc. degree in Computer Science and his M.Sc. in Computer Security and Intelligent Systems, both from URV. He holds a Ph.D. in Computer Science from URV with honours (A cum laude) and the best dissertation award. He completed several stays in international research institutions such as ISCTE-IUL and the University of Piraeus. His research has an interdisciplinary focus and combines several knowledge areas with disruptive technologies. Some keyword related to his research are pattern recognition, cognitive security, privacy protection cybercrime and digital investigations recommender systems supply chain and blockchain. He has authored more than 60 publications in peer-reviewed international conferences and journals. He was listed in the world's top 2% most influential scientists in his field by Stanford University.

Peio lopez-iturri received a degree in telecommunications engineering a master's degree in communications and a phD in communication engineering from the public university of navarre (UPNA), Pamplona, Navarre in 2011, 2012, and 2017, Respectively. in 2019, he partly worked as a researcher at tafco metawireless. He has worked on ten different public and privately funded research projects. he has over 150 contributions to internationally indexed journals, book chapters and conference contributions. Currently, he is affiliated with the institute for smart cities (ISC), UPNA. His research interests include radio propagation, wireless sensor networks, electromagnetic dosimetry, modelling of radio interference sources, mobile radio systems, wireless power transfer, IoT networks and devices, 5G communication systems and EMI/EMC.

Constantinos Patsakis holds a B.sc. in mathematics from the university of athens Greece and an M.sc. in information Security from Royal Holloway, University of London. He obtained his PhD in cyber security from the university of piraeus. His main research areas include cryptography, malware, security, privacy and cybercrime. He has participated in several national and European R&D projects. Additionally, he has worked as a researcher at the UNESCO Chair in data privacy, at Trinity college, Dublin, Ireland, and the Luxembourg Institute of Science and technology. Currently, he is an Associate Professor at the University of Piraeus and an adjunct researcher at Athena Research and Innovation centre.