sustainability

Article

Identifying Challenges for Clients in Adopting Sustainable Public Cloud Computing

Muhammad Janas Khan [1], Fasee Ullah [1,*], Muhammad Imran [2], Jahangir Khan [1], Arshad Khan [2], Ahmed S. AlGhamdi [3] and Sultan S. Alshamrani [3]

[1] Department of Computer Science & Informational Technology, Sarhad University of Science & Informational Technology, Peshawar 25120, Pakistan
[2] Institute of Computer Sciences and Information Technology (ICS/IT), The University of Agriculture, Peshawar 25120, Pakistan
[3] Department of Information Technology, College of Computer and Information Technology, Taif University, Taif 21944, Saudi Arabia
[*] Correspondence: faseekhan@gmail.com or fasee.csit@suit.edu.pk

Abstract: Sustainable Cloud Computing is the modern era's most popular technology. It is improving daily, offering billions of people sustainable services. Currently, three deployment models are available: (1) public, (2) private, and (3) hybrid cloud. Recently, each deployment model has undergone extensive research. However, relatively little work has been carried out regarding clients' adoption of sustainable public cloud computing (PCC). We are particularly interested in this area because PCC is widely used worldwide. As evident from the literature, there is no up-to-date systematic literature review (SLR) on the challenges clients confront in PCC. There is a gap that needs urgent attention in this area. We produced an SLR by examining the existing cloud computing models in this research. We concentrated on the challenges encountered by clients during user adoption of a sustainable PCC. We uncovered a total of 29 obstacles that clients confront when adopting sustainable PCC. In 2020, 18 of the 29 challenges were reported. This demonstrates the tremendous threat that PCC still faces. Nineteen of these are considered critical challenges to us. We consider a challenge a critical challenge if its occurrence in the final selected sample of the paper is greater than 20%. These challenges will negatively affect client adoption in PCC. Furthermore, we performed three different analyses on the critical challenges. Our analysis may indicate that these challenges are significant for all the continents. These challenges vary with the passage of time and with the venue of publication. Our results will assist the client's organization in understanding the issue. Furthermore, it will also help the vendor's organization determine the potential solutions to the highlighted challenges.

Keywords: sustainable public cloud computing; big data; challenges; systematic literature review

check for updates

Citation: Khan, M.J.; Ullah, F.; Imran, M.; Khan, J.; Khan, A.; AlGhamdi, A.S.; Alshamrani, S.S. Identifying Challenges for Clients in Adopting Sustainable Public Cloud Computing. *Sustainability* **2022**, *14*, 9809. https://doi.org/10.3390/su14169809

Academic Editors: Osama Sohaib, Muhammad Asif and Tin-Chih Toly Chen

Received: 17 April 2022
Accepted: 1 August 2022
Published: 9 August 2022

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

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

1. Introduction

Sustainable cloud computing (CC) is a developing technology [1,2]. The versatility, broad accessibility, and efficient process of computer assets are all unique properties of CC. A flexible paradigm gives different organizations various options regarding diverse resources [3,4]. It plays a key role in big data [2,3]. CC, according to the National Institute of Standards and Technology (NIST), is a method of providing ubiquitous, convenient, on-demand access to a network of shared fields of configurable computer resources (such as networks, servers, data warehouses, applications, and services) that can be quickly provided and delivered with minimal service provider involvement. That is, it controls a huge amount of data (Big data) by applying an efficient mechanism [5,6]. Various organizations benefit from its flexibility to adequately and reliably utilize big data and compete in the market. Because of CC, multiple businesses have grown [7–11].

CC is a significant area of interest in information technology (I.T.). It does not only offer flexibility and scalability [12]. However, it also has the advantages of being simple to use, having market access, saving time, and being cost-effective. Because of these benefits, businesses have turned to CC [13–15].

In recent years, the adoption of public cloud computing (PCC) has gained great significance in the industry and academia [16]. PCC is becoming more widely adopted worldwide because of its potential to deliver significant benefits to the industry and the community [17]. A contract-based arrangement between a cloud client(s) and a cloud vendor(s) constitutes a CC implementation. In such an agreement, the customer agrees to transfer some or all of their organization's digital assets to the cloud vendor [18], who provides agreed-upon services on a "pay-as-you-go" basis [19].

The public cloud (P.C.) infrastructure is available for the general public or a large-scale industrial organization selling the cloud services [20]. In the P.C., resources are available through the internet with the concept of pay-per-usage. Grace explained that the users could use the services on demand, for which they do not need to buy special hardware. The P.C. provides the services according to the required capacity of the users [21]. According to Peter et al., cloud services can be owned and distributed by a third-party company [22]. Its primary distributed source is the internet. It is designed so that everyone can use it easily [23]. Consumers of the P.C. are primarily residential users who can connect to the services using a shared internet connection [24]. Tim et al. argue that Google, Amazon, and Microsoft are the best examples of using the P.C. [25]. Oskar explained that users' data could be managed and stored on third-party vendor servers [26].

The advantages of PCC include the following [27]:

- Data availability;
- 24/7 technical expertise is provided;
- Scalability is on-demand;
- Easy and cost-efficient;
- No resource wastage.

The disadvantages of PCC include:

- Data security;
- Privacy.

In PCC, you may be unable to know about your data residency. One may be unable to know about the backup procedure of the data. Reliability can also be an issue with public cloud computing [28].

Even though much work has been carried out in PCC, very little in adoption has been carried out on the challenges clients face in adopting PCC. This work focuses on identifying challenges that clients face in adopting PCC.

2. Background

This section contains related public cloud computing research. We have described some of them as follows:

Ren et al. [29] outlined many key security concerns for commercial and P.C., but their list is far from complete. For example, although CC allows for almost unlimited compute capacity while lowering prices, the question of how to prevent hostile cloud users from exploiting cloud resources remains unsolved. Password/key cracking, malicious data hosting, and botnet command and control are examples of misuse. One method to address this risk is to adopt stricter monitoring of cloud resource utilization, which will inevitably conflict with legal users' privacy rights. As a result, more research is required.

Chakrawarti et al. [30] argued that storing data in an encrypted format is a typical data privacy protection method, but it exposes user data to the danger of unauthorized exposure. They presented a system that combines other identity management and accessed control technologies to improve enterprise P.C. authentication and security to address the problem.

Users can access the P.C. through the internet and cloud subscribers can undertake administrative tasks. This paradigm raises security vulnerabilities in and of itself because remote access exposes possible cyber attackers. While these flaws expand the threat landscape, other concerns constitute an equal, if not greater, security risk [31].

He et al. [32] state that health authorities may mishandle or exploit data obtained via digital mobile apps for long-term and other objectives. Many people are concerned about whether or not these COVID-19-fighting apps are safe to use, how they will protect privacy, and what regulations will be required to avoid abuse [33]. These worries will likely erode public trust and limit people's willingness to accept new technologies.

People's use of technological innovations, mainly providing their data to meet the issues posed by the COVID-19 pandemic, requires public confidence and trust. [32].

The P.C. also has some configuration, security, and SLA precision limits, making it less than ideal for services that use confidential material and are vulnerable to compliance rules [34].

According to Kaura et al. [35], users must relinquish control over various security-related issues to the cloud provider when using the P.C. The service agreements given by the service provider may not guarantee that the cloud provider will resolve a challenge that exposes security vulnerability.

Hlatshwayo and Zuva [36] argue that mobile cloud computing (MCC), as one of the future mobile technology developments, provides top services for mobile consumers by combining the advantages of both cloud computing and mobile computing. As more and more people become aware of the data on businesses and individuals being stored in the cloud, MPCC users' privacy and data integrity are concerns that must be addressed. Many cloud providers must deal with this issue.

Aslam et al. [37] discuss that V.M. migration, an essential function for cloud service providers, for various administrative reasons, poses several security risks, jeopardizing the cloud service's dependability. They established essential user requirements that serve as the foundation for our proposed V.M. Migration mechanism to solve this. They employed trusted platform module (TPM) capabilities to create a trusted credential (i.e., Trust Token) that ensures the security and trustworthiness of cloud platforms.

Baror et al. [38] argue that in document communications such as texts, emails, or instant chats, public cloud users (whether a possible victim of a cyberattack or a digital forensic investigator) intrinsically communicate using natural human language in the form of sentences and semantics. Their study uses natural human language as an identifier to establish a revolutionary digital forensic readiness (DFR) architecture for cloud computing to detect cybercrime. The DFR framework uses natural language processing techniques to create a mechanism that simulates a near real-time approach to cybercrime detection in the cloud. To construct a DFR framework, natural language understanding algorithms were employed to analyze text data from users in the public cloud and text data from reported cybercrimes. The suggested DFR framework can reduce the time it takes to identify cybercrimes on the public cloud and the time it takes to investigate them.

As a result, cloud users can be identified by their natural human language interaction.

Kaneko et al. [39] developed a V.M. scaling strategy for adjusting the number of V.M.s by forecasting unanticipated performance fluctuations. They tested the proposed method and found that it enhanced the message processing success rate by up to 15% compared to basic methods that do not account for unexpected performance fluctuations.

The related work suggests a few studies conducted in the PCC domain. The studies that are conducted have different approaches. Our focus is on the client-side aspects of PCC.

3. Research Methodology

The strong belief is that selecting the data collection method significantly impacts the analysis process [40]. So, this selection has been made very carefully. We chose the SLR and Questionnaire survey for the data collection to conduct this research. "A systematic literature review (SLR) is a means of identifying, evaluating, and interpreting all available research relevant to a particular research question, topic area, or phenomenon of interest. Individual studies contributing to a systematic review are called primary studies; a systematic review is a form of secondary study" [41]. According to Kitchenham and Charters [42], the critical steps of SLR are conducted in three stages, i.e., planning, conducting, and reporting [43,44].

3.1. Research Questions

The following research questions have been formulated to achieve our research objectives:

RQ1: What challenges, as acknowledged by the literature, are confronted by client organizations that decide to adopt public cloud computing?

RQ1.1: Do these challenges vary across continents?

RQ1.2: Do these challenges differ across publication years?

RQ1.3: Do these challenges differ across different publication venues?

Section 4 presents the answers to all the above questions.

3.2. Search Strategy

Initially, the following trail search was used to search in Google scholar. The papers accessed through the following search string were used for the final search term.

Trail Search string: ("cloud computing") AND (Challenges)

Synonyms and Boolean operations are used to construct the final search string. "AND" and "OR" are the key terms in this search string.

(("Public cloud" OR "Public cloud computing") AND ("Challenges" OR "risks" OR "barriers" OR "problems") AND ("Clients" OR "Users" OR "Customers")).

Different digital libraries have different interfaces, so we apply the above search string to each library. Irrespective of the date bound, we searched the available literature after constructing the search string. The following digital libraries are searched:

- IEEE explore: (https://ieeexplore.ieee.org)
- ACM Portal: (https://dl.acm.org)
- Springer Link: (www.springerlink.com)
- Science Direct: (www.sciencedirect.com)
- Cite Seer: (www.citeseer.ist.psu.edu)
- Google Scholar: (www.scholar.google.com)

3.3. Publication Selection

First, we reviewed the title, keyword, and abstract for the primary selection of the retrieved publications, as known in Table 1. After that, primarily selected papers' contents are probed by reading the complete text. As shown in Figure 1, inclusion and exclusion criteria were used for the publication quality assessment.

Table 1. Outcomes of the search string as per database.

