RSM analysis based cloud access security broker: a systematic literature review

Shahnawaz Ahmad1 · Shabana Mehfuz1 · Fateh Mebarek-Oudina2 · Javed Beg3

Received: 20 November 2021 / Revised: 8 February 2022 / Accepted: 20 April 2022 / Published online: 11 May 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
A Cloud Access Security Broker (CASB) is a security enforcement point or cloud-based software that is placed between cloud service users and cloud applications of cloud computing (CC) which is used to run the dimensionality, heterogeneity, and ambiguity correlated with cloud services. They permit the organization to amplify the reach of their security approaches past their claim framework to third-party computer programs and storage. In contrast to other systematic literature reviews (SLR), this one is directed at the client setting. To identify and evaluate methods to understand CASB, the SLR discusses the literature, citing a comprehension of the state-of-the-art and innovative characterization to describe. An SLR was performed to compile CASB related experiments and analyze how CASBs are designed and formed. These studies are then analyzed from different contexts, like motivation, usefulness, building approach, and decision method. The SLR has discussed the contrasts present between the studies and implementations, with planning accomplishments conducted with combinations of market-based courses of action, simulation tools, middleware’s, etc. Search words with the keywords, which were extracted from the Research Questions (RQs), were utilized to recognize the essential consideration from the journal papers, conference papers, workshops, and symposiums. This SLR has distinguished 20 particular studies distributed from 2011 to 2021. Chosen studies were evaluated concurring to the defined RQs for their eminence and scope to particular CASB in this way recognizing a few gaps within the literature. Unlike other studies, this one concentrates on the customer’s viewpoint. The survey uses a systematic analysis of the literature to discover and classify techniques for realizing CASB, resulting in a comprehensive grasp of the state-of-the-art and a novel taxonomy to describe CASBs. To assemble studies relating to CASB and investigate how CASB are engineered, a systematic literature review was done. These investigations are then evaluated from a variety of angles, including motivation, functionality, engineering approach, and methodology. Engineering efforts were directed at a combination of “market-based solutions”, “middlewares”, “toolkits”, “algorithms”, “semantic frameworks”, and “conceptual frameworks”, according to the study, which noted disparities in the studies’ implementations. For further understanding, the different independent parameters influencing the CASB are studied using PCA (Principal Component Analysis). The outcome of their analysis was the identification of five parameters influencing the PCA analysis. The experimental results were used as input for Research Surface Methodology (RSM) to obtain an empirical model. For this, five-level coding was employed for developing the model and considered three dependent parameters and four center values. For more understanding of these independent variables’ influence, on the CASB study, RSM analysis was employed. It was observed from the CCD (Central Composite Design) model that the actual values show significant influence with $R^2 = 0.90$. This wide investigation reveals that CASB is still in a formative state. Even though vital advancement has been carried out in this zone, obvious challenges stay to be tended to, which have been highlighted in this paper.

Keywords Cloud computing · CASBs · SLR · RSM · CCD model
1 Introduction

Cloud Computing (CC) has emerged as the need of every enterprise in recent times and is turning into an integral part of all other technologies such as IoT, Big data, and Quantum computing [1]. Technology Review followed the coinage of the term “Cloud Computing” (CC) back two-decade earlier, to November 14’ 1996, and an office park outside Houston by “George Favaloro” and “Sean O’Sullivan” [2]. Indeed even though numerous individuals accept that CC may be a quite newborn marvel, it has its roots within the thoughts expected in the 1960s. J.C.R. Licklider of ARPANET is generally described as the primary one to present the thought of an “intergalactic computer network” in 1969, a machine that can be accessed from any place within the world. But even before him, in 1961, John McCarthy floated the thought of computation being given as an open benefit just like any other benefit, a concept he named as “utility computing” [3], and in numerous ways, typically completely what CC is these days. Over the 1960s and’70 s, expansive banks of computers included so-called “time-sharing” services to nearby and inaccessible partners. In the 1980s and early 90 s, expansive scattered data centers were installed by huge enterprises. There was not an earth-shattering breakthrough until the Web got to be very common and effortlessly available. In the year 1999, Saalesforce.com was the primary company that was supplying the working application through the web to the clients. In the year 2002, Amazon Web Services (AWS) aws.amazon.com emerged and provided a heap of cloud services such as capacity and computing. Later in 2006, Elastic Compute Cloud (EC2) also known as EC2 clusters, was introduced by Amazon which helped in setting up small and medium companies and let people rentout their servers for performing pointed computation. In the very same year, Simple Storage Service (S3) was also launched by Amazon which enabled people to use the cloud for storing their information online. After this many tech industries jumped into the business of different cloud services. Google in the year 2009, introduced “Google Apps” compatible with its chrome browser which helped engineers to develop their items and also permits them to host them on Google servers as a web application. Simultaneously Microsoft and Apple pushed their cloud capacity items too, i.e. OneDrive and iCloud respectively. Meanwhile, Microsoft started Microsoft Azure too to be utilized by the buyers to fulfill a variety of objectives from online capacity to databases, web APIs to full-grown web applications to fully presented Linux and Windows VM. As time passed, many stakeholders kept entering this field, and cloud computing technology is expected to be more reasonable easily accessible, and useful in the future, particularly by techstartups and administrators [4]. To share imaginative thoughts and developments in this cloud computing field, a premier conference was started in 2009 with the name “International conference on cloud computing” (ICCC). The effectiveness of the cloud lies in its boundless supply of services such as servers, the storage of information, and anything as a benefit (XaaS) is conceivable [5]. Cloud computing is a live field. This image remained the toast of conferences and gatherings in the IT spaces these days and we have found boosting clues of its services and acknowledgment within the ventures as well as the scholarly community [6]. Another conference named “International Conference on Parallel, Distributed and Grid Computing (PDGC – 2010)” has been started in 2010, due to the emerging importance of cloud computing. The ICCC and PDGC conferences emerged as the platform to share the ideas of the academicians and analysts of the zone of cloud computing. Besides these conferences, a separate journal dedicated to cloud computing was introduced to share the ideas within the said field by the name of “Journal of Cloud Computing: Advances Systems and Applications”, published by Springer. But despite all its buildup and utilization, the idea of CCIs pretty elusive and its definitionis still very unclear. In over simplified terms, the cloud gives further computing and capacity services from a pool of shared assets to its customers. A much more accurate definition is given in Table 1.

Distinctive cloud computing services have been created to demonstrate CC which is, SaaS, IaaS, PaaS, CaaS, DaaS, BaaS, NaaS, OaaS, FaaS, HaaS, and XaaS [7]. Table 2 shows the list of CC services alongside its existing field.

Several systematic literature reviews (SLR) in different areas of CC have been performed to synthesize the available research on different topics. For example, [33] presented an SLR on the “Cloud Brokerage: A Systematic Survey”. Hibatullah Alzhrani et al. [34] performed “A Brief Survey of Cloud Computing” to recognize the research gap in the field of cloud computing. As per the audit [35], a requirement of a study is present which includes recognition, evaluation, and interpretation of the CASB strategies and also provides guidance for the research work to be carried out in the future. Afterward, an SLR on CASB is shown by taking into account the rules of the cloud environment [33], to address the above said-searched problem.In Sect. 4, this may be the essential consideration which appears the SLR on CASB with the point to address the RQs.

The cloud services market is flooded with a large number of heterogeneous cloud solutions, making cloud service selection a difficult undertaking for the Cloud Services Customer (CSC) [36–38]. Furthermore, because each CSP exposes its API, designing and developing an application so that it can be deployed on a specific CSP
## Table 1: Definitions of Cloud Computing