Search String	Library	Initial Results	Initial Selection	Final Selection
(("Public cloud") AND ("Challenges OR risks OR barriers OR problems"))	IEEE Xplore	3044	75	32
	Springer Link	1164	42	15
	Science Direct	1576	39	14
	ACM	284	35	10
	Cite Seer	28	13	2
	Google Scholar	27,496	117	25
	Total	33,592	321	98

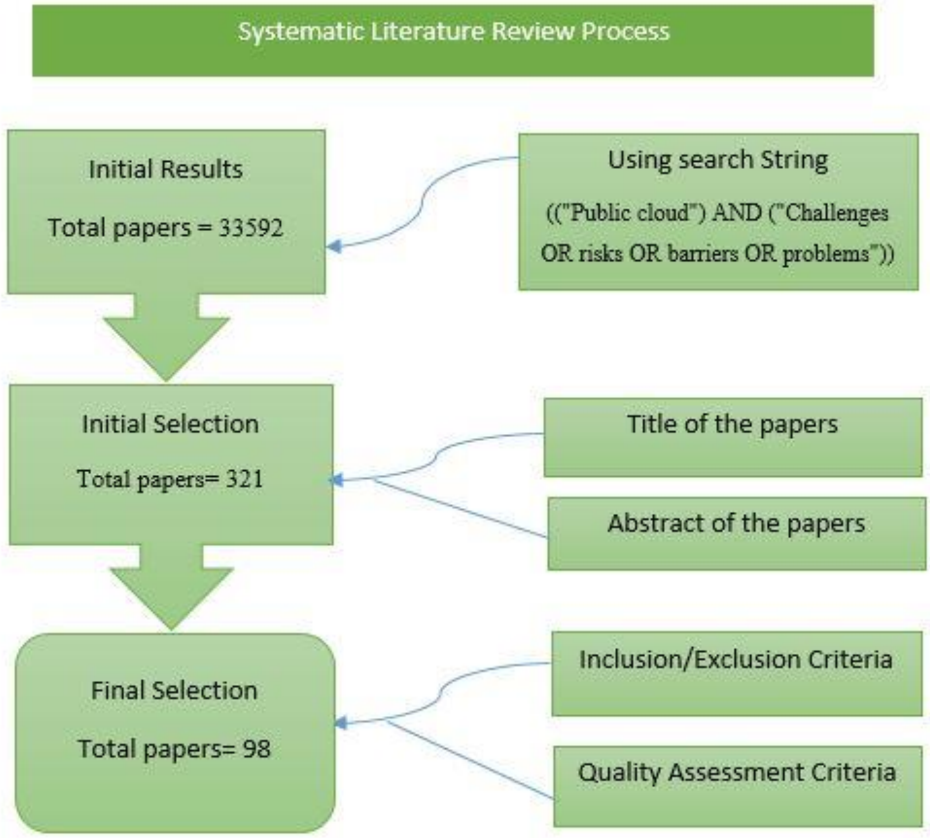
Systematic Literature Review Process
Initial Results
Total papers = 33592
Using search String
(("Public cloud") AND ("Challenges OR risks OR barriers OR problems"))
Initial Selection
Total papers= 321
Title of the papers
Abstract of the papers
Final Selection
Total papers= 98
Inclusion/Exclusion Criteria
Quality Assessment Criteria

Figure 1. SLR Process.

3.3.1. Inclusion Criteria (IC)

IC1: Studies present PCC in general
IC2: Studies that addressed the challenges/issues/risks in the domain of CC, specifically PCC
IC3: Relevant publish papers in the English Language

3.3.2. Exclusion Criteria (E.C.)

EC1: Studies which does not describe challenges/risks in the PCC adoption
EC2: Excludes those papers and articles discussing CC challenges in the P.C. domain.
EC3: Published paper other than the English Language

3.4. Study Quality Assessment

The following questions were used to assess the quality of the final selected publications:

QA1: Are there fine pieces of evidence provided by the study?
QA2: Is the author unbiased regarding the positive and negative results?
QA3: Are the data collection methods clear?

These questions were marked 'YES,' 'NO,' 'Partial,' and 'N.A.'

3.5. Data Extraction and Synthesis

We extracted the article title from our finally selected sample of papers, as shown in Appendix A Table A1. As presented in Appendix A Table A2, we also extracted data related to each paper, such as publishing year, journal/conference proceedings/others, databases, and author's continent. We also extracted PCC risks, challenges, and barriers from each publication and article. An Excel sheet was used to record these data.

4. Results and Discussion

In this section, we present the SLR results conducted to identify challenges faced by clients in adopting PCC. The details are given in Section 4.1. We also performed three different analyses on the challenges. The details are available in Section 4.2.

4.1. Challenges Confronted Clients in the Adoption of Public Cloud Computing

We dig out 29 challenges for clients during the adoption of PCC, as shown in Table 2. Table footer shows the “Frequency of each challenge in SLR” and Table footer shows the ˝Percentage of each challenge in SLR”. “Lack of security” has the highest frequency of 64. The second most cited challenge is “Lack of privacy,” with a frequency of 44. The third most cited challenge is “Data loss or leakage,” having a frequency of 41. For more specifications, we also analyze the critical challenges more thoroughly. We considered a challenge a critical challenge if its percentage occurrence in SLR is =>20. We evaluated nineteen challenges as being pressing challenges. We consider these challenges will negatively affect PCC. CC# represents critical challenges. The identified challenges are as follows:

CC#1 Lack of security

In PCC, security remains an issue, not understanding how your data is backed up or stored. However, the CC model presents chances for advanced security services that can boost individual users and organizations [36,45,46].

Table 2. Challenges identified through SLR.

s.no	Challenge	Paper ID	Freq	%
C1	Lack of security	1,2,3,4,5,6,7,8,9,10,11,14,15,17,19,22,23,24,25,26,28,29,30,31,32, 33,34,35,36,38,40,41,42,43,46,47,50,51,52,56,57,58, 60,61,63,64,66,67,73,74,75,76,81,82,83,85,86,87,90,92,93, 95,96,98	64	65
C2	Lack of privacy	1,2,3,8,9,11,15,17,21,23,26,33,35,36,39,41,42,43,46,47,29, 50,51,52,55,59,60,61,64,66,67,73,74,76,80,82,85,86,87,88, 89,90,95,96,98	44	45
C3	Data loss or leakages	2,8,9,11,13,20,21,25,28,29,31,34,37,38,41,42,43,47,48,49,50, 51,52,54,56,62,63,64,65,66,73,77,79,81,83,84,87,89,90,95,96	41	42
C4	Data and service availability	2,4,5,6,8,11,18,25,27,31,34,36,38,40,42,43,45,47,48,50,52, 54,57,63,64,65,66,67,68,73,74,77,81,83,84,86,87,88,89,90	40	41
C5	Perceived Industry Pressure	2,5,12,14,15,17,20,23,25,27,29,30,35,36,38,41,44,45,47,49, 51,54,57,60,63,64,65,66,70,71,72,75,77,79,81,83,87,89,93, 97	40	41
C6	Geographical Dispersion	2,3,5,6,8,12,17,25,27,31,34,37,38,40,42,43,45,47,48,50,53, 54,57,63,64,65, 67,69,72,74,77,81,83,84,86,89,90,95	38	39
C7	Compliance and legal aspects	2,5,11,17,22,23,25,29,34,38,39,40,41,43,47,49,50,51,52,63, 64,66,70,72,77,79,80,81,85,86,87,88,89,90,95	35	36
C8	lack of user control	2,11,13,16,19,22,25,27,28,34,35,37,38,42,43,47,49,50,51,52, 55,5658,62,63,70,72,77,78,79,81,82,85,87,92	35	36
C9	Lack of accepted standards	2,8,12,13,17,20,21,25,30,34,37,38,41,43,44,48,50,53,59,61, 62,63,66,70,71,72,75,77,81,85,86,87,88,95	34	35
C10	Lack of Customer Trust	1,2,3,5,8,12,17,20,21,25,26,31,36,39,40,42,46,47,52,59,61, 63,68,69,70,74,77,81,82,84,87,88,93	33	34
C11	Lack of Quality of service	1,5,7,8,12,13,16,17,23,24,25,28,35,37,39,45,53,54,57,60,64,65,69, 70,71,72,75,77,79,84,87,94	32	33
C12	Lack of awareness/ Lack of Customer Support/ lack of understanding	2,8,12,14,17,20,21,22,25,26,30,36,40,41,42,46,47,56,58,60, 63,64,65,71,74,76,77,81,82,87,94	31	32

Table 2. *Cont.*

s.no	Challenge	Paper ID	Freq	%
C13	Training and Education	2,8,16,17,25,26,28,34,37,38,42,47,52,53,60,62,63,66,67,68, 69,73,77,80,83,86.87,88,90,95	30	31
C14	Lack of Communication & Coordination	1,2,5,9,12,13,15,18,24,27,32,35,43,44,48,52,55,56,59,62,65,81,85,86,90,93,95	27	28
C15	Lack of Reliability	2,8,17,22,24,25,26,28,32,36,41,42,45,53,57,58,62,65,66,67, 77,79,85,86,87,94	26	27
C16	SLA breach	2,5,12,17,23,27,29,36,38,41,49,51,57,63,64,65,66,70,75,77, 79,81,83,87,89	25	26
C17	Poor bandwidth	8,16,17,25,26,34,52,53,60,62,63,66,67,68,69,777,80,83,86.87,88,90	23	23
C18	Lack of Standard interface	1,2,10,20,31,35,38,46,54,58,62,70,74,77,79,81,85,86,87,88, 91	21	21
C19	Authentication and Authorization	2,5,8,10,13,20,23,24,25,31,34,37,43,50,63,66,77,79,80,81,87, 91	21	21
C20	Multi tenancy	2,5,24,25,37,38,47,63,70,72,77,81,84,87,88,96	15	15
C21	Vendor lock-in	5,26,36,38,52,64,65,75,77,81,84,85,87,88.96	15	15
C22	Loss Of Governance	2,5,8,11,34,36,42,47,52,54,58,77,81,85,87	13	13
C23	Interoperability	2,5,8,10,17,35,37,53,65,77,92	11	11
C24	Hidden cost	2,3,6,8,26,27,43,44,46,54,57,72,82	10	10
C25	Malicious insider	2,5,6,10,35,65,81,93,98	9	9
C26	Insecure or incomplete data deletion	5,10,24,48,77,81	6	6
C27	Lack of Cultural Differences	8,34,55,67,93	5	5
C28	Lack of Focus on key Business Processes	42,63,75,91	4	4
C29	Power consumption	1,2,8,16,29,67	3	3

CC#2 Lack of privacy

In the new digital world, enterprise applications generally export user data to P.C. storage to take advantage of cloud infrastructure's flexibility and efficiency and make corporate goals more cost-efficient. Service providers and consumers face a complex problem with security and privacy concerns in cloud settings [34].

CC#3 Data loss or leakages

Information is lost as a result of data breaches. Outsiders are not the only ones who pose a threat; insiders also play an essential role. Insiders can be any member of a cloud service provider who can pose a risk to any user. When unauthorized customer data exposure occurs, secret and proprietary information are at risk [47,48].

CC#4 Data and service availability

The service provider's servers that keep the user's data in the cloud may be situated elsewhere or far away [49]. If an issue with that server happens, the user may not even have control over that instance [50]. If a node goes down, loses power, a hard drive crashes, or is locked out of their account, the user will not have immediate access to personal records or rectify the problem or issue. The data in the cloud does not guarantee that it is often accessible to the users [50].

CC#5 Perceived industry pressure

The amount of cloud computing competence in the firm's industry and its competitors is called industry pressure. Companies are more inclined to implement I.T. advancements because of their business partners' recommendations and requirements [51]. If their competitors are implementing new I.T., businesses will be pushed to follow suit to stay competitive. Businesses' perceptions of I.S. performance improve due to pressure from business partners and competitors. As a result of industry pressure from competitors and business partners, I.S. adoption is strongly predicted [51].

CC#6 Geographical dispersion

Big data for data processing can be stored in various locations worldwide and keeping such large servers in multiple locations is costly for a company [52]. Cloud computing significantly reduces the cost of large amounts of data by storing and processing data across geographically dispersed and virtual computers [52].

CC#7 Compliance and legal aspects

Legislative and jurisdictional issues are critical information systems management issues in cloud computing due to the likelihood of data center's being placed in jurisdictions with differing laws [53,54]. Lawmakers must urgently develop effective regulations that will aid in assessing the acceptability of legislation in circumstances where data is stored in many jurisdictions [53,54].

CC#8 Lack of user control

The cloud appears to contradict user-centric control: when a SaaS platform is used, the service provider assumes responsibility for data storage, and our data is placed in the hands of a third party with limited flexibility and control [54]. So, how can a consumer retain control over their data when it is kept and accessed in the cloud by a third party? [55].

CC#9 Lack of accepted standards

Customers may face vendor lock-in and data portability issues if cloud providers do not use any form of common open standards. Cloud service providers are not approved by any official certification agency [56,57].

CC#10 Lack of customer trust

The customer relies on the vendor for many services in the CC architecture. Trust is a larger concept than security because it encompasses subjective technique and experience [58]. On the provider's end, the consumer must store his personal information. SaaS adoption is dependent on trust, and openness is a critical mechanism [59]. The dealer chain's lack of control and visibility will create suspicion and distrust [55].

CC#11 Lack of Quality of service

Quality-of-Service (QoS) management, which is the problem of sharing resources with the application to ensure a service level across variables such as performance, availability, and dependability, is a challenge cloud applications offer [60].

CC#12 Lack of awareness/ Lack of Customer Support/lack of understanding

Consumers are usually unaware of how their data is used and dispersed in the cloud, and whether it is used for purposes other than those for which it was obtained. For example, in some circumstances, such as Google Drive or Dropbox, the primary aim of the service is to store personal information in the cloud, and so use is transparent [61]. Other applications, such as those in the sphere of the Internet of Things (IoT), are less evident. Data can be saved on the device, locally, or in the cloud, or a mix of these options. Consumers may be unaware of where their data is kept [61]. Inadequate service provider expertise, such as data privacy and security policies, is thus a significant barrier to PCC adoption [62].

CC#13 Training and education

Education and training have always welcomed new teaching methods and tools [62]. Lack of training and education of experts significantly affects PCC.

CC#14 Lack of communication and coordination

PCC makes use of a vast number of networked computers to deliver better services to customers, such as database access, software application execution, and file storage [63]. These services can be provided to users by a single computer server. However, it is impossible to pinpoint a specific machine in the cloud that is providing services to users. Distance between customers and suppliers adds additional issues, such as a difficult communication and coordination process, cultural and linguistic barriers, time zone variances, information management problems, and collaboration problems. [63–66].

CC#15 Lack of Reliability

Consumers are more concerned about the availability of resources in the CC [67,68]. The term "availability" here refers to the cloud service's reachability and the transaction's positive outcome. The availability among most cloud providers is not defined in this way. The term "availability" is used by cloud providers to illustrate the level of reliability they may expect from their cloud services. Most cloud providers claim that their servers are available 99.99% of the time. Still, it is unclear if this refers to a single server where a customer's virtual instance sits or to all servers in data centers worldwide. There have already been several recorded outage occurrences in cloud providers' data centers [40,67], sending a negative message to cloud customers about the providers' trustworthiness [56].

CC#16 SLA breach

An SLA is a contract between a service provider and a client that defines specifications and requirements, as well as the availability of services, contract term, security, and a contingency plan. The PCC also has some configuration, security, and SLA specificity limits, making it less than ideal for services that use confidential material and thus are subject to compliance rules [35].

CC#17 Poor bandwidth

Compared to wired networks, limited bandwidth, congestion, and poor bandwidth efficiency are critical issues in mobile networks [69,70].

CC#18 Lack of Standard interface

Web interfaces are the primary interface between mobile devices and the cloud. These interfaces are not designed for mobile devices; thus, they have a hefty price tag. Compatibility across mobile devices could be a problem. A standard protocol and an interface must be devised [36].

CC#19 Authentication and Authorization

Software usage is incomplete without authentication, authorization, and access control (AAA), a critical mechanism [71]. The service providers must set up various rights for users, and if either of these rights is broken, the user's account can be deleted, and all privileges granted to the user. It should be clearly defined in the Service Level Agreement (SLA) [48,71].

Other challenges include:

Multi-tenancy

Multi-tenancy in CC occurs when a service provider provides services from many data centers, resulting in data isolation and inconsistency [72,73]. Resource pooling, in which users share resources, is one of the primary properties of CC. When the first user uses a resource and shares it with other users, the first user's data is overwritten by another user's data, making it difficult for digital forensics to locate data during resource pooling [72,74]. The problem arises when the results are in two sorts of data: attacker and user. The goal is to find attacker data while respecting user privacy [72,75].

Loss of Governance

Users must relinquish control over various security-related issues to the cloud provider using the public cloud. The service agreements given by the service provider may not guarantee that the cloud provider will resolve such difficulties. It exposes a security vulnerability [76].

Hidden Cost

According to institutional and transaction cost economics, customers should estimate other expenses beyond the price. Cloud consumers may be unaware of such charges, resulting in frustration, disappointment, and implementation issues [77].

Insecure or incomplete data deletion

The user's data may not be wiped if a contract with a provider is terminated. There are frequent backup copies of data, and there is a potential that this data will be jumbled with other customers' data. As a result, multi-tenancy poses a greater risk to consumers than embedded systems [34].

Power consumption

Unlike disc and memory, energy is a resource that cannot be replenished by activities performed on mobile devices once it has been depleted and can only be filled by external operations [10]. Smart phones have insufficient battery life in response to energy-intensive applications such as video games, audio and video streaming, and running sensors, etc. In MCC, smartphone energy consumption is a problem [78,79].

4.2. Comparison of the Related Surveys

We compare the results of the existing surveys related to public cloud computing. We found 13 survey papers in our total sample of 98. Table 3 shows the comparison of the 19 critical challenges with the survey papers. In the table "✓" shows that the challenges are discussed in the survey. "-" shows that the challenge is not discussed in the survey. Additionally, (C1 to C19) shows the critical challenges identified by us through SLR. It was found that the limited challenges are discussed in each survey in terms of PCC. Further there are no up-to-date systematic literature reviews carried out on the challenges associated with clients in PCC, as evident from the literature.

Table 3. Comparison of the past surveys related with our SLR findings.

S.no	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19
[80]	✓	-	-	-	-	-	✓	✓	-	✓	-	-	-	-	-	-	-	-	-
[35]	✓	-	-	-	-	-	✓	-	-	-	✓	-	-	-	-	✓	-	-	-
[81]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
[82]	✓	-	-	-	-	-	-	✓	-	-	-	-	-	-	✓	-	-	-	-
[78]	-	-	-	-	-	-	-	-	-	-	✓	-	-	-	-	✓	✓	-	-
[76]	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	✓	✓	-	-	-
[83]	✓	✓	✓	-	-	-	✓	-	-	-	-	✓	-	-	-	-	-	-	-
[84]	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	-
[55]	-	-	✓	-	-	-	-	✓	✓	✓	-	-	-	-	-	✓	-	-	✓
[85]	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	✓	-	-	-	-
[86]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	-	✓	-	-
[87]	-	-	✓	-	-	-	✓	✓	-	-	✓	-	-	-	✓	-	-	-	-
[88]	-	-	-	✓	-	-	-	-	-	-	✓	-	-	-	✓	-	-	-	-

4.3. Analysis of the Challenges

We performed three different analyses on the critical challenges. The objective of the analysis was to specify each challenge from a different perspective. We performed a linear-by-linear chi-square test (LBL-CST) on each analysis because the data type ordinal can be found in the SPSS data collection. The literature shows that this test is favored and more potent than the Pearson chi-square test when examining the differences between ordinal variables [89]. The following theory was put to the test:

Hypothesis 0 (H0): *There is no significant difference in exposing communication and coordination issues between the various study approaches used for a specific task.*

Hypothesis 1 (H1): *There is a significant difference in revealing the communication and coordination issues between the various studies approaches used for a particular topic.*

If the value of '*p*' is more significant than 0.05, we will study H0 for obstacles clients face in PCC adoption; otherwise, H1 will be considered.

4.3.1. Year-Wise Analysis of the Challenges

For year-wise analysis, we divided the selected papers' publication years into two periods, i.e., period one from (2010 to 2015) and period two from (2016 to 2021). The same approach is evident in the papers [2,90]. The aim was to find out the intensity of each challenge in each period in order to help us determine the scope of the challenge and whether the identified challenges vary from time to time. Out of the selected papers, 38 were published from 2010 to 2015 and 60 from 2016 to 2021, as shown in Table 4. The results show that many articles were published in the second period. It indicates that PCC still faces many problems that need to be taken seriously. The findings also show that much work has been carried out and is ongoing in this area. We included the three most significant challenges in each period and the three least significant ones to help us find the difference between the first and second periods and help us determine what challenges were crucial in the first and second periods.

The highest occurrence is "Lack of security," in period one, having 63%. The second-highest occurrence is "Perceived Industry Pressure," having 47%. The third highest occurrence is "Data and service availability," having 42%. The lowest occurrence is "Lack of Communication and Coordination," having 8%. The second most minor occurrence is "poor bandwidth," with 21%.

In period two, the highest occurrence is "Lack of security" with 67%. The second-highest occurrence is "Lack of privacy," which has 50%. The third highest occurrence is "Data loss or leakages," having 43%. The lowest occurrence is "Lack of standard interface," having 17%. The second most minor occurrence is "SLA breach," with 20%.

Table 4. Analysis of the challenges based on year.

S.NO	**Challenge**	**Occurrence in Slr (N = 98)**				**Chi-Square Test (Linear-by-Linear Association) a = 0.05, df = 1**	
		From 2010–2015 (N = 38)		**From 2016–2021 (N = 60)**		χ^2	p
		Freq	**%**	**Freq**	**%**		
1	Lack of security	24	63	40	67	0.125	0.724
2	Lack of privacy	14	37	30	50	1.612	0.204
3	Data loss or leakages	14	37	26	43	0.402	0.526
4	Data and service availability	16	42	25	42	0.002	0.966
5	Perceived Industry Pressure	18	47	23	38	0.773	0.379

Table 4. *Cont.*

S.NO	Challenge	Occurrence in Slr (N = 98)				Chi-Square Test (Linear-by-Linear Association) a = 0.05, df = 1	
		From 2010–2015 (N = 38)		From 2016–2021 (N = 60)		X^2	*p*
		Freq	%	Freq	%		
6	Geographical Dispersion	14	37	24	40	0.097	0.756
7	Compliance and legal aspects	15	39	20	33	0.378	0.539
8	lack of user control	10	26	25	42	2.364	0.124
9	Lack of accepted standards	15	39	20	33	0.378	0.539
10	Lack of Customer Trust	14	37	19	32	0.276	0.599
11	Lack of Quality of service	14	37	18	30	0.490	0.484
12	Lack of awareness/Lack of Customer Support/lack of understanding	11	30	20	33	0.205	0.651
13	Training and Education	10	26	20	33	0.534	0.465
14	Lack of Communication & Coordination	3	8	24	40	11.892	0.001
15	Lack of Reliability	9	24	17	28	0.255	0.613
16	SLA breach	13	34	12	20	2.447	0.118
17	Poor bandwidth	8	21	14	23	0.069	0.793
18	Lack of Standard interface	11	30	10	17	2.063	0.151
19	Authentication and Authorization	9	24	13	22	0.054	0.817

We also performed LBL-CST to find out if there was any significant difference between the challenges. We determined one significant difference for the challenge "Lack of Communication and Coordination," having an LBL-CST value of 0.001, which is less than the predefined value of 0.05. This is because this challenge has only 8% in period one. In the second period, the challenges' occurrence significantly increased to 40%. This may indicate that this challenge has grown in recent years. The rest of the challenges show no significant difference.