| References | Definition of Cloud Computing |
|------------|-------------------------------|
| NIST [8]   | “Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., network, servers, storage, applications, and services) that can be rapidly provisioned and released with minimum management effort or service provider interaction” |
| [9]        | “Cloud Computing, in which not just our data but even our software resides within the cloud, and we access everything not only through our PCs but also cloud-friendly devices, such as smartphones, PDAs...the mega computer enabled by virtualization and software as a service...this is utility computing powered by massive utility data centers” |
| [10]       | “Cloud Computing is a style of computing where scalable and elastic IT capabilities are provided as a service to multiple external customers using Internet technologies” |
| [11]       | “Cloud Computing is a complex infrastructure of software, hardware, processing, and storage, all of which are available as a service” |
| [12]       | “Cloud Computing is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and customers” |
| [13]       | “a Cloud is a pool of virtualized computer resources” |
| [14]       | “Cloud computing is a delivery of extremely scalable IT-related facilities as a service through the internet to multiple clients” |
| [15]       | “Cloud computing heralds the shift to an asset-free IT provisioning model where highly scalable hardware, software, and data resources are available over a network” |
| [16]       | “a network solution for providing inexpensive, reliable, easy and simple access to IT resources” |
| [17]       | “Cloud computing as the name suggests is a technology through which exchange of information and software management could be done through virtual means” |
| [18]       | “Cloud computing simply involves the provision of information technology (IT) solutions as a service rather than as a product through the Internet” |
| [19]       | “a parallel and distributed computing system consisting of a collection of connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers” |
| [20]       | “A style of computing where massively scalable IT-related capabilities are provided as a service across the Internet to multiple external customers” |
| [21]       | “A pool of abstracted, highly scalable, and managed infrastructure capable of hosting end-customer applications and billed by consumption” |
| [22]       | “The illusion of infinite computing resources available on-demand, the elimination of up-front commitments by cloud users, and the ability to pay for use of computing resources on a short-term basis as needed” |
| [23]       | “Cloud computing embraces cyber-infrastructure, and builds on virtualization, distributed computing, grid computing, utility computing, networking, and Web and software services” |
| [24]       | “A type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers” |
| [25]       | “A large pool of easily usable and accessible virtualized resources (such as hardware, development platforms, and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure provider using customized SLAs” |
| [26, 27]   | “Cloud Computing is primarily a new business paradigm that enables on-demand access, elasticity, pay-per-use, connectivity, resource pooling, and abstracted infrastructure” |
| [28]       | “a style of computing in which massively scalable IT-related capabilities are provided as a service using Internet technologies to multiple external customers” |
| [29]       | “a service model that combines a general organizing principle for IT delivery, infrastructure components, an architectural approach, and an economic model—basically, a confluence of grid computing, virtualization, utility computing, hosting and software as a service (SaaS)” |
| [30]       | “an emerging IT development, deployment, and delivery model enabling real-time delivery of products, services, and solutions over the Internet (i.e., enabling cloud services)” |

Merrill Lynch, 2008
“Cloud Computing is the dynamic provisioning of computing capabilities (hardware, software or services) provided by a third party via the network”
does little to reduce the development effort required to move the application to the selected CSP, for example, if it performs poorly. To fill in the gaps mentioned above, the cloud community has long advocated for CASB to act as a middleman between CSCs and CSPs, reducing the risk of choosing the wrong CSP. A CASB is a middleman between CSCs and CSPs who helps CSCs make decisions and improve service delivery (Barker et al. 2015) [39]. The range of difficulties surrounding CASB has prompted so much study that it is necessary to evaluate suggested solutions methodically. Few studies have looked into CASB research initiatives such as methodologies of selection of cloud services [40], cloud portability and interoperability [41], and different mechanisms of resource allocation [42], enhancing the security of cloud environment with CASB [43], different CASB policies [43], and Fuzzy CASB for requirements negotiation and prioritization [44]. They have discussed CASB from the perspective of a CSP, with a focus on portability and interoperability between CSP cloud services (i.e., IaaS, SaaS, PaaS, etc.). Furthermore, to our knowledge, no SLR on RSM Analysis-based CASB has been conducted, which is essential to assess progress in this subject and recommend dimensions for future research. This article presents the findings of an SLR conducted on the topic of RSM Analysis based CASB.

An SLR distinguishes, categories, and changes comparative suggestions of the current research and centers on information exchange within the research community [45]. Moreover, for this article, an SLR was carried out, with the essential aim to make out, taxonomically categorize, and methodically compare the existing research, based on arranging, implementation, and approving the relocation of bequest frameworks for CASB-based programs.

In this regard, the contribution of this article is to examine and evaluate existing solutions in terms of:

- researching methods for designing and implementing CASB;
- providing a thorough overview of existing CASB strategies, as well as how they have been applied to a cloud computing environment;
- having a fundamental understanding of the functions performed by CASB;
- highlighting areas for a future study where improvements can be made and recognizing the fundamental limits of present solutions;
- investigating the reasons behind the demand for CASB;

More particularly, the article endeavors to answer the following questions, through conducting a methodological review of existing research:

1. What are the driving strengths behind CASB for cloudsecurity?
2. What are the current assignments, strategies, and processes to fortify CASB of legacy on-premise software to cloud environment? Additionally, What is the relevant existing research themes?
3. What measures ought to be taken in arrange to create future research direction about measurements in legacy to-cloud CASB?

Table 1 (continued)

| References | Definition of Cloud Computing |
|------------|------------------------------|
| [Authors]  | The processing of heterogeneous data and delivery of computing services (like storage, databases, networking, software, analytics, computing power, and intelligence) via the remote servers hosted on internet is called cloud computing |

Table 2 Cloud service models

| S. No | Domain                          | Services                                               |
|-------|---------------------------------|--------------------------------------------------------|
| 1     | Computational resources         | IaaS (Infrastructure as a service)                     |
| 2     | Cloud software environment      | PaaS (Platform as a service)                           |
| 3     | Communication                   | CaaS (Communication as a service)                      |
| 4     | Storage                         | DaaS (Database/Development/Desktop as a service)       |
| 5     | Firmware/hardware               | HasS (Hardware as a service)                           |
| 6     | Software applications            | SaaS (Software as a service)                           |
| 7     | Business applications            | BaaS (Business as a service)                           |
| 8     | Network applications             | NaaS (Network as a service)                            |
| 9     | Organizational structure         | OaaS (Organization as a service)                        |
| 10    | Framework                       | FaaS (Framework as a service)                          |
| 11    | Any other domain                | XaaS (Anything as a service)                           |
The motive behind this work is to uniformly distinguish and categorize available resources on encryption and decryption of CASB [46]. Thereafter, correspondingly providing comparative analysis and foundations of the current research work.

The remainder of this article consists of seven sections: Sect. 2 present the related work. Section 3, defines the details of the CASB for the disciplined working of CC. Section 4 presents an understanding of the research process. Section 5 demonstrates the vulnerability. Section 6 shows the outcomes of this SLR and deliberates the solutions of the RQs. Section 7 represents the RSM analysis using CCD model for the CASB system. Section 8 analyzes the open challenges, issues, and future directions. Finally, Sect. 9 presents the conclusion and future research directions.

2 Related work

CASB is a big but fragmented area, with significant differences in contributions and the terminology used to describe them in academic papers. To our knowledge, this is the first survey that addresses this discrepancy and, in doing so, provides a full review of the state-of-the-art as well as precise and well-supported recommendations for future work. Table 3 shows the related previous work.

Although the proposed approach is comparable to theirs in some ways, the proposed analysis is from the standpoint of the CSC (i.e., how the CASB benefits the CSCs), whereas theirs is from the perspective of the CSP (i.e., the interoperability and collaboration between the CSPs). Other aspects of CC have been studied, including design [57], resource management [58] and [59], monitoring [60], migration [61], service composition [62], and security [63] and [64].

3 Cloud access security brokers

Cloud is the new place to store data, applications, and resources nowadays but the cloud providers are not able to ensure the secure experience of using the cloud. CASB could be a prelude educate inside the field of CC whose aim is to recognize and survey all the cloud applications in use, give dealing with sensitive data, encrypt or tokenize sensitive substance to uphold the privacy, security, and workable make use of cloud organizations over a few cloud platforms [35]. CASB may be a colossal but ambiguous field. There is a critical conflict between commitments and the expression utilized to depict them in investigation papers. In [35], Gartner envisions the CASB as a course of activity of four interconnected columns, i.e., “visibility”, “compliance”, “data security”, and “threat protection” as depicted in Fig. 1. CASBs are a data-key arrangement for securing data end-to-end, from any application to any gadget. Whereas early cloud security solutions were centered on SaaS security, CASBs have advanced into wide stages that ensure information over SaaS, IaaS, and private cloud applications. CASB works as a tool that sits between an organization’s premises framework and a cloud provider’s framework. As per the demand of organizations, which are transiting from internal bound-based applications to the cloud, deep visibility over corporate data as well as IT administrators’ granular control over data access is provided by CASBs by intermediating or “proxying” traffic between cloud applications and end-user devices. The movement of “packets” between users and applications essentially changes the strength of cloud and mobility. This has raised a necessity to adjust the list and the expenditure preferences in security controls for exhausting cloud services by any organization. By 2022 (Strategic Planning Assumptions) 60% of tremendous wanders will utilize a cloud CASB arrange for their cloud organizations, which is up from less than 20% these days [65]. Even though 2023, at the smallest 99% of cloud security disillusionments will be the customer’s fault [65]. The applications of CC and the encouragement to CASB are portrayed in Table 4.

3.1 Challenges in CASB

In the SLR carried out, we have laid down (as shown by Table 5) various challenges within the CASB development and have attempted to reply to RQ2 by listing out different challenges that enterprises face, while adopting the CASB.

3.2 Best practices for CASB

Figure 2 shows the ten major categories of best practices for CASB in cloud computing.