Figure 2 shows the graphical representation of the papers selected for the two periods for a better understanding. The *x*-axis shows the two periods, and the *y*-axis shows the frequency of each period. The statistical graph shows that extensive work is ongoing in the area. The bar graph shows a consistent increase in the second period.

Table 5 shows the occurrence of each challenge each year. The table shows the frequency of each challenge each year. Y represents YES, showing that the papers presented the challenges, while N stands for No; it demonstrates that the paper fails to present the challenge. The year 2021 shows six frequencies because the data was obtained first. Among the twelve years, the highest range of papers was selected in 2020, which shows that PCC computing is still being rigorously researched. The lowest range of 2 papers is selected from 2015, as shown in Figure 3. This may indicate that relatively few papers were published in 2015.

The *x*-axis shows the publication year of the selected sample, i.e., 2010–2021, while the *y*-axis shows the paper published each year.

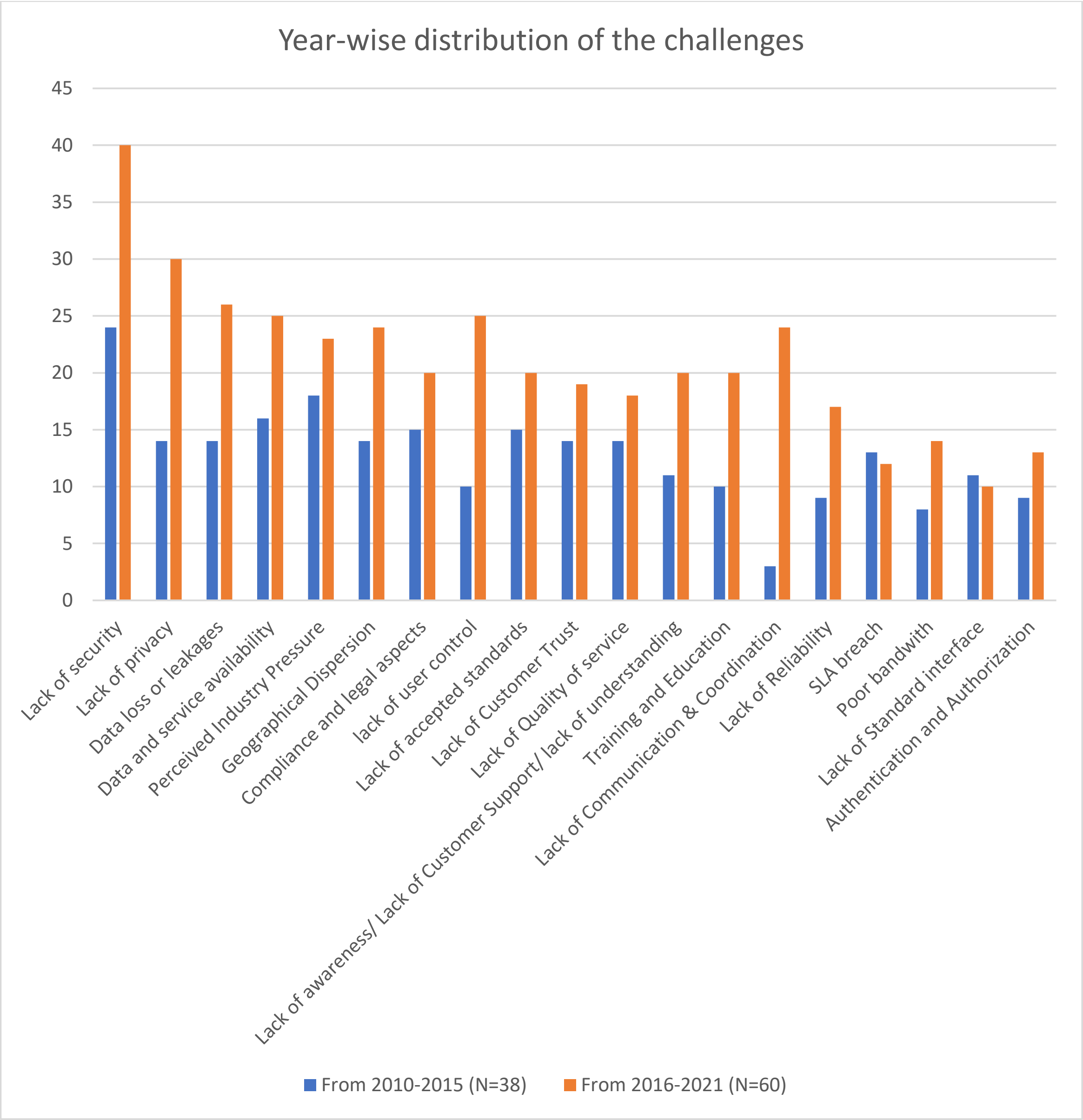

Figure 2. Graphical representation of challenges across both periods.

Table 5. Challenges occurrence in each year from 2010 to 2021.

Challenge	**2010 (N = 3)**		**2011 (N = 8)**		**2012 (N = 9)**		**2013 (N = 7)**		**2014 (N = 9)**		**2015 (N = 2)**		**2016 (N = 11)**		**2017 (N = 7)**		**2018 (N = 9)**		**2019 (N = 10)**		**2020 (N = 17)**		**2021 (N = 6)**	
	Y	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**	**Y**	**N**
Lack of security	2	1	3	5	7	2	5	2	5	4	2	0	8	3	4	3	7	2	7	3	10	7	4	2
Lack of privacy	1	2	3	5	3	6	3	4	3	6	1	1	4	7	2	5	6	3	6	4	9	8	3	3
Data loss or leakages	0	3	5	3	1	8	5	2	2	7	1	1	7	4	3	4	4	5	8	2	2	15	2	2
Data and service availability	1	2	2	6	4	5	5	2	3	6	1	1	6	5	6	1	5	4	5	5	3	14	0	6
Perceived Industry Pressure	1	2	6	2	6	3	3	4	1	8	1	1	7	4	3	4	0	9	6	4	4	13	3	3

Table 5. *Cont.*

Challenge	2010 (N = 3)		2011 (N = 8)		2012 (N = 9)		2013 (N = 7)		2014 (N = 9)		2015 (N = 2)		2016 (N = 11)		2017 (N = 7)		2018 (N = 9)		2019 (N = 10)		2020 (N = 17)		2021 (N = 6)	
	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N
Geographical Dispersion	1	2	2	6	5	4	3	4	2	7	1	1	6	5	5	2	4	5	6	4	2	15	1	5
Compliance and legal aspects	1	2	3	5	5	4	4	3	0	9	2	0	6	5	2	5	3	6	5	5	3	14	1	5
lack of user control	1	2	2	6	3	6	2	5	1	8	1	1	8	3	2	5	5	4	5	5	4	13	1	5
Lack of accepted standards	1	2	6	2	5	4	1	6	2	7	0	2	4	7	1	6	3	6	5	5	5	12	2	4
Lack of Customer Trust	2	1	4	4	3	6	2	5	2	7	1	1	5	6	2	5	3	6	3	7	6	11	0	6
Lack of Quality of service	1	2	4	4	3	6	2	5	4	5	0	2	4	7	3	4	2	7	4	6	4	13	1	5
Lack of awareness/Lack of Customer Support/lack of understanding	1	2	4	4	2	8	1	6	2	7	1	1	6	5	2	5	2	7	5	5	3	14	2	4
Training and Education	2	1	1	7	2	8	2	5	3	6	0	2	4	7	1	6	6	3	4	6	4	13	1	5
Lack of Communication & Coordination	0	3	1	7	1	9	0	7	1	8	0	2	4	7	4	3	5	4	4	6	6	11	1	5
Lack of Reliability	1	2	2	6	2	8	2	5	2	7	0	2	2	9	1	6	6	3	5	5	2	15	1	5
SLA breach	1	2	5	3	4	6	2	5	0	9	1	1	5	6	3	4	0	9	4	6	0	17	0	6
Poor bandwidth	2	1	1	7	1	9	2	5	2	7	0	2	3	8	0	7	5	4	2	8	4	13	0	6
Lack of Standard interface	0	3	4	4	3	7	2	5	2	7	0	2	3	8	1	6	2	7	2	8	1	16	1	5
Authentication and Authorization	0	3	4	4	1	9	2	5	2	7	0	2	4	5	1	6	2	7	4	6	2	15	0	6

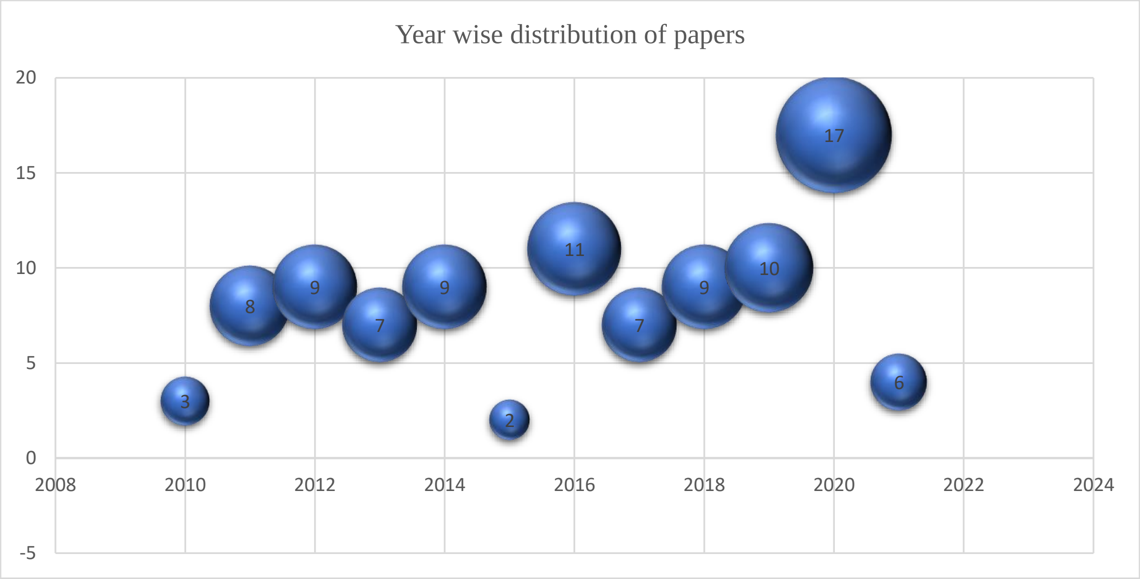

Figure 3. Graphical presentation of year-wise analysis.

4.3.2. Analysis Based on the Authors' Continent

We performed a statistical analysis of the challenges based on the author's continent. As we have a lot of papers from Asia in the list of total papers having a frequency of 51, we analyzed them in two categories, ASIA and other continent. We merged all the other continents into one category, having a frequency of 47, which we called other continents, as shown in Table 6. Similar categorization is evident from published papers [2,90]. We did this to generate a better LBL-CST on the challenges. We may deduce from the analysis that a significant amount of research has been carried out in Asia. It may be because PCC is less expensive than the other deployment models. In Asia, most countries are in the developing stage, and the users cannot afford the cost of other models. The other reason may be that Asia is the most populated continent globally, as more people live in Asia. That is why there are more papers published in the area of Asia relevant to PCC.

Table 6. Analysis based on the author's continent.

S.NO	**Challenge**	**Occurrence in Slr (N = 98)**				**Chi-Square Test (Linear-by-Linear Association) a = 0.05, df = 1**	
		ASIA (N = 51)		**Other Continent (N = 47)**		χ^2	p
		Freq	**%**	**Freq**	**%**		
1	Lack of security	35	69	29	62	0.512	0.474
2	Lack of privacy	21	41	23	49	0.589	0.443
3	Data loss or leakages	23	47	17	36	0.799	0.371
4	Data and service availability	19	37	22	47	0.908	0.341
5	Perceived Industry Pressure	20	39	21	45	0.297	0.586
6	Geographical Dispersion	17	33	21	45	1.313	0.252
7	Compliance and legal aspects	19	37	16	34	0.109	0.742
8	lack of user control	17	33	18	38	0.260	0.610
9	Lack of accepted standards	19	37	16	34	0.109	0.742
10	Lack of Customer Trust	15	29	18	38	0.856	0.355
11	Lack of Quality of service	17	33	15	32	0.022	0.882
12	Lack of awareness/ Lack of Customer Support/ lack of understanding	17	33	14	30	0.141	0.708
13	Training and Education	18	35	12	26	1.086	0.297
14	Lack of Communication & Coordination	15	29	12	26	0.183	0.669
15	Lack of Reliability	14	27	12	26	0.046	0.831
16	SLA breach	11	22	14	30	0.861	0.354
17	internet quality issues	13	25	9	19	0.559	0.455
18	Lack of Standard interface	11	22	10	21	0.001	0.972
19	Authentication and Authorization	15	29	7	15	2.931	0.087

The highest occurrence in ASIA is "Lack of security," with 69%. The second-highest occurrence is "Data loss or leakages," at 47%. The third highest occurrence is "Lack of privacy," with 41%. The lowest occurrence is "Lack of standard interface," and "SLA breach", with 22%.

In Figure 4, the x-axis shows each continent of the authors, while the y-axis shows the number of publications from each continent.

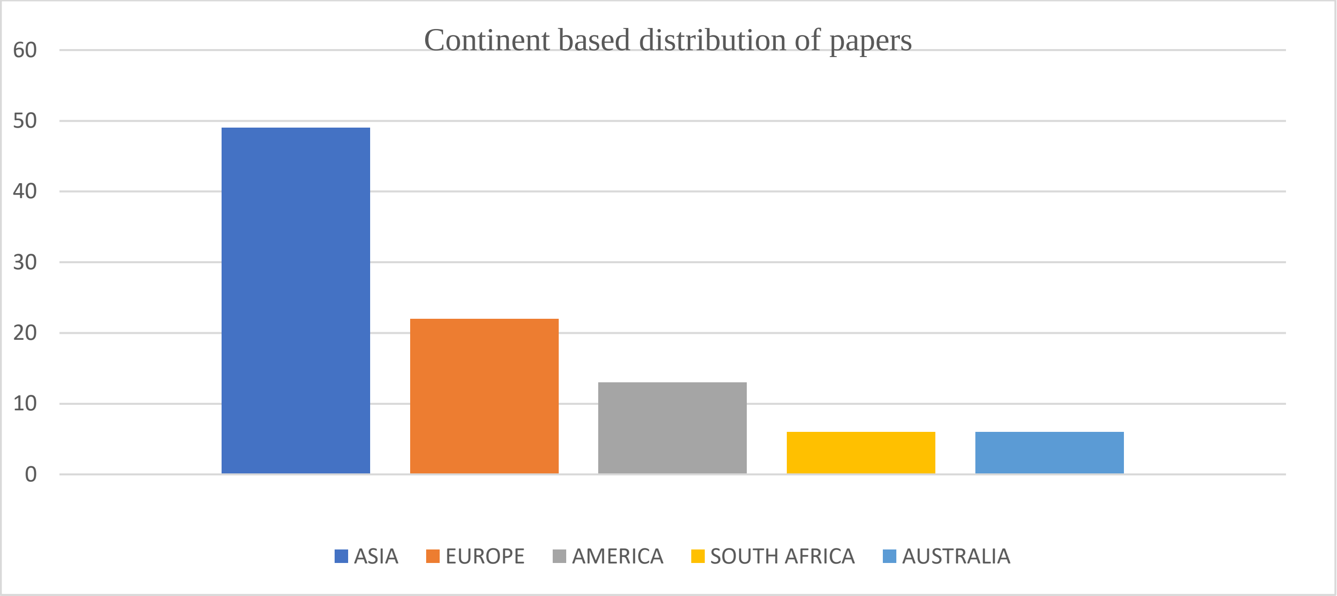

Figure 4. Graphical presentation of author's continent.

The highest occurrence is "Lack of security" in other continents' categories, at 62%. The second-highest occurrence is "Lack of privacy," having 49%. The third highest occurrence is "Data and service availability," at 47%. The lowest occurrence is "Authentication and Authorization," which has the same 15%.

Both categories consider "lack of security" the most critical challenge. Therefore, it can be deduced that, first and foremost, this challenge needs to be mitigated. The lowest critical challenges considered by both are different across continents.

We also performed LBL-CST to find any significant difference between the challenges across the two categories, i.e., ASIA and other continents. There are changes in both the categories across each challenge. We found that none of the challenges have less than a 0.05 value of LBL-CST. This may mean that the challenges are considered equally across the continents. It may also indicate that all the challenges have significance on each continent.

To give a better understanding of the statistical analysis based on the continent. Figure 4 shows the graphical representation of the papers selected across the different continents. We present a graphical representation of all the authors' continents. We have selected 49 papers from Asia, 21 from Europe, 12 from America, seven from Australia, and seven from South Africa. Appendix A Table A2 presents the author's continent in each paper for internal validity. It also indicates that Europe is the second highest paper retrieval continent, from which 21 papers have been selected.

4.3.3. Analysis Based on Publication Venue

We performed an analysis on the paper publication venue. We divided it into two categories: journals, and conferences. We merged the papers of conferences, symposiums, and workshops into one general category called "conference." We merged them to produce a better analysis, as evident from Other researchers' work [90]. This analysis helped us find the venue with the most relevant published papers. This analysis also helped us to find a relevant journal for future publication. Out of the 98 selected papers, 64 are published in journals and 34 in conferences. This may indicate that PCC researchers are keener to publish their work in journals.

From Table 7, in the journal category, the highest occurrence is "Lack of security," with a 69% occurrence. The second-highest occurrence is "Lack of privacy," at 50%. The third highest occurrence is "Data and service availability," with 45%.

Table 7. Analysis based on publication venue.

S.NO	Challenge	Occurrence in SLR (N = 98)				Chi-Square Test (Linear-by-Linear Association) a = 0.05, df = 1	
		Journal (N = 64)		Conference (N = 34)		χ^2	p
		Freq	%	Freq	%		
1	Lack of security	44	69	20	59	0.956	0.328
2	Lack of privacy	32	50	12	35	1.921	0.166
3	Data loss or leakages	25	39	15	44	0.232	0.630
4	Data and service availability	29	45	12	35	0.906	0.341
5	Perceived Industry Pressure	26	41	15	44	0.110	0.740
6	Geographical Dispersion	26	41	12	35	0.263	0.608
7	Compliance and legal aspects	24	38	11	32	0.254	0.615
8	lack of user control	22	34	13	38	0.143	0.706
9	Lack of accepted standards	21	33	14	41	0.670	0.413
10	Lack of Customer Trust	21	33	12	35	0.061	0.806
11	**Lack of Quality of service**	**16**	**25**	**16**	**47**	**4.863**	**0.027**
12	Lack of awareness/ Lack of Customer Support/lack of understanding	19	30	12	35	0.319	0.572
13	Training and Education	21	33	9	26	0.416	0.519
14	Lack of Communication and Coordination	15	23	12	35	1.548	0.213
15	Lack of Reliability	17	27	9	26	0.001	0.992
16	SLA breach	14	22	11	32	1.270	0.260
17	Poor bandwidth	14	22	8	24	0.035	0.853
18	Lack of Standard interface	16	25	5	15	1.383	0.240
19	Authentication and Authorization	14	22	8	24	0.035	0.853

The lowest occurrence is that of "SLA breach," "Poor bandwidth," and "Authentication and Authorization," having 22%. The highest occurrence in the conference category is "Lack of security," which has 59%. The second-highest occurrence is "Lack of service quality," with 47%. The third highest occurrence is "Perceived Industry Pressure "and "Data loss or leakage," having 36% each.

The lowest occurrence is "Lack of Standard interface," having 15%. The second least cited are "Poor bandwidth" and "Authentication and Authorization," having 24%. We also performed LBL-CST to find significant differences across both venues. We found that one challenge, "Lack of quality of service," has a CST value of "0.027," which is less than the predefined value of 0.05. The analysis shows that "Lack of security" has been considered the most critical challenge in the publication venue. The least critical challenges considered in both venues are different. It indicates a clear difference between the venues regarding most minor critical challenges. Each selected paper′s internal validity publication venue has been presented in Appendix A Table A2. If someone has any doubt about the data for this analysis, they can verify it.

We also present the graphical representation of the graph in Figure 5. It can be seen all the challenges are cited more in journals compared to conferences. This may be because there are more journals in PCC than in conferences. We may also deduce that more compact papers are published in the area of PCC.

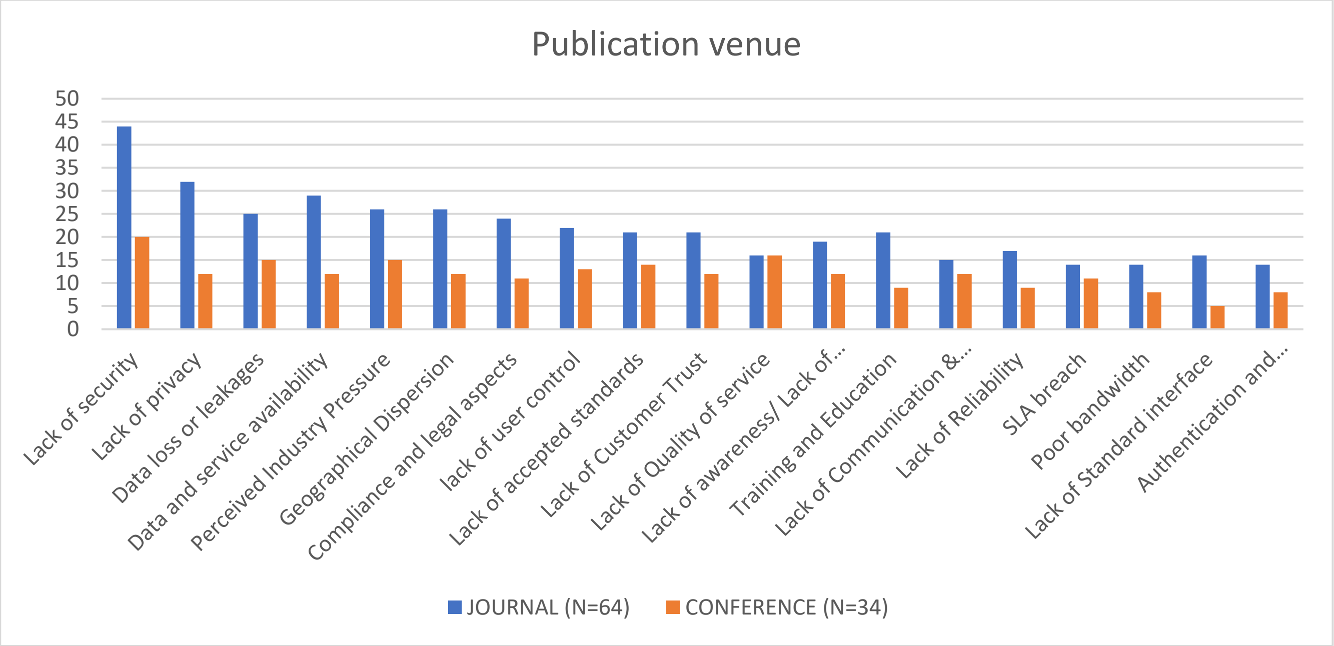

Figure 5. Graphical representation of the challenges across publication venue.