3.3 Cloud security work flow and cloud security life cycle-A conundrum

Cloud computing faces two main challenges Security and Reliability. As any other client can access the client’s data in the cloud, this raises security issues in the cloud. Hackers could attempt to steal client data by authenticating using authorized user names and passwords, modifying the data, and making changes. So many techniques are available to achieve security in the cloud, such as Encryption, Authorization, and Authentication. Cloud security risks can be categorized into cloud users and cloud service providers. Some of the cloud security risks are Data leakage, Data breaches, and loss, Hacking, Denial of Service, malicious
Table 3 Related previous work

| References                  | Focus                                      | Description                                                                                                                                 |
|-----------------------------|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Eisa et al. [40]            | cloud services selection (CSS)             | The authors have examined three commercial CSP search tools that assist CSCs in finding cloud services. Several academic works on cloud selection have also been presented in the survey. The authors conclude that cloud brokers who can extend and apply cloud services selection tools to aid CSCs are needed. |
| Sun et al. [47]             | CSS                                        | In this work, state-of-the-art CSS approaches have been examined from five perspectives: “decision-making techniques”, “data representation models”, “cloud service attributes and characteristics”, “contexts”, and “goals”. |
| Sheikh and Navimipour [42] | CSS                                        | To our knowledge, it is the only other survey that clearly distinguishes between CSC and CSP-centric selection. |
| Aldawsari et al. [48]       | Selection of CASB                         | The authors have discussed that the current state-of-the-art fails to meet the demand for energy-efficient intermediaries, and have proposed concepts for an energy-aware CASB. |
| Barker et al. [39]          | Prominent commercial solutions             | Authors have examined popular commercial CASB solutions from an academic standpoint, putting them into one of four categories (“performance”, “migration”, “theoretical models”, and “data”), and laying forth a research agenda in light of their findings. |
| Grozev and Buyya [49]       | Brokering mechanisms                      | Grozev and Buyya (2014) investigated some early cross-cloud application brokering methods. |
| Bittencourt [50]            | Cloud federations                          | The authors have laid down the required functional and non-functional features for cloud federations by identifying the key architectures in the literature and evaluating these architectures based on the given functional and non-functional properties. |
| Al-Dhuraibi et al. [51]     | Cloud scaling                              | This paper has worked towards the identification of the element which contributes to a variety of particular cloud security challenges. |
| Loutas et al. [2011] [41]   | Interoperability challenge                 | The focus of Loutas et al. (2011) is on semantic divergence in the cloud ecosystem as a root cause of the interoperability problem. |
| Zhang et al. [52]           | Interoperability at the IaaS level         | The authors propose a high-level taxonomy of IaaS interoperability concerns, which includes everything from APIs and GUIs to “virtualization technologies”, “encryption techniques”, and “SLA verification”. |
| Kaur et al. [53]            | Survey and analyze                         | Kaur et al. (2017) investigate and compare methods for providing interoperability and portability in various inter-cloud models. |
| Jyoti et al. [54]           | Load balancing and service brokering       | This survey article compares and contrasts the various load balancing algorithms used in load balancers, as well as the brokering policies utilized for each service and its scheduling types. |
| Wiem Abderrahim et al. [55] | Cloud Services                             | The goal of this work is to offer a broker architecture that assures that the provided cloud service meets behavioral criteria in terms of dependability features at the infrastructure, platform, and service levels. |
| Ahmad et al. [43]           | Security of CC with CASB                   | In this research, a strategy for enhancing cloud security with CASB called Goal Oriented Security Issues Mind Map Generation (GOSIMMG) has been proposed. |
| Ahmad et al. [44]           | CASB Policies under COVID-19 Pandemic      | The authors found various new CASB policies for safeguarding data at work from home in this research. |
| Ahmad et al. [56]           | CASB for Requirements Negotiation and Prioritization | In this study paper, the authors present a fuzzy CASB-based technique for needs negotiation and prioritizing. Finally, a case study is used to demonstrate the use of CASB. |

insiders attack, and some shared technology issues. Authentication, authorization, data protection, etc., are some of the security aspects that cloud service providers must cover and basic security goals that need to constitute basic security principles, and it became more crucial as data move to the cloud. Trust of the cloud service provider (CSP) and its services is among the principal drivers of a customer deciding to migrate to a cloud platform or conform to the legacy framework [67]. Trust relies upon deciding whether the provider is responsible for all risks such as data protection, VM security, and other regulatory concerns. “Confidentiality, Integrity and Availability” are the three considerations considered during the cloud system security review (CIA) [68]. This section’s primary objective is to generalize security requirements for the modern cloud infrastructure since the CIA domain is the commonly used method for defining security vulnerabilities in the conventional information system. Figure 3
Fig. 1  Pillars of sCASBs [48]

Table 4  Applications of CASB

| S.No | Author’s/year/title/ID                                                                 | Domain               | Applications                      |
|------|---------------------------------------------------------------------------------------|----------------------|-----------------------------------|
| 1    | Jon Friedman Mark Bouchard et al. (2015), “Definitive Guide to Visibility, Security, and Compliance for Applications and Data in the Cloud | Business Applications | Salesforce, Ariba                 |
| 2    | Jon Friedman Mark Bouchard et al. (2015), “Definitive Guide to Visibility, Security, and Compliance for Applications and Data in the Cloud | Productivity Applications | Office 365, Google Apps          |
| 3    | Jon Friedman Mark Bouchard et al. (2015), “Definitive Guide to Visibility, Security, and Compliance for Applications and Data in the Cloud | Cloud Drives and collaborative applications | Box, Dropbox, OneDrive, Google Drive |

Table 5  CASB challenges [66]

| S.No | Challenges                                                                                                                                                                                                 |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Many IT organizations miss the mark to frequently include executive staff and business units when developing a cloud approach, identifying business-critical cloud apps in use, mitigating cloud risk, and educating cloud users                  |
| 2    | Many enterprises are not conscious of all the cloud services and data in use all over the organization. Most have 20 times more apps in use than they would estimate                                                  |
| 3    | Most enterprises cannot identify, classify, granularly control access to, and manage to encrypt/decrypt handling of sensitive data, compliance-related data in these apps, even when cloud services are known            |
| 4    | CASBs provide a combination of user-centric and threat-centric capabilities as well as a range of deployment options, increasing the complexity of evaluation                                                                                       |
| 5    | Many enterprises have no way to detect cloud threats such as malware, account compromises, data destruction, data theft, and account compromises                                                                                          |
| 6    | Most organizations apply the same controls to all cloud-sensitive data, compliance requirements (FRs and NFRs), regardless of data type, or data sensitivity                                                                                  |
| 7    | Focusing disproportionately on the prevention of cloud data loss, risky user behavior, and account compromise, many organizations manage the sensitive need for threat detection, post-incident response, and continuous monitoring |
depicts the essential features of data security in cloud computing, as well as potential risks and defense techniques [69].

### 3.4 Confidentiality and privacy

The security of some business properties from exposing unauthorized users implies secrecy. Consumers like unauthorized access to data stored in the same database in a cloud world as the CSP data may be clients. The CSP itself can even include unethical or nefarious representatives who may access or even tamper with confidential, sensitive consumer data. Besides client info, the network of virtual computers, virtual pictures, etc., ultimately need secrecy.

Certain confidentiality concerns related to cloud data include:

- A variety of cloud storage services send content to customer data-containing web folders.
- Another aspect that impacts data security is the whole geographical area of the client’s information.

Cloud services are believed to be reliable but odd in some cases. They want to hear more about the details of personal data files and user privilege data. They want to hear more about the contents of user data files and user privilege data. The owners should formulate appropriate access management procedures to prevent specific scenarios.

The security of information systems, according to (Dukes 2015) [70], is characterized as “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability”. There are three main security services:

#### 3.4.1 Integrity

Integrity applies to an asset’s security property that ensures that it has not been changed by third-party employees who are not allowed to do so. Consequently, the accuracy and correctness of the asset concerning its owner are ensured by this property. Typically, inserting, removing, or modifying operations are assumed to alter the integrity of any support. With the user accessing cloud resources through web browsers, all web attacks in the cloud environment are widespread, causing user file contents, database, virtualized storage, or, indeed, WSDL files to be changed [71–75]. The following problems of data security were addressed here under the separate integrity specifications of the public cloud:
3.4.2 Data outsourcing

The outsourcing of data at the CSP end constitutes a direct challenge to its credibility. CSP will be able to erase any legitimate consumer data tuples, which the customer could never create.

3.4.3 Insecure API

The web developer has used the insecure API from Obscure sources for a lot of time, where the API key can lead to the attacker.

3.4.4 Collision attack

A collision attack is an operation that can merge several copies of media or other files to create a new copy. The tasks that include, but are not limited to, are data averaging, substitution, linear data mix, etc.

3.4.5 Wrapping attack

Is another common network attack that is naturally extremely likely to occur for cloud systems. The text and signature are duplicated and sent to the server as an authentic user during SOAP translation in TLS (Transport Layer service) layer.

3.4.6 Availability

Demand is one of the most critical protection factors to be maintained by a CSP. Multiple business organizations who utilize cloud-based technology to support their consumers should guarantee that these services remain available as a minor downtime will result in a significant irrecoverable financial loss. A standard service-level agreement lays out what the supplier has promised to supply and respond to demand. For, e.g., the service level could state that 99.999 percent of the time, if more than 80% of the support given is used, the programs will be utilizable, and more resources will be dynamically available.