5. Limitations and Threats to Validity

We used a systematic literature review as a research methodology, with appropriate strings and a sufficient sample. However, we can suppose that we may have missed some essential data. The two authors suggested keywords to verify the study's validity and include as much relevant material as feasible.

For example, we searched just the most relevant and well-known libraries in computer disciplines, limiting the number of libraries searched and increasing the danger of data exploitation. To reduce the risk, we have listed the publications in Appendix A Table A1 from which the data was extracted for interested viewers. To reduce the risk, the collaborating scholars reviewed and evaluated each phase of the SLR. The alteration was made because similar research has employed the same technique. Another danger was that we only selected articles in English, which raised the likelihood of papers in the same domain.

The search results also ended in 2021. To reduce the danger, we will publish more outcomes in the future. Additionally, only papers in English were chosen.

6. Conclusions and Future Work

We conducted an SLR for the challenges faced by PCC clients. We first executed a general search string in five well-known digital libraries to identify the gap. We then developed our research string for this study. Following SLR guidelines, we sifted through the final 98 papers to identify the challenges that clients face when adopting PCC. We identified a total of 29 challenges. Out of the 29 challenges, we considered 19 challenges to be critical challenges. We consider a challenge critical if its occurrence in SLR is greater than 20%. We also performed further analysis on the challenges. We aimed to analyze the challenges from a different perspective. We performed three different analyses, i.e., the publication year of the selected papers, publication venue, and continents. The result will assess clients to identify the challenges faced by them. It will also assess PCC vendors in developing systems based on clients' challenges.

In the future, we intend to find out the best practices for each challenge. Furthermore, we will conduct an empirical study to validate the findings of SLR. We will then develop a public cloud client's adoption model (PCCAM) that will assess organization capabilities for clients. We will also conduct a case study to validate the model from PCC companies.

Author Contributions: M.J.K. conducted the SLR and retrieved data from the papers. F.U. supervised the entire process. M.I. is the co-supervisor who extracted the data for analysis. J.K. performed the analysis. A.K., A.S.A. and S.S.A. provided funding for the paper. They also review the paper several times for any improvements. They are also response to the reviewer's comments. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by Taif University Researchers supporting Project number (TURSP-2020/311), Taif University, Taif, Saudi Arabia.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: We provided the sources from which the data has been collected in the Appendix A. All the paper titles are available for validation.

Acknowledgments: We are thankful to Taif University Researchers supporting Project number (TURSP-2020/311), Taif University, Saudi Arabia, for supporting this work.

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

Appendix A

Table A1. Titles of the selected papers.

Paper ID	Tracking ID	Title
1	IEEE-01	Mobile Public Cloud Computing, Merits and Open Issues
2	IEEE-02	Cloud Security Issues Based on People, Process and Technology Model: A Survey
3	IEEE-03	Security and Trust Preserving VM Migrations in Public Clouds
4	IEEE-04	An enhanced data security and trust management enabled framework for cloud computing systems
5	IEEE-05	Survey paper on cloud computing security
6	IEEE-06	Security Challenges for the Public Cloud
7	IEEE-07	An Efficient Public Key Searchable Encryption Scheme for Mobile Smart Terminal
8	IEEE-08	Mobile Cloud Computing: Issues and Challenges
9	IEEE-09	A survey on cloud security issues and Blockchain
10	IEEE-10	Cloud Computing: Security Model Comprising Governance, Risk Management and Compliance
11	IEEE-11	Security Concerns and risk at different levels in Cloud Computing
12	IEEE-12	SLA-Oriented Resource Provisioning for Cloud Computing: Challenges, Architecture, and Solutions
13	IEEE-13	The architectural framework for public cloud security
14	IEEE-14	Survey on Access Control Issues in Cloud Computing
15	IEEE-15	KeySea: Keyword-based Search with Receiver Anonymity in Attribute-based Searchable Encryption
16	IEEE-16	A Survey of Challenging Issues and Approaches in Mobile Cloud Computing
17	IEEE-17	Cloud Computing Landscape and Research Challenges regarding Trust and Reputation
18	IEEE-18	Virtual Machine Scaling Method Considering Performance Fluctuation of Public Cloud

Table A1. *Cont.*

Paper ID	Tracking ID	Title
19	IEEE-19	Can Public-Cloud Security Meet Its Unique Challenges?
20	IEEE-20	TrustCloud: A Framework for Accountability and Trust in Cloud Computing
21	IEEE-21	Authorized Private Keyword Search over Encrypted Data in Cloud Computing
22	IEEE-22	Key Factors Impacting Cloud Computing Adoption
23	IEEE-23	Towards Cloud Computing SLA Risk Management: Issues and Challenges
24	IEEE-24	Cloud Computing Digital Forensic challenges
25	IEEE-25	A Review On Cloud Computing
26	IEEE-26	Cloud Computing Adoption in Higher Education Institutions: A Systematic Review
27	IEEE-27	Analysis of Performance Variability in Public Cloud Computing
28	IEEE-28	Enhancing data storage security in cloud using certificate less public auditing
29	IEEE-29	Risk Management on the Security Problem in Cloud Computing
30	IEEE-30	Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing
31	IEEE-31	Security Challenges in Vehicular Cloud Computing
32	IEEE-32	Key-Policy Attribute-Based Encryption with Keyword Search in Virtualized Environments
33	SP-01	Security Frameworks in Mobile Cloud Computing
34	SP-02	Cloud Computing: Vulnerability and Threat Indications
35	SP-03	Develop Ten Security Analytics Metrics for Big Data on the Cloud
36	SP-04	Trust as a facilitator in cloud computing: a survey
37	SP-05	Security concerns and countermeasures in cloud computing: a qualitative analysis
38	SP-06	A quantitative analysis of current security concerns and solutions for cloud computing
39	SP-07	Trust mechanisms for cloud computing
40	SP-08	Trust model at service layer of cloud computing for educational institutes
41	SP-09	Smart Innovation, Systems and Technologies
42	SP-10	Cloud Computing Adoption Decision in E-government
43	SP-11	Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective
44	SP-12	Cloudy transaction costs: a dive into cloud computing economics
45	SP-13	Quality-of-service in cloud computing: modeling techniques and their applications
46	SP-14	Factors Influencing the Adoption of Cloud Computing by Small and Medium Size Enterprises (SMEs)
47	SP-15	A survey of compliance issues in cloud computing
48	SD-01	A Comprehensive Survey on Security in Cloud Computing
49	SD-02	A Study on Data Storage Security Issues in Cloud Computing
50	SD-03	Enabling Privacy and Security in Cloud of Things: architecture, applications, security & privacy challenges
51	SD-04	Security in cloud computing: Opportunities and challenges
52	SD-05	Key Issues for Embracing the Cloud Computing to Adopt a Digital Transformation: A study of Saudi Public Sector
53	SD-06	Advantages and challenges of adopting cloud computing from an enterprise perspective
54	SD-07	Risk perception and risk management in cloud computing: Results from a case study of Swiss companies
55	SD-08	Towards an integrated sociotechnical approach for designing adaptive privacy aware services in cloud computing

Table A1. *Cont.*

Paper ID	Tracking ID	Title
56	SD-09	Conceptualizing a model for adoption of cloud computing in education
57	SD-10	Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability
58	SD-11	Challenges of Deploying Cloud Computing in eHealth
59	SD-12	Information Technology Solutions, Challenges, and Suggestions for Tackling the COVID-19 Pandemic
60	SD-13	Impact of Coronavirus Pandemic Crisis on Technologies and Cloud Computing Applications
61	SD-14	Security and privacy of electronic health records: Concerns and challenges
62	ACM-01	Challenges and Solutions in Cloud Forensics
63	ACM-02	Security, Privacy Issues and challenges In Cloud Computing: A Survey
64	ACM-03	Cloud Computing Adoption: A Short Review of Issues and Challenges
65	ACM-04	Issues and Challenges of Load Balancing Techniques in Cloud Computing: A Survey
66	ACM-05	Management Issues with Cloud Computing
67	ACM-06	A Manifesto for Future Generation Cloud Computing: Research Directions for the Next Decade
68	ACM-07	CloudCmp: Comparing Public Cloud Providers
69	ACM-08	Cloud Computing: Survey on Energy Efficiency
70	ACM-09	State-of-the-art Cloud Computing Security Taxonomies A classification of security challenges in the present cloud computing environment
71	ACM-10	Scalable Query Processing and Query Engines over Cloud Databases: Models, Paradigms, Techniques, Future Challenges
72	CS-01	Security Issues: Public vs Private vs Hybrid Cloud Computing
73	CS-02	An Assessment Of Cloud Computing: Evolution
74	GS-01	Data Security and Privacy in Cloud Computing
75	GS-02	Cloud Computing Security Issues and Challenges
76	GS-03	Public vs. Private vs. Hybrid vs. Community—Cloud Computing: A Critical Review
77	GS-04	A Data Security Implementation Model For Cloud Computing In Government Parastatals
78	GS-05	A Study on E-Learning and Cloud Computing
79	GS-06	A Survey on Cloud Computing Security, Challenges and Threats
80	GS-07	Cloud Applications for Data Management and Deployment: Analysis for Financial Institutions
81	GS-08	Cloud computing security: protecting cloud-based smart city applications
82	GS-09	Understanding Determinants Of Cloud Computing Adoption Using An Integrated Diffusion Of Innovation (Doi)- Technological, Organizational And Environmental (Toe) Model
83	GS-10	Cloud Computing Performance Evaluation: Issues And Challenges
84	GS-11	Government Cloud Computing and National Security
85	GS-12	Challenges of Cloud Computing Adoption From the TOE Framework Perspective
86	GS-13	Cloud Computing: Research Issues and Implications
87	GS-14	Cloud Computing: Security Issues and Research Challenges
88	GS-15	Major Challenges Facing Cloud Migration
89	GS-16	Perceived impacts of Cloud Computing adoption on the role of an IT department of a higher institution in a developing country.
90	GS-17	Cloud Computing: Study Of Security Issues And Research Challenges
91	GS-18	Cloud Computing Avoids Downfall Of Application Service Providers
92	GS-19	Internal audits in the digital era: opportunities risks and challenges

Table A1. *Cont.*

Paper ID	Tracking ID	Title
93	GS-20	Privacy Preservation In Cloud Using Glowworm Swarm-Based Whale Optimization Algorithm (Gwoa) With 128 Key Size In Cleveland Database
94	GS-21	A Survey on QoS Requirements Based on Particle Swarm Optimization Scheduling Techniques for Workflow Scheduling in Cloud Computing
95	GS-22	Public Health Innovation through Cloud Adoption: A Comparative Analysis of Drivers and Barriers in Japan, South Korea, and Singapore
96	GS-23	Cloud Computing's Impact on Enterprises In Term of Security and Cost
97	GS-24	A natural human language framework for digital forensic readiness in the public cloud
98	GS-25	Data control in public cloud computing: Issues and challenges

Table A2. Data gather from the selected papers for analysis.

Paper ID	Year	Publication Venue	Country
1	2016	Conference	South Africa
2	2019	Journal	Iran
3	2012	Conference	Sweden
4	2014	Conference	India
5	2017	Conference	India
6	2012	Journal	USA
7	2020	Journal	China
8	2018	Conference	India
9	2019	Conference	India
10	2014	Journal	Kuwait
11	2013	Conference	India
12	2011	Conference	Australia
13	2014	Conference	India
14	2016	Journal	India
15	2020	Journal	India
16	2016	Conference	China
17	2010	Symposium	Germany
18	2017	Conference	Japan
19	2010	Conference	USA
20	2011	Conference	SINGAPORE
21	2011	Conference	China
22	2013	Journal	Ireland
23	2012	Conference	Switzerland
24	2018	Conference	India
25	2019	Conference	India
26	2019	Journal	Malaysia
27	2017	Conference	Australia
28	2017	Conference	India
29	2011	Conference	Japan

Table A2. *Cont.*

Paper ID	Year	Publication Venue	Country
30	2012	Conference	India
31	2013	Journal	China
32	2020	Journal	China
33	2020	Journal	USA
34	2020	Journal	India
35	2019	Journal	USA
36	2012	Journal	Germany
37	2019	Journal	India
38	2012	Journal	Brazil
39	2013	Journal	USA
40	2015	Journal	Pakistan
41	2019	Journal	UK
42	2018	Journal	Greece
43	2016	Journal	UK
44	2020	Journal	Germany
45	2014	Journal	UK
46	2014	Journal	Canada
47	2016	Journal	USA
48	2017	Work Shop	Australia
49	2016	Conference	India
50	2019	Journal	France
51	2015	Journal	USA
52	2018	Conference	UK
53	2014	Conference	Romania
54	2013	Journal	Switzerland
55	2020	Journal	Greece
56	2016	Journal	USA
57	2016	Journal	Mexico
58	2021	Conference	Egypt
59	2020	Journal	USA
60	2020	Journal	Malaysia
61	2020	Journal	Saudi Arabia
62	2018	Conference	Pakistan
63	2016	Conference	India
64	2017	Conference	Malaysia
65	2019	Conference	India
66	2013	Journal	South Africa
67	2018	Journal	Australia
68	2010	Journal	Australia
69	2014	Journal	Australia
70	2012	Conference	India
71	2021	Conference	France

Table A2. *Cont.*

Paper ID	Year	Publication Venue	Country
72	2012	Journal	India
73	2014	Journal	India
74	2017	Journal	China
75	2011	Journal	Nigeria
76	2014	Journal	India
77	2016	Journal	Nairobi
78	2018	Journal	India
79	2011	Journal	India
80	2020	Journal	Jordan
81	2016	Journal	Greece
82	2020	Journal	Turkey
83	2013	Journal	Iran
84	2020	Journal	Egypt
85	2018	Journal	Jordan
86	2012	Journal	India
87	2011	Journal	India
88	2020	Journal	Brazil
89	2019	Journal	Sweden
90	2018	Journal	India
91	2011	Journal	USA
92	2020	Journal	Cyprus
93	2020	Journal	India
94	2020	Journal	Malaysia
95	2021	Journal	Singapore
96	2021	Journal	Turkey
97	2021	Journal	India
98	2021	Conference	India

References

1. Khan, S.U.; Ullah, N. Practices for Clients in the Adoption of Hybrid Cloud: Practices for Clients in the Adoption of Hybrid Cloud. *Proc. Pak. Acad. Sci. A Phys. Comput. Sci.* **2017**, *54*, 13–32.
2. Khan, S.U.; Ullah, N. Challenges in the adoption of hybrid cloud: An exploratory study using systematic literature review. *J. Eng.* **2016**, *2016*, 107–118. [CrossRef]
3. Vafamehr, A.; Khodayar, M.E. Energy-aware cloud computing. *Electr. J.* **2018**, *31*, 40–49. [CrossRef]
4. Shabir, M.Y.; Iqbal, A.; Mahmood, Z.; Ghafoor, A. Analysis of classical encryption techniques in cloud computing. *Tsinghua Sci. Technol.* **2016**, *21*, 102–113. [CrossRef]
5. Pańkowska, M.; Pyszny, K.; Strzelecki, A. Users' adoption of sustainable cloud computing solutions. *Sustainability* **2020**, *12*, 9930. [CrossRef]
6. Yoo, S.-K.; Kim, B.-Y. A decision-making model for adopting a cloud computing system. *Sustainability* **2018**, *10*, 2952. [CrossRef]
7. Bandyopadhyay, S.; Sengupta, M.; Maiti, S.; Dutta, S. Role of middleware for internet of things: A study. *Int. J. Comput. Sci. Eng. Surv.* **2011**, *2*, 94–105. [CrossRef]
8. Priyadarshinee, P.; Raut, R.D.; Jha, M.K.; Gardas, B.B. Understanding and predicting the determinants of cloud computing adoption: A two staged hybrid SEM-Neural networks approach. *Comput. Hum. Behav.* **2017**, *76*, 341–362. [CrossRef]

9. Gupta, A.; Bhadauria, H.; Singh, A.; Patni, J.C. A theoretical comparison of job scheduling algorithms in cloud computing environment. In Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 4–5 September 2015.
10. Shaukat, U.; Ahmed, E.; Anwar, Z.; Xia, F. Cloudlet deployment in local wireless networks: Motivation, architectures, applications, and open challenges. *J. Netw. Comput. Appl.* **2016**, *62*, 18–40. [CrossRef]
11. Bal, P.K.; Mohapatra, S.K.; Das, T.K.; Srinivasan, K.; Hu, Y.-C. A Joint Resource Allocation, Security with Efficient Task Scheduling in Cloud Computing Using Hybrid Machine Learning Techniques. *Sensors* **2022**, *22*, 1242. [CrossRef] [PubMed]
12. Mlotshwa, L.; Leonard, A.; Ntawanga, F. A conceptual framework for cloud-computing management: An end-user environment perspective. In Proceedings of the 2015 IST-Africa Conference, Lilongwe, Malawi, 6–8 May 2015.
13. Chang, B.-Y.; Hai, P.H.; Seo, D.-W.; Lee, J.-H.; Yoon, S.H. The determinant of adoption in cloud computing in Vietnam. In Proceedings of the 2013 International Conference on Computing, Management and Telecommunications (ComManTel), Ho Chi Minh City, Vietnam, 21–24 January 2013.
14. Gai, K.; Qiu, M.; Zhao, H. Energy-aware task assignment for mobile cyber-enabled applications in heterogeneous cloud computing. *J. Parallel Distrib. Comput.* **2018**, *111*, 126–135. [CrossRef]
15. Duan, H.; Chen, C.; Min, G.; Wu, Y. Energy-aware scheduling of virtual machines in heterogeneous cloud computing systems. *Future Gener. Comput. Syst.* **2017**, *74*, 142–150. [CrossRef]
16. Goundar, S. Cloud Computing: Opportunities and Issues for Developing Countries. DiploFoundation: Internet Governance Research Paper. 2010. Available online: https://www.researchgate.net/profile/Sam-Goundar/publication/265060137_Cloud_computing_Opportunities_and_issues_for_developing_countries/links/55c30f9508aebc967defeb3b/Cloud-computing-Opportunities-and-issues-for-developing-countries.pdf (accessed on 16 April 2022).
17. Alhamazani, K.; Ranjan, R.; Mitra, K.; Rabhi, F.; Jayaraman, P.P.; Khan, S.U.; Guabtni, A.; Bhatnagar, V. An overview of the commercial cloud monitoring tools: Research dimensions, design issues, and state-of-the-art. *Computing* **2015**, *97*, 357–377. [CrossRef]
18. Pahl, C.; Xiong, H.; Walshe, R. A comparison of on-premise to cloud migration approaches. In Proceedings of the Second European Conference, ESOCC 2013, Málaga, Spain, 11–13 September 2013; pp. 212–226.
19. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I. A view of cloud computing. *Commun. ACM* **2010**, *53*, 50–58. [CrossRef]
20. Mell, P.; Grance, T. *The NIST Definition of Cloud Computing*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.
21. Lewis, G. *Basics about Cloud Computing*; Software Engineering Institute Carniege Mellon University: Pittsburgh, PA, USA, 2010.
22. Mell, P.; Grance, T. Effectively and securely using the cloud computing paradigm. *NIST Inf. Technol. Lab.* **2009**, *2*, 304–311.
23. Nelson, M.R. Building an open cloud. *Science* **2009**, *324*, 1656–1657. [CrossRef] [PubMed]
24. Baliga, J.; Ayre, R.; Sorin, W.V.; Hinton, K.; Tucker, R.S. Energy consumption in access networks. In Proceedings of the OFC/NFOEC 2008—2008 Conference on Optical Fiber Communication/National Fiber Optic Engineers Conference, San Diego, CA, USA, 24–28 February 2008.
25. Mather, T.; Kumaraswamy, S.; Latif, S. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2009.
26. Hamrén, O. Mobile Phones and Cloud Computing: A Quantitative Research Paper on Mobile Phone Application Offloading by Cloud Computing Utilization. Master's Thesis, Umeå University, Umeå, Sweden, 2012.
27. Jansen, W.; Grance, T. *Sp 800–144. Guidelines on Security and Privacy in Public Cloud Computing*; National Institute of Standards & Technology: Gaithersburg, MD, USA, 2011.
28. Meng, S.; Luo, L.; Qiu, X.; Dai, Y. Service-Oriented Reliability Modeling and Autonomous Optimization of Reliability for Public Cloud Computing Systems. *IEEE Trans. Reliab.* **2022**, *71*, 527–538. [CrossRef]
29. Ren, K.; Wang, C.; Wang, Q. Security challenges for the public cloud. *IEEE Internet Comput.* **2012**, *16*, 69–73. [CrossRef]
30. Chakrawarti, R.K.; Singhai, K. The architechtural framework for public cloud security. In Proceedings of the 2014 International Conference of Soft Computing Techniques for Engineering and Technology (ICSCTET), Bhimtal, India, 7–8 August 2014; pp. 1–5.
31. Kaufman, L.M. Can public-cloud security meet its unique challenges? *IEEE Secur. Priv.* **2010**, *8*, 55–57. [CrossRef]
32. He, W.; Zhang, Z.J.; Li, W. Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. *Int. J. Inf. Manag.* **2021**, *57*, 102287. [CrossRef]
33. O'Neill, P. H.; Ryan-Mosley, T.; Johnson, B. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*, 7 May 2020. [CrossRef]
34. Chaudhari, P.; Das, M.L. KeySea: Keyword-based Search with Receiver Anonymity in Attribute-based Searchable Encryption. *IEEE Trans. Serv. Comput.* **2020**, *15*, 1036–1044. [CrossRef]
35. Kaura, W.C.N.; Lal, A. Survey paper on cloud computing security. In Proceedings of the 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 17–18 March 2017; pp. 1–6.
36. Hlatshwayo, C.M.; Zuva, T. Mobile public cloud computing, merits and open issues. In Proceedings of the 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), Durban, South Africa, 28–29 November 2016; pp. 128–132.