3.4.7 Actors in cloud computing

In terms of responsibilities and roles, the reference architecture identifies five main actors (as shown by Fig. 4). Cloud consumers, cloud providers, cloud auditors, cloud brokers, and cloud carriers are among the actors [76, 77].

Cloud consumer Who (person/organization) maintains business relationships with Cloud Providers and uses their services?

Cloud provider A (person/organization/entity) guarantees that a service is available to those who are interested.

Cloud broker A third party that can estimate cloud services, performance, information system operations, and security of cloud installation separately.

Cloud carrier An intermediary that provides cloud service connectivity and transmission (from CPS to Cloud Consumers). Once a person is familiar with the cloud security workflow and cloud security lifecycle [see Figs. 5 and 6], one can adopt CASB and other cloud security solutions to provide full coverage for cloud applications usage [66].

3.5 CASB management portal

Enterprise CASB management portal should plan to integrate with their existing identity sources such as compute,
data services, data storage, app services, and CASB pillars as shown by Fig. 7.

3.6 CASB use cases

In the SLR work, various use cases in the CASB process have been identified (refer to Table 6).

3.7 Identifying and protecting sensitive cloud data

In this SLR work, various sensitive cloud data processes have been identified (refer to Table 7).
4 Research methodology

To distinguish the research gaps with the help of a literature survey of the CASB; we have applied the steps proposed by Kitchenham and Charters [79]. The steps include “research questions” (RQs), “search strategy”, “study selection”, and “data synthesis”. These steps form the backbone of our review protocol.

4.1 Research questions (RQs)

The objective of this study is to get how different CASB frameworks were developed from the beginning of the state charts to cloud services and to identify an area for further research by considering the strength and weaknesses of the existing services. To achieve this objective, the following research questions (RQs) were formulated (Table 8):

4.2 Search policy

We have figured out the subsequent search string to extract the essential studies from five electronic database assets, i.e., “IEEE Xplore”, “ACM Digital Library”, “Springer”, “Science Direct”, and “Google Scholar”, based on the RQs given in Table 9. Based on the RQs listed above, we have created the search string as depicted below.

Search string (SS): (\(\text{Cloud OR cloud computing OR cloud access security broker OR RSM, PICO method, and CCD Model}\)) AND (\(\text{Cloud Simulators OR challenges of CASB OR automation OR limitations OR weaknesses OR strength OR advantages OR disadvantages}\)) AND (\(\text{review OR systematic review OR literature review OR systematic}\))
literature review OR survey OR journey OR literature mapping OR systematic literature mapping OR state-of-the-art). The succeeding SSAs shown by Table 10 issuitably intended by using keywords, which are resulting from RQs through the PICO method. These SS are constructed by using Boolean ORs and ANDs.

This plan works in satisfying the queries related to key research questions successfully. SS was developed by using keywords. SSIs structured by finding outsubstitutes and different orthographic studies for each of the query components and connecting them by using the Boolean OR and Boolean AND. Keywords are determine during the Population Intervention Comparison Outcomes (PICO) process [79] as shown by Table 8 and are used to make. The basics components of PICO are listed as under:

1) Population: The population could be any of the particular part, application, and the state of CASB.

   - Population – cloud computing.

2) Intervention: The intervention is the tool innovation or method that addresses a particular issue.

   - Intervention – CASB.

3) Evaluation Usually a device or innovation or strategy with which intercession is being compared.

   - Evaluation – Legacy on-premises application.

4) Results: Results should co-relate to factors of ranks to practitioners such as improved security, consistence, and cost assistance. All results ought to be indicated.

   - Results – Encrypt/Decryptframework for CASB, better performance, cost asset, applications, upgraded security features, methods, and tools.

### 4.3 Determination procedure

We also evaluated the pertinence, reliability, and applicability of the selected studies through some QA questions that include. Figure 8 shows the determination procedure for the same. In the first stage of the process, we have
| S. No | Domain | Category | Description |
|------|--------|----------|-------------|
| 1    | Adopt Adaptive Access Control | Manage cloud access | Protecting cloud app usage is to integrate CASB with an authentication service, preferably one that leverages device and behavior profiling to block risky login attempts. |
| 2    | Uncover and rate cloud applications | Identify and rate cloud apps | Use CASB to:  
- Uncover apps on your network  
- Provide a security risk assessment on each app  
- Assist in the process of determining which apps should be allowed, or replaced with safer alternatives. |
|      |        | Upload logfiles | Upload logfiles to CloudSOC Audit for Shadow IT discovery. |
|      |        | Anonymize logfiles | Anonymize logfiles before uploading to Audit. |
| 3    | Plan data governance strategy | Determine corporate app business requirements | Consult with Executive Stakeholders to:  
- Negotiate substitutes for non-secure apps  
- Identify business-critical apps  
- Look at policy exceptions for non-secure apps without alternatives. |
|      |        | Block non-secure cloud apps | Block access to cloud apps that don’t meet your organization’s risk tolerance. |
| 1    | Plan data governance strategy | Determine corporate data security requirements | Before defining your cloud security strategy, consult with executive stakeholders to identify:  
- Sensitive data types  
- Data loss risk tolerance by data type  
- Compliance requirements. |
|      |        | Define DLP dictionaries | Based on discussions with stakeholders, define dictionaries for cloud DLP, i.e.:  
- Gambling  
- Violence  
- Obscenities. |
|      |        | Define content risk security profile | Apply a risk severity rating to all data types that would be most damaging if leaked:  
- High (H)  
- Medium (M)  
- Low (L)  
- Critical. |
|      |        | Classify cloud data | Classify data as:  
- Computing  
- Business  
- Secure code  
- Engineering  
- Health  
- Legal  
- Design  
- Digital certificates. |
|      |        | Identify risk types | Identification of sensitive compliance data like as:  
- External DLP  
- Virus/Malware. |
|      |        | Identify over-exposed sensitive data | The category of sensitive/risky data as:  
- Internally exposed data  
- Externally exposed data  
- Publicly exposed data. |
|      |        | Determine user risk | Based on cloud use behavior and file sharing, categorize the user as:  
- High risk  
- Medium risk  
- Low risk. |
| S. No | Domain | Category | Description |
|-------|--------|----------|-------------|
| 4 | Establish data use policy | Validate data governance strategy | Collaborate with executive management Bus, to identify a data governance strategy. Set policies based on:  
- Monitoring and removing exposures of sensitive files  
- Protecting your data from risky user behavior  
- Monitoring and controlling file-sharing behavior  
- Monitoring and controlling file uploads and downloads  
- Monitoring and controlling user access and activities in cloud services (IaaS, PaaS, SaaS, IDaaS) |
| 5 | Set Threat Detection Thresholds | Set Threshold Based Incident Detection Strings | We can set duration and importance of threshold-based on activities:  
- Critical  
- Less important  
- Important  
- Very Important |
| 5 | Set Threat Detection Thresholds | Set Sequence-Based Incident Detection Strings | Develop sequence-based detectors:  
- Importance  
- Steps  
- Duration |
| 6 | Monitor Cloud Accounts for Violations and Threats | Respond to Policy Violations | Policy violations responses may include:  
- Set link expiration  
- Remove shared link  
- Email, text, or ticket alert  
- Update file permissions  
- Export Data  
- Export data for offline analysis  
- Rate Threat Incidents  
- Set rate incidents as:  
- Low risk  
- Medium risk  
- High risk  
- Detect/ Block Malware  
- Identify and block the traditional malware  
- Detect/Classify Risky Behavior  
- Group/Classify threat incidents as:  
- Account takeover  
- Data exfiltration  
- Data destruction |
| 7 | Investigate Post Incident | Post Incident Response | Respond to incidents by:  
- Revising policy in consultation with executive management  
- Educating users  
- Developing an audit report  
- Post Incident Investigation | Perform a deep dive analysis on historical cloud activity |
| 8 | Generate reports | Schedule Reports | Need to schedule daily, weekly, monthly, yearly report  
- Create Dashboards Reports and Infographics | Need to create dashboard, reports, and infographics for executive staff |
selected 173 studies from “IEEE Xplore; ACM Digital Library; Springer; Science Direct; Google Scholar. CC Journal, and Journal of Object Technology (JOT)”. Some of these selected studies were found to be redundant and irrelevant after being scrutinized based on the title and thus were removed from the SLR. Consequently, 82 primary studies were short listed. In the next phase, the selected papers were further reviewed based on abstract and conclusion. Thus, after this phase, 41 studies were shortlisted. Further in the selection process, quality assessment (QA) criteria were employed on the selected studies. Finally, 20 studies were identified and selected after the study selection process. These selected studies, grouped as primary studies, are used to answer the formulated RQs. We also

Table 8  Research questions and their motivation

| RQs     | Motivation                                                                 |
|---------|-----------------------------------------------------------------------------|
| RQ-1    | What is the motivation for designing CASB?                                  |
|         | The goal is to determine which aspects of cloud security have been investigated and which aspects have not |
| RQ-2    | What are the functionalities of a CASB have?                               |
|         | The idea is to identify the way over which any explicit security issue has been determined in its ongoing research |
| RQ-3    | What are the approaches for engineering CASB?                              |
|         | The goal of the ongoing research is to determine the current methodologies in cloud security frameworks, as well as the true reason for organizations not implementing CASB and how it has been allocated. |
| RQ-4    | What are the simulation tools available for CC research?                    |
|         | The idea is to exchanging authentication and authorization data between parties (service and identity providers), “unauthorized redistribution of digital media”, “continuous data monitoring”, “investigate and response to exceptions”, “business process modeling”, and “threat protection” |

Table 9  RQs and SSs

| RQs     | Search strings (SS)                                                                 |
|---------|------------------------------------------------------------------------------------|
| RQ-1    | (Motivation OR Requirement OR Advantages) AND (Cloud Computing OR Cloud Access Security Broker OR Limitation OR Implementation) |
| RQ-2    | (Challenges OR Issues OR Security Issues) AND (Cloud Computing OR Cloud Access Security Broker OR CASB Development OR Requirements) AND (Security or Issues OR Loopholes OR Threats) |
| RQ-3    | (Cloud Computing OR CASB OR Weakness OR Strength OR Advantages OR Disadvantages) AND (Tools OR Implementation OR CASB Framework OR Methods OR Benchmark) |
| RQ-4    | (Cloud Computing OR Cloud Access Security Broker OR Limitation) AND (Ongoing state OR SLR OR Systematic Literature Review) AND (Encryption/Decryption process OR Cloud OR CASB) |

Table 10  RQs and keywords

| RQs     | Motivation                                                                 |
|---------|-----------------------------------------------------------------------------|
| RQ-1    | Why is there an urge to go to CASB?                                         |
|         | Functional and Non-functional requirements, need, benefits, motivation, limitation, and cloud |
| RQ-2    | What are the challenges in CASB?                                            |
|         | Challenges, issues, process, cloud, security, broker                        |
| RQ-3    | What are the live methods or tools for CASB?                                |
|         | Existing process, tools, criteria, CASB framework                           |
| RQ-4    | What is the ongoing state and ongoing research issues for CASB?             |
|         | Current state, existing research issues, cloud, security, broker            |

Fig. 8  Search and selected process
evaluated the pertinence, reliability and the applicability of the selected studies through some QA questions that include (i) “Are the objective of the research clearly expressed?” (ii) “Is the proposed CASB clearly described?” (iii) “Are the services applied on some case study?” (iv) “Does the research add value to the academia or industry?”. Assessment of these questions was done based on the following weighting or scoring score: “YES = 1, NO = 0, and PARTIALLY = 0.5”. The selected 41 studies were evaluated on the premise of the over QA questions, and as a result, we have considered those things which have quality scores more noteworthy than 2 (50% of the rating score). Finally, 36 relevant papers using abstract were excepted from the starting inspected studies, and 20 most relevant papers were chosen in this SLR. Appendices 16 and 17 present the list of chosen studies and the quality scores of the chosen studies.

4.3.1 Criteria of inclusion

Table 11 was utilized to incorporate the chosen papers.

4.4 Criteria of exclusion

The excluded existing research article that did not meet the prerequisites expressed as appeared in Table 5 and the listed constraints:
- studies with no-peer reviewed
- abstracts and editorials
- articles shorter than six pages

4.5 Statistics fusion

The purpose of data synthesis is to abbreviate confirmation from the selected studies to verify the responses of the RQs. In this article, selected studies were created and implemented in the following ways:

- Information associated with RQ-1 has been presented by bar charts.
- RQ-2, RQ-3, and RQ-4 and RQ-5 have appeared in Pie charts which show the discussions as well as experimental results.

5 Vulnerability

Based on the strategies for searching, as per the previous discussions that contained different databases selecting criteria and quality criteria, studies were chosen to perform the SLR. Some possibilities still lie in missing studies as it is not practically possible to extract all the studies by only the usage of terms that appears in the RQs. To overcome this problem, extracted studies need to be scrutinized physically so that studies can be identified which were missed while searching initially. Besides the previous searches, articles from CC and CASB were also taken into consideration to figure out those studies that were not identified during the exploring procedure. To reduce the incorrectness of redundant data, a self-sufficient valuation is done by the author on the extracted studies based on the QA questions.

6 Discussions as well as experimental results

Based on our SLR, we have distinguished ten unmistakable studies distributed from 2011 to 2021, as shown in Figs. 9 and 10. Within the chosen articles, there are five journal articles, three conference articles, and 2 other articles.

6.1 RQ-1: how to assess CASB with their functionalities?

The following objectives shows the CASB functionalities:

| Table 11 Inclusion criteria |
|-----------------------------|
| Stages                      | Criteria                                                                 |
| Overall description         | English language, paper published in journals/conferences/web articles/workshop, non-duplicate, date of publication |
| Full text                   | Improved security, broker, advantages, loopholes, tools in CASB, presence of the empirical data in the article |
| Title, keywords, abstract   | Based on the contents, which matches to the RQs, based on keywords and SS |
| Introduction and conclusion | Focusses on answering the RQs, contains CASB |
| Revenue and deployment      | Sales of CASB products are required |
| Geography                   | At least two of the four key regional marketplaces must be competed in |
| Product configuration       | The product must be marketed as primarily satisfying stand-alone CASB use cases |
| Product features            | Gartner’s definition of a CASB must be met |
1. Form the hub of data (Server) that is concerned about the CASB, and felicitate the above information among the researchers.
2. To analyze more novelty in the field of CASB.
3. Characterize continuous arrangements within the area of CASB, and clear up the likenesses and differences between them employing a description system.
4. Simultaneously characterize of work that focuses on the methodology of CASB.

6.2 RQ-2: what are the key challenges for designing CASB?

RQ-2 focuses to identify the requirements, i.e., functional requirements (FRs) and non-functional requirements (NFRs) that have motivated the research and advancement of CASB. The purpose of this RQ is to find the dwares inside the CC degree that moved the assurance for CASBs. It has been established that CASBs are encourged by the necessities to address the following five key challenges [35]:

1. More enterprises’ insufficiency a complete understanding of the cloud managements they retain and threats they achieve, which makes similarity and security tough.

2. Although cloud administrations are known, numerous companies endeavor to reliably confirm the secured approach of exact information interior and over these divergent services.
3. Enterprises have no calculated way to uncover whether (and when) compromised unmanaged gadgets are utilized to urge cloud organizations.
4. The CASB gives an arrangement of access-centric and threat-centric efficiencies, creating the complexity of a decision.
5. Several enterprises have entered the CASB advertise with a wide extent of competencies and gets to, complicating likely enterprises and obscuring use cases.

6.3 RQ-3: what are the fundamental duties of a CASB?

RQ-3 recognizes the scope of forms that are executed by CASB to attain its goals. RQ-3 makes a difference to look at the breaches between the supportive gestures and effectiveness of the arrangement and thus recognize areas of future research direction in CASB. Eight fundamental duties have been extricated from the chosen articles from [31] i.e., (i) “Decision Support”, (ii) “Resource Monitoring”, (iii) “Policy Enforcement”, (iv) “SLA Transaction”, (v) “Application Deployment”, (vi) “Relocation”, (vii) “API (Application Programming Interface) Abstraction”, (viii) “VM (Virtual Machine) Interoperability”.

6.4 RQ-4: what are the techniques available for designing the CASB framework?

RQ-3 distinguishes building strategies utilized to execute CASB and analyzes affiliations between strategies and results. The objective of this RQ is to explore how CASB

---

**Fig. 9** Distribution of publication types of selected studies

**Fig. 10** Distributed of selected studies by years

**Fig. 11** Distribution of publication types of selected studies

**Fig. 12** Distribution of publication types of selected studies
| S. No | Simulators name | Proposed by | Description | Availability |
|-------|----------------|-------------|-------------|--------------|
| 1     | CloudSim [34]  | Calheiros and Buyya | “Capacities bolster for modeling, empowering consistent modeling, simulation of huge-scale computing information centers, additionally it customizes approaches for provisioning, has assets to virtual machines” | Open Source |
| 2     | CloudAnalyst [34] | Wickremasinghe | “The points to examine the conduct of web applications on a huge scale in a cloud environment and works to dissimilar simulation experimentation work out from programming work out” | Open Source |
| 3     | GreenCloud [34] | Dzmitry Kliazovich | “The simulator is utilized to create novel arrangements in checking, asset allotment, workload planning as well communication conventions, enhancement, and organizing foundation” | Open Source |
| 4     | iCanCloud [34] | Nunez | “It empowers an adaptable and fully customizable worldwide hypervisor and can conduct expansive tests” | Open Source |
| 5     | EMUSIM | Calheiros | “It is a coordinates engineering plan to predict service conduct on cloud platforms” | Open Source |
| 6     | GroudSim [34] | Ostermann | “It pays consideration to IaaS ranges of cloud and is conveniently extensible to back extra models like cloud capacity or platform as a service” | - |
| 7     | Network Groud Sim | Garg | “Support displaying of real cloud information centers conjointly summed up applications such as HPC, e-commerce, and workflows” | Open Source |
| 8     | SPECI | Sriram | “It is to recreate the capability and code of large information centers on the premise of the estimate of input and middleware plan policy” | - |
| 9     | DC(DataCentre) Sim | Tighe | “It is to accomplish the prerequisite for simulation tools for quick development and assessment of information center administration techniques” | Open Source |
| 10    | MDC Sim | – | “It helps the analyzer to show unmistakable hardware characteristics of different components of the information center like servers, communication joins, and switches that are collected from completely distinctive merchants and licenses estimation of power utilization” | Commercial |
| 11    | Open Cirrus | Hewlett-Packard | “Planned to back investigation into planning, provisioning, and administration of administrations at a worldwide, multi-datacenter scale” | Open Source |
| 12    | OCT | Grossman | “It planned to compare and evaluate performances of distinctive cloud computing frameworks and to scrutinize the capacity of making frameworks work together” | Limited |
| 13    | CDOSim [80] | Fittkau et al | “CDOSim toolkit is used to simulate cost and performance characteristics in the cloud deployment. Thus, CDOSim tool accurately predicts the execution time for each service provider” | Open Source |
| 14    | TeachCloud [81] | Y. Jararweh et al | “TeachCloud is the generalization of CloudSim, a research-oriented simulator that is used to extend and validate cloud computing. TeachCloud also allows students to experiment with the real cloud system at different cost conditions” | Open Source |
| 15    | DartCSim [82] | Li et al | “DartCSim defines a user-friendly interface and hence users can set the parameters of simulation such as cloudlets, network topology, and management algorithm with a visual interface” | Open Source |
| 16    | DartCSim + [83] | Li et al | “DartCSim + defines a resend mechanism to present a more realistic network model to resolve the failure of transmission” | Open Source |
| 17    | ElasticSim [84] | Cai et al | “ElasticSim supports the impacts of the task execution time probability distribution and the tightness of workflow deadlines on the scheduling strategies. Finally, ElasticSim has a graphical user interface to show the execution state in real-time” | Open Source |
| 18    | FederatedCloudSim [85] | Kohne et al | “The main goal of FederatedCloudSim is to test various types of cloud federations” | Open Source |
| 19    | FTCloudSim [86] | Zhou et al | “FTCloudSim toolkit is used for modeling the different service reliability enhancement methods. For investigating the performance of each approach, FTCloudSim triggers failure events and provides some performance metrics” | Open Source |
| 20    | WorkFlowSim [87] | Chen and Deelman | “WorkFlowSim is used for modeling Scientific Workflows in a cloud environment. Workflows in heterogeneous distributed systems show different levels of overheads that are explained based on computational operations and miscellaneous works” | Open Source |
| S. No | Simulators name | Proposed by | Description | Availability |
|-------|----------------|-------------|-------------|-------------|
| 21    | CloudReports [88] | Teixeira Sá et al | “CloudReports presents a complete report that includes the log of operations. It also draws different charts with detailed information for resources usage, virtual machine allocations, execution of cloudlets, and energy consumption of data center” | Open Source |
| 22    | CEPSim [89] | Higashino et al | “CEPSim adds a new model by the directed acyclic graphs (DAGs) to CloudSim. It tries to show continuous queries processing fast streams of data and execute these queries in various systems (i.e., including private, public, and multiple)” | Open Source |
| 23    | DynamicCloudSim [90] | Bux and Leser | “DynamicCloudSim models the external loads that are created due to sharing common resources with other machines and applications. Finally, DynamicCloudSim provides straggler VMs and failures to model fault-tolerant approaches” | Open Source |
| 24    | CloudExp [91] | Jararweh et al | “CloudExp simulator is used to address virtualization and business process management in cloud system. CloudExp has a suitable GUI for setting cloud configurations and showing results with charts. Finally, this simulator develops Mobile Cloud Computing (MCC) simulation framework” | Open Source |
| 25    | CM Cloud [92] | Alves et al | “CM Cloud can design any cost model using XML and support current cloud service providers such as Google, Microsoft Azure, and Amazon by retrieving values directly from their web pages dynamically” | Open Source |
| 26    | MR-CloudSim [93] | Jung and Kim | “MR-CloudSim is very common for large data processing that focuses on MapReduce computing model on CloudSim” | Open Source |
| 27    | UCloud [94] | Sqalli et al | “The architecture of UCloud used here is based on a hybrid cloud model that uses both public and private clouds and is developed using CloudSim” | Open Source |
| 28    | GDCSim [95] | Gupta et al | “GDCSim is expanded as part of the BlueTool (BlueTool is a computer infrastructure project funded by NSF). The purpose of this project is to provide suitable research infrastructures in both hardware and software to raise the level of awareness of the environmental importance of data centers operating worldwide” | Open Source |
| 29    | CloudNetSim [96] | Cucinotta and Santogidis | “CloudNetSim introduces CPU scheduling for hypervisor and at the guest OS levels. Moreover, it presents VM deployment and scheduling 33 algorithms with application models. It can model thousands of nodes with important QoS metrics” | Open Source |
| 30    | CloudNetSim + [97] | Malik et al | “CloudNetSim + + is the first cloud computing simulator to use actual physical properties of the network to model the distributed data centers” | Open Source |
| 31    | SecCloudSim [98] | Rehman and Anwar | “SecCloudSim provides a framework that researchers can develop the security characteristics such as encryption, decryption, encapsulation, authentication, and privacy assurance” | Open Source |
| 32    | CloudShed [99] | Tian et al | “CloudSched generates the distribution of service time, arrival process, and request distribution by a random function. It is used to present various resource scheduling strategies in the cloud. These strategies take into account CPU, storage and the network bandwidth of physical machines and virtual machines to avoid bottlenecks” | Open Source |
| 33    | SimIC [100] | Sotiriadis et al | “The main characteristic of SimIC is the automation of service distribution that is varied among decentralized meta-brokers” | Open Source |
| 34    | SCORE [101] | Fernández-Cerero et al | “SCORE tries to simulate the parallel scheduling, energy-efficient monolithic schema, and synthetic workloads. The empirical experiment proved that SCORE is an efficient and reliable framework for evaluating security, energy, and scheduling algorithm in cloud systems” | Open Source |
| 35    | GAME-Score [102] | Fernández-Cerero et al | “GAME-Score simulation tool is used to implement the scheduling model with the Stackelberg game and tries to model the energy-efficient IaaS of the clouds” | Open Source |
| 36    | DISSECT-CF [103] | Kecskemeti | “DISSECT-CF presents a more complete IaaS stack simulation. It allows to users to derive energy consumption from several resource usage counters” | Open Source |
Table 13  Input parameters for modeling in CCD

| Standard | Run | Vendor Profile(A) | Visibility & governance(B) | Compliance (C) | Threat protection (D) | Data security (E) | Vendor outcomes |
|---------|-----|-------------------|-----------------------------|----------------|-----------------------|------------------|-----------------|
| 1       | 2   | -1                | -1                          | -1             | -1                    | -1               | 58.6            |
| 2       | 11  | -1                | -1                          | -1             | -1                    | -1               | 60              |
| 3       | 28  | -1                | -1                          | -1             | -1                    | -1               | 62.4            |
| 4       | 36  | 1                 | -1                          | -1             | -1                    | -1               | 63.9            |
| 5       | 42  | -1                | 1                           | -1             | -1                    | -1               | 63              |
| 6       | 31  | -1                | 1                           | -1             | -1                    | -1               | 72              |
| 7       | 45  | -1                | 1                           | -1             | -1                    | -1               | 59.6            |
| 8       | 19  | 1                 | 1                           | -1             | -1                    | -1               | 65.7            |
| 9       | 23  | -1                | -1                          | -1             | -1                    | -1               | 59.6            |
| 10      | 8   | 1                 | -1                          | -1             | -1                    | -1               | 59              |
| 11      | 17  | -1                | 1                           | -1             | -1                    | -1               | 70.6            |
| 12      | 18  | 1                 | -1                          | -1             | -1                    | -1               | 63              |
| 13      | 5   | -1                | 1                           | -1             | -1                    | -1               | 63.1            |
| 14      | 43  | 1                 | -1                          | 1              | -1                    | -1               | 65.9            |
| 15      | 48  | -1                | 1                           | 1              | -1                    | -1               | 62.7            |
| 16      | 34  | 1                 | 1                           | 1              | 1                     | -1               | 65              |
| 17      | 27  | -1                | -1                          | -1             | -1                    | 1                | 63.1            |
| 18      | 14  | 1                 | -1                          | -1             | -1                    | 1                | 63.9            |
| 19      | 35  | -1                | 1                           | -1             | -1                    | 1                | 69.2            |
| 20      | 39  | 1                 | -1                          | -1             | 1                     | 1                | 67              |
| 21      | 38  | -1                | -1                          | 1              | -1                    | 1                | 69.3            |
| 22      | 40  | 1                 | -1                          | 1              | -1                    | 1                | 72.8            |
| 23      | 47  | -1                | 1                           | 1              | -1                    | 1                | 61.7            |
| 24      | 13  | 1                 | 1                           | 1              | -1                    | 1                | 69.2            |
| 25      | 3   | -1                | -1                          | -1             | 1                     | 1                | 69.4            |
| 26      | 10  | -1                | -1                          | -1             | 1                     | 1                | 63.7            |
| 27      | 37  | -1                | 1                           | -1             | 1                     | 1                | 73.1            |
| 28      | 41  | 1                 | -1                          | -1             | 1                     | 1                | 65.7            |
| 29      | 50  | -1                | -1                          | 1              | 1                     | 1                | 65              |
| 30      | 9   | 1                 | -1                          | 1              | 1                     | 1                | 69.1            |
| 31      | 21  | -1                | 1                           | 1              | 1                     | 1                | 65.9            |
| 32      | 26  | 1                 | 1                           | 1              | 1                     | 1                | 62.7            |
| 33      | 49  | 2.37841           | 0                           | 0              | 0                     | 0                | 63.1            |
| 34      | 22  | 2.37841           | 0                           | 0              | 0                     | 0                | 63.6            |
| 35      | 7   | 0                 | -2.37841                    | 0              | 0                     | 0                | 64.9            |
| 36      | 33  | 0                 | 2.37841                     | 0              | 0                     | 0                | 66              |
| 37      | 40  | 0                 | 0                           | -2.37841       | 0                     | 0                | 62              |
| 38      | 12  | 0                 | 2.37841                     | 0              | 0                     | 0                | 68.9            |
| 39      | 30  | 0                 | 0                           | -2.37841       | 0                     | 0                | 61.6            |
| 40      | 46  | 0                 | 0                           | 0              | 2.37841               | 0                | 66              |
| 41      | 4   | 0                 | 0                           | 0              | 0                     | -2.37841        | 63.9            |
| 42      | 24  | 0                 | 0                           | 0              | 0                     | 2.37841         | 70.9            |
| 43      | 6   | 0                 | 0                           | 0              | 0                     | 0                | 64              |
| 44      | 32  | 0                 | 0                           | 0              | 0                     | 0                | 63.7            |
| 45      | 15  | 0                 | 0                           | 0              | 0                     | 0                | 64              |
| 46      | 29  | 0                 | 0                           | 0              | 0                     | 0                | 61.8            |
| 47      | 1   | 0                 | 0                           | 0              | 0                     | 0                | 65              |
| 48      | 44  | 0                 | 0                           | 0              | 0                     | 0                | 63.6            |
has been caught on. Six fundamental methods has been extracted from the chosen articles from [33] i.e., (i) “Enterprises-based”, (ii) “Framework and Models”, (iii) “Toolkits”, (iv) “Middlewares”, (v) “Semantics”, and (vi) “Pseudo Code/Algorithms”.

6.5 RQ-5: which cloud simulators are available for CC research?

The CC simulators [35] have been created for diverse sorts of modeling. For illustration, CC simulators have been created to bolster taking after documentations: the “SAML (Security Assertion Markup Language)” for trading verification and approval information between organizations (personality supplier and a benefit supplier), “DRM (Digital rights management)” for the illegal redeployment of computerized media, “Cloud DLP (Data loss prevention)” for incessant information observing, “SIEM (Security Information and Event Management)” for explore and react to special cases, “IAM (Identity and Access Management)” for trade handle modeling, and “IPSs (Intrusion Prevention Systems)” for risk security [35]. In expansion to the CASB-Simulators, we have distinguished 46 clouds simulators based on comparison which has been proposed for the modeling of highly sensitive data as shown by Table 12.

7 RSM analysis using CCD model for CASB

The experimental results were used as input for Research Surface Methodology (RSM) to obtain an empirical model. RMS is used to conduct many research works as [104]. For this, the five-level coding was employed for developing the model, three dependent parameters and four center values were considered. A model was developed that predicts vendor outcomes. The said model was seen on a polynomial equation obtained in terms of coded factors as shown in Table 13. The equations are developed to find the outcome for the vendor when the dependent and independent variables show correlation with each other. The predicted value of each can be depicted by Eq. 1. The equations developed for predicting the outcome for the vendor is as follows:

\[
\text{Outcome for Vendors} = +63.51 + 0.3114A + 0.2890B + 0.8522C + 0.2901D + 1.69E - 0.5719AB + 1.62AC - 1.34AD - 0.5469AE - 2.04BC + 0.5594BD - 0.4219BE - 0.9344CD - 0.6031CE - 0.1656DE + 0.0074A^2 + 0.3786B^2 + 0.3786C^2 + 0.0869D^2 + 0.7233E^2
\]

The condition in terms of coded components can be utilized to form desires nearly the reaction for given levels of each calculation. By default, the tall levels of the factors are coded as +1 and the moo levels are coded as −1. The coded condition is valuable for recognizing the relative influence of the components by comparing the figure coefficients. The values predicted from the model as well as actual values can easily be seen from Fig. 10. The principal component analysis (PCA) was used to assess the most influential parameters for vendors outcomes. This PCA has been done using Statistical Package for the Social Sciences (SPSS). The five components namely Vendor profile, Visibility and Governance, Compliance, Threat Protection, Office 365 security, IaaS, and custom apps security and data security were considered for the analysis. In terms of eigenvalue being greater than one, variance has been extracted as shown in Table 14. Component 1 i.e., Vendor profile explains about 52.13% of the variance in terms

| Vendor outcomes | Data security (E) | Threat protection (D) | Compliance (C) | Visibility & governance (B) | Vendor Profile (A) | Standard Run |
|-----------------|-------------------|-----------------------|----------------|----------------------------|-------------------|--------------|
| 64              | 0                 | 0                     | 0              | 0                          | 0                 | 49           |
| 61.7            | 0                 | 0                     | 0              | 0                          | 0                 | 50           |

Table 14  Determination of variance explained by components

| Component | Initial eigenvalues | Extraction sums of squared loadings |
|-----------|---------------------|------------------------------------|
| 1         | 2.607               | 52.132                             |
| 2         | 1.373               | 27.461                             |
| 3         | 0.604               | 12.084                             |
| 4         | 0.276               | 5.524                              |
| 5         | 0.234               | 2.11                               |
| 6         | 0.140               | 2.799                              |

| Component | Initial eigenvalues | Extraction sums of squared loadings |
|-----------|---------------------|------------------------------------|
| 1         | 2.607               | 52.132                             |
| 2         | 1.373               | 27.461                             |
| 3         | 0.604               | 12.084                             |
| 4         | 0.276               | 5.524                              |
| 5         | 0.234               | 2.11                               |
| 6         | 0.140               | 2.799                              |
of the Outcome needed for the Vendor. The variance can be best explained by using the criteria having a cumulative percentage greater than 90, the 6 variables that emerged to be influential are Vendor profile, visibility and governance, compliance, threat protection, and data security have a cumulative percentage of 91.677%. The vendor outcome is predicted from Central Composite Design (CCD) using research surface methodology. The model was randomized so that the best and most appropriate polynomial model can be judged. The model was analyzed using 50 randomized field outputs that were collected from a field study (Fig. 11).

The scree plot (as shown by Fig. 12) is a graphical representation of the component with its eigenvalue. The contribution of a component is assessed by its eigenvalue. The more the eigenvalue, the more is the contribution of that component in the vendor’s outcome. As shown in Fig. 11, there appears to be a strong contribution of the Vendor profile, visibility and governance, compliance, threat protection, and data security on vendors outcome out of six factors considered for the study. SaaS (software as a service) is becoming popular among businesses. Companies’ IT teams must oversee the safety of a potentially huge number of apps that handle sensitive data. Customers are responsible for protecting their data, even while the service provider has a robust security system in place (the provider does not understand the data semantics). The CASB is a newly developed system software type that can coordinate this form of security management (CASB). In addition to limiting application users’ access to resources, CASB guards against malicious code infiltrating the system. This system’s design pattern. In cloud ecosystems, they play a critical role (Fig. 13).

The KMO and Bartlett’s test has been considered for statistical analysis. KMO and Bartlett’s test also found some significant results. The Kaiser–Meyer–Olkin Degree of Sampling Adequacy came out to be 0.67. KMO test results of greater than 0.500 signify acceptable results. The foremost component examination requires that the likelihood related to Bartlett’s test of Sphericity be less than the level of

---

**Outcome for Vendors**

Color points by value of Outcome for Vendors:

58.6 | 73.1

---

![Scree Plot](image)

Fig. 11 The graph between Actual values and Predicted values

![Outcome for Vendors](image)

Fig. 12 Scree plot
importance. The probability related to the Bartlett test is \( < 0.001 \), which is also satisfied as it is 0.000. Thus, the result is satisfactory as per the KMO & Bartlett’s test and is presented in Table 15. Consumers may now benefit from a wide range of cloud-based products and services. Around 600 services are routinely used by most firms, mostly those of the SaaS kind. There may be a significant logistical challenge in controlling access to both external and internal resources since they might provide employees access to extremely sensitive corporate data. No matter how good a provider’s security architecture is, the customer is ultimately responsible for managing who has access to their critical data. There is a new system program that can help manage these apps, and it’s called the Cloud Access Security Broker (CASB). According to the literature review, there are now at least 14 different manufacturers of this product. It becomes a fundamental aspect of the institution’s IT governance framework when CASBs are implemented. 

![Contour graph of the predicted model](image)

**Table 15** Bartlett’s test and KMO

| Test and KMO                                | Value    |
|---------------------------------------------|----------|
| Kaiser–Meyer–Olkin measure of sampling adequacy | 0.671    |
| Bartlett’s test of sphericity               | Approx. Chi-Square 8.686 |
| Df                                          | 10       |
| Sig                                         | 0.562    |
manage a wide range of access scenarios, including mobile devices like smartphones, tablets, and laptops, as well as granting temporary access to cloud apps for certain users. It is also crucial to have CASBs as part of your cloud infrastructure. Software product line extension to encompass systems other than the product itself and their interactions with it is known as an ecosystem. As part of cloud ecosystems, the CASB offers network functionalities for cloud reference architecture. When a software product line architecture expands to incorporate systems outside the product, it is called an “ecosystem”. This ecosystem is defined by the Cloud Security Reference Architecture (SRA).

To determine the suitability of the models, Analysis of variance (ANOVA) and the statistical analysis including coefficient of determination, F value, and p value for each Vendors' outcome have been done and are listed in Table 15. Agreeing to ANOVA examination, for the more prominent values of F and P-value less than 0.05, it can be concluded that the models are factually critical. The tall values of the relationship coefficients moreover speak to the accuracy of the models to anticipate the reactions. The graphs of the 3D space model are as shown in Fig. 14. The graphs show the independence of variables and the outcome of the model space. The independent variable chosen from the PCA analysis was quite a significant influencing factor on the model and its outcomes. Within the same vein, the need for a fit test was not measurably noteworthy (p > 0.05) which demonstrated the tall wellness of the models. Concurring to the ANOVA test, a quadratic polynomial demonstration is measurably noteworthy to speak to the genuine relationship between reactions and the factors. Show F values of 13.32 with a little p value (< 0.0001) for all three reactions demonstrated the exactness of the show. A tall coefficient of assurance (R² = 0.90) demonstrated the capacity of anticipating the relationship between dependent and free variables. This design pattern explains how to protect a key component of a cloud ecosystem by allowing users to decide which cloud services they have access to. It will be validated as a pattern when designers implement it into their systems. The reaction surface plots were created for diverse intuition of any two independent factors, whereas keeping the esteem of the other variable consistent. The contour graph of the predicted model is as shown in Fig. 13, employing the range of space and independent variable locations.

**8 Issues, problems, and future trends**

The important CASB research concerns that have not yet been fully and properly studied as future research directions are described in this section. No support for multiple cloud service architectures (i.e., public, private, community, and hybrid cloud) and no ideal support for QoS features are common challenges for all CASBs. The CASB issues must be identified to assist future CASB designers in making them effective. In addition, some specific CASB in CC challenges are included below.

- To achieve zero execution time
- Reduced VM and data center costs, as well as data transfer processing time.
- Introduced multi-user-multi-key scenario typical at the cloud-scale for AWS.
- The CASB assists in the understanding of the person’s intended outcomes and assists in the organization of resources and assistance needed to attain these outcomes.

**9 Critical assessment and conclusion**

This study assists in building an understanding of numerous results in the sprout field of CASB. Thus, we proceed with an SLR to guarantee an exact investigation of such answers. We focused on correctly characterizing the ongoing state-of-art in CASB and recognizing key accomplishments and challenges with different aspects of any enterprise. To perform the search, twenty main papers were considered for the SLR of CASB. The search was conducted using seven major publication databases. We examined 173 papers from which we have considered 36 outlining worthy significance to the study topic. Understanding the different independent parameters influencing the CASB is studied using PCA. It was agreed that five parameters were influencing PCA analysis. For more understanding of these independent variables’ influence, on the CASB study, RSM analysis was employed. It was observed from the CCD model that the actual values showed significant influence with R² = 0.90.

In this review paper, we have identified some studies which focus on the services of CASB [105]. In expansion to this, CC services [106], cloud service choice for CASB [106], and CASB columns [107] are the dynamic states which have gotten consideration by the CC society for modeling with RSM and PCA analysis. The CC Simulators have been created for modeling the “SAML”, “DRM”, “Cloud DLP”, “SIEM”, “IAM” and “IPSs” etc. We have distinguished 36 supportive simulators for modeling the security prerequisites [34, 80–103]. In [35], it was pointed out that SLR within the state of CASB is disregarded cloud computing state by SLR. The applications, use cases, best practices, identifying and protecting sensitive cloud data/information of the continuous CASB have moreover been distinguished. Hence, in this article, a challenge has been made to fulfill this research gap. The major findings reveal that CASB has arisen as a cross-cloud model, driven by the heterogeneity and dimensionality of present cloud computing services, as well as the single-cloud paradigm’s inability to meet the needs of clients. The
The proposed CASB will be responsible for a variety of functions, including “assisting clients with decision-making”, “application deployment”, “SLA negotiations”, and “resource monitoring”. Our extensive meta-analysis reveals that CASB is still in its infancy. Even though tremendous progress has been made in this subject, significant challenges remain, which are also noted in this survey. We have identified several prospective avenues in the field of CASB based on our analysis and reflection:

- More work is needed in this area to aid CSCs in defining their applications’ requirements, adapting them, and intelligent decision-making approach about cloud providers (i.e., AWS, Microsoft AZURE, and Google Cloud Compute) and services (SaaS, IaaS, and PaaS).
- To create the CASBs system for the effective working of the Key Management System (KMS) is required [108].
- Outlining the important areas in which further research on the application of load balancing techniques in the CASB process can be developed [109].
- Examining future CC difficulties and the role that load balancing and CASB can play.
- No CASBs system has been coordinating with KMS. It is a critical issue how to integrate CASB with KMS.

Fig. 14 3D surface plot of Vendors output (i) Visibility % Governance vs Vendors Profile (ii) Compliance vs Vendors Profile (iii) Threat Protection vs Vendor Profile (iv) Data Security vs Vendors Profile.
• KMS has been broadly utilized in the cloud environment for safeguarding delicate data on the cloud [5]. More work is required to check the fitness of the CASB system with KMS.

• Employing the RSM analysis for the CASB system, it can be understood that, the different influencing variables can be analyzed separately. The independent variables have a future scope of deep research and understanding their interrelationship with each other and on the system.

Appendix

See Tables 16, 17.

Table 16 Included studies

| Paper ID | Complete reference |
|----------|--------------------|
| S1       | Hibatullah Alzahrani, “A Brief Survey of Cloud Computing”, Global Journal of Computer Science and Technology: Cloud and Distributed, Global Journals Inc. (USA), ISSN: 0975–4172 & Print ISSN: 0975–4350 |
| S2       | Gartner Report: How to Evaluate and Operate a Cloud Access Security Broker, December 8’ 2015 |
| S3       | Chuanyi Liu, Guofeng Wang, Peiyi Han, Hezhong Pan, Binxing Fang, “ A Cloud Access Security Broker Approach for Encrypted Data Search and Sharing”, International Conference on Computing, and Networking and Communications (ICNC): Cloud Computing and Big Data, 2017 |
| S4       | Sameer Singh Chauhan, Emmanuel S. Pilli, R.C Joshi, Girdhari Singh, and M.C Govil, “ Brokering in interconnected cloud computing environments: A survey”, Journal of Parallel and Distributed Computing, 2018 |
| S5       | Abdessalam Elhabbash, Faiza Samreen, James Hadley, and Yehia Elkhatib, “Cloud Brokerage: A Systematic Survey”, ACM Computing Surveys, Vol. 51, No. 6, Article 119, 2019 |
| S6       | Ioannis Patiniotakis, Yiannis Verginadis, and Ggregoris Mentzas, “PuLSaR: preference-based cloud service selection for cloud service broker”, Journal of Internet Services and Applications (2015), 6:26 |
| S7       | Prashant Khanna, Sonal Jain, “ Distributed Cloud Federation Brokerage: A Live Analysis”, 7th International Conference on Utility and Cloud Computing, 978–1-4799–7881-6/14, 2014 IEEE/ACM |
| S8       | https://pages.ciphercloud.com/rs/830-ILB-474/images/CipherCloud-CASB-Plus-Data-Sheet-v1.pdf |
| S9       | P. Khanna, and B.V. Babu, “ Cloud Computing Brokering Service: A Trust Framework”, in the Third International Conference on Cloud Computing, GRID’s and Virtualization, Nice, 2012 |
| S10      | C. N. Hofer, and G. Karagiannis, “ Cloud computing services: taxonomy and comparison”, J Internet Sev Appl 2011, 2:81–94 |
| S11      | Ahmad S., Mehfuz S., Beg J. (2021) Enhancing