37. Aslam, M.; Gehrmann, C.; Björkman, M. Security and trust preserving VM migrations in public clouds. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; pp. 869–876.
38. Baror, S.O.; Venter, H.S.; Adeyemi, R. A natural human language framework for digital forensic readiness in the public cloud. *Aust. J. Forensic Sci.* **2021**, *53*, 566–591. [CrossRef]
39. Kaneko, Y.; Ito, T.; Ito, M.; Kawazoe, H. Virtual Machine Scaling Method Considering Performance Fluctuation of Public Cloud. In Proceedings of the 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honololu, HI, USA, 25–30 June 2017; pp. 782–785.
40. Morawiec, P.; Sołtysik-Piorunkiewicz, A. Cloud Computing, Big Data, and Blockchain Technology Adoption in ERP Implementation Methodology. *Sustainability* **2022**, *14*, 3714. [CrossRef]
41. Weidt, F.; Silva, R. Systematic Literature Review in Computer Science—A Practical Guide; Relatórios Técnicos Do DCC/UFJF; 2016. Available online: https://www.semanticscholar.org/paper/Systematic-Literature-Review-in-Computer-Science-A-Weidt-Silva/0a582fd8d9ceeb16466e0e6da756dfff39febf2f (accessed on 16 April 2022).
42. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; EBSE Technical Report EBSE-2007-01; University of Durham: Durham, UK, 2007.
43. Quezada-Gaibor, D.; Torres-Sospedra, J.; Nurmi, J.; Koucheryavy, Y.; Huerta, J. Cloud Platforms for Context-Adaptive Positioning and Localisation in GNSS-Denied Scenarios—A Systematic Review. *Sensors* **2021**, *22*, 110. [CrossRef] [PubMed]
44. Myeong, S.; Park, J.; Lee, M. Research Models and Methodologies on the Smart City: A Systematic Literature Review. *Sustainability* **2022**, *14*, 1687. [CrossRef]
45. He, Q.; He, H. A Novel Method to Enhance Sustainable Systems Security in Cloud Computing Based on the Combination of Encryption and Data Mining. *Sustainability* **2020**, *13*, 101. [CrossRef]
46. Roy, P.; Kumar, R. Onion Encrypted Multilevel Security Framework for Public Cloud. In Proceedings of the 2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India, 21–22 January 2022; pp. 1–5.
47. Kandias, M.; Virvilis, N.; Gritzalis, D. The insider threat in cloud computing. In Proceedings of the 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, 8–9 September 2011; pp. 93–103.
48. Singh, V.; Pandey, S. Cloud computing: Vulnerability and threat indications. In *Performance Management of Integrated Systems and Its Applications in Software Engineering*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 11–20.
49. Sharma, A.; Jha, P.; Singh, S. Data control in public cloud computing: Issues and challenges. *Recent Adv. Comput. Sci. Commun. (Former. Recent Pat. Comput. Sci.)* **2021**, *14*, 564–579. [CrossRef]
50. Puri, G.S.; Tiwary, R.; Shukla, S. A review on cloud computing. In Proceedings of the 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 10–11 January 2019; pp. 63–68.
51. Chang, Y.-W.; Hsu, P.-Y.; Huang, S.-H.; Chen, J. Determinants of switching intention to cloud computing in large enterprises. *Data Technol. Appl.* **2019**, *54*, 16–33. [CrossRef]
52. Islam, M.; Reza, S. The Rise of Big Data and Cloud Computing. *Internet Things Cloud Comput.* **2019**, *7*, 45. [CrossRef]
53. Khajeh-Hosseini, A.; Greenwood, D.; Sommerville, I. Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS. In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, 5–10 July 2010; pp. 450–457.
54. Akande, A.O.; April, N.A.; van Belle, J.-P. Management issues with cloud computing. In Proceedings of the ICCC'13: 2013 The Second International Conference on Innovative Computing and Cloud Computing, Wuhan, China, 1–2 December 2013; pp. 119–124.
55. Nishad, L.S.; Paliwal, J.; Pandey, R.; Beniwal, S.; Kumar, S. Security, privacy issues and challenges in cloud computing: A survey. In Proceedings of the ICTCS'16: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, Udaipur, India, 4–5 March 2016; pp. 1–7.
56. Habib, S.M.; Ries, S.; Muhlhauser, M. Cloud computing landscape and research challenges regarding trust and reputation. In Proceedings of the 2010 7th International Conference on Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing, Xi'an, China, 26–29 October 2010; pp. 410–415.
57. Everett, C. Cloud computing—A question of trust. *Comput. Fraud. Secur.* **2009**, *6*, 5–7. [CrossRef]
58. Verma, A.; Kaushal, S. Cloud computing security issues and challenges: A survey. In Proceedings of the First International Conference, ACC 2011, Kochi, India, 22–24 July 2011; pp. 445–454.
59. Pearson, S.; Benameur, A. Privacy, security and trust issues arising from cloud computing. In Proceedings of the 2010 IEEE Second International Conference on Cloud Computing Technology and Science, Indianapolis, IN, USA, 30 November–3 December 2010; pp. 693–702.
60. Ardagna, D.; Casale, G.; Ciavotta, M.; Pérez, J.F.; Wang, W. Quality-of-service in cloud computing: Modeling techniques and their applications. *J. Internet Serv. Appl.* **2014**, *5*, 11. [CrossRef]
61. Nikkhah, H.R.; Sabherwal, R. Information disclosure willingness and mobile cloud computing collaboration apps: The impact of security and assurance mechanisms. *Inf. Technol. People*, 2021; *Online Ahead of Print*. [CrossRef]
62. Attaran, M.; Attaran, S.; Celik, B.G. Promises and challenges of cloud computing in higher education: A practical guide for implementation. *J. High. Educ. Theory Pract.* **2017**, *17*, 20–38.

63. Qasem, Y.A.M.; Abdullah, R.; Jusoh, Y.Y.; Atan, R.; Asadi, S. Cloud Computing Adoption in Higher Education Institutions: A Systematic Review. *IEEE Access* **2019**, *7*, 63722–63744. [CrossRef]
64. Alharthi, A.; Yahya, F.; Walters, R.J.; Wills, G. An overview of cloud services adoption challenges in higher education institutions. In Proceedings of the 2nd International Workshop on Emerging Software as a Service and Analytics—ESaaSA, Lisbon, Portugal, 20–22 May 2015.
65. González-Martínez, J.A.; Bote-Lorenzo, M.L.; Gómez-Sánchez, E.; Cano-Parra, R. Cloud computing and education: A state-of-the-art survey. *Comput. Educ.* **2015**, *80*, 132–151. [CrossRef]
66. Sultan, N. Cloud computing for education: A new dawn? *Int. J. Inf. Manag.* **2010**, *30*, 109–116. [CrossRef]
67. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.H.; Konwinski, A.; Lee, G.; Patterson, D.A.; Rabkin, A.; Stoica, I. *Above the Clouds: A Berkeley View of Cloud Computing*; Technical Report UCB/EECS-2009–28; EECS Department, University of California: Berkeley, CA, USA, 2009.
68. Catteddu, D.; Hogben, G. *An SME Perspective on Cloud Computing—Survey*; Technical Report; European Network and Information Security Agency: Athens, Greece, 2009.
69. Suganya, V.; Shanthi, A.L. Mobile Cloud Computing Perspectives and Challenges. *Int. J. Innov. Res. Adv. Eng.* **2014**, *2*, 71–76.
70. Sahu, I.; Pandey, U. Mobile cloud computing: Issues and challenges. In Proceedings of the 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 12–13 October 2018; pp. 247–250.
71. Ranjith, D.; Srinivasan, J. Identity security using authentication and authorization in cloud Computing. *Int. J. Comput. Organ. Trends* **2013**, *3*, 122–129.
72. Neware, R.; Khan, A. Cloud computing digital forensic challenges. In Proceedings of the Informing Science & IT Education Conference (InSITE), Tampa, FL, USA, 29 June–25 July 2015; pp. 1090–1092.
73. Dykstra, J. Seizing electronic evidence from cloud computing environments. In *Cloud Technology: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2015; pp. 2033–2062.
74. Almulla, S.; Iraqi, Y.; Jones, A. A state-of-the-art review of cloud forensics. *J. Digit. Forensics Secur. Law* **2014**, *9*, 2. [CrossRef]
75. Alex, M.E.; Kishore, R. Forensic model for cloud computing: An overview. In Proceedings of the 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 23–25 March 2016; pp. 1291–1295.
76. Habib, S.M.; Hauke, S.; Ries, S.; Mühlhäuser, M. Trust as a facilitator in cloud computing: A survey. *J. Cloud Comput. Adv. Syst. Appl.* **2012**, *1*, 19. [CrossRef]
77. Makhlouf, R. Cloudy transaction costs: A dive into cloud computing economics. *J. Cloud Comput.* **2020**, *9*, 1–11. [CrossRef]
78. Fan, Q.; Liu, L. A survey of challenging issues and approaches in mobile cloud computing. In Proceedings of the 2016 17th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), Guangzhou, China, 16–18 December 2016; pp. 87–90.
79. Satyanarayanan, M. Avoiding dead batteries. *IEEE Pervasive Comput.* **2005**, *4*, 2–3. [CrossRef]
80. Ghaffari, F.; Gharaee, H.; Arabsorkhi, A. Cloud security issues based on people, process and technology model: A survey. In Proceedings of the 2019 5th International Conference on Web Research (ICWR), Tehran, Iran, 24–25 April 2019; pp. 196–202.
81. Pavithra, S.; Ramya, S.; Prathibha, S. A survey on cloud security issues and blockchain. In Proceedings of the 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 21–22 February 2019; pp. 136–140.
82. Charanya, R.; Aramudhan, M. Survey on access control issues in cloud computing. In Proceedings of the 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), Pudukkottai, India, 24–26 February 2016; pp. 1–4.
83. Yimam, D.; Fernandez, E.B. A survey of compliance issues in cloud computing. *J. Internet Serv. Appl.* **2016**, *7*, 1–12. [CrossRef]
84. Ramachandra, G.; Iftikhar, M.; Khan, F.A. A Comprehensive Survey on Security in Cloud Computing. *Procedia Comput. Sci.* **2017**, *110*, 465–472. [CrossRef]
85. Kumar, P.; Kumar, R. Issues and challenges of load balancing techniques in cloud computing: A survey. *ACM Comput. Surv. (CSUR)* **2019**, *51*, 1–35. [CrossRef]
86. Mastelic, T.; Oleksiak, A.; Claussen, H.; Brandic, I.; Pierson, J.-M.; Vasilakos, A.V. Cloud computing: Survey on energy efficiency. *Acm Comput. Surv.* **2014**, *47*, 1–36. [CrossRef]
87. Choubey, R.; Dubey, R.; Bhattacharjee, J. A survey on cloud computing security, challenges and threats. *Int. J. Comput. Sci. Eng. (IJCSE)* **2011**, *3*, 1227–1231.
88. Farid, M.; Latip, R.; Hussin, M.; Hamid, N.A.W.A. A Survey on QoS Requirements Based on Particle Swarm Optimization Scheduling Techniques for Workflow Scheduling in Cloud Computing. *Symmetry* **2020**, *12*, 551. [CrossRef]
89. Wooditch, A.; Johnson, N.J.; Solymosi, R.; Ariza, J.M.; Langton, S. Measures of Association for Nominal and Ordinal Variables. In *A Beginner's Guide to Statistics for Criminology and Criminal Justice Using R*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 209–225.
90. Ahmad, A.; Khan, S.U.; Khan, H.U.; Khan, G.M.; Ilyas, M. Challenges and Practices Identification via a Systematic Literature Review in the Adoption of Green Cloud Computing: Client's Side Approach. *IEEE Access* **2021**, *9*, 81828–81840. [CrossRef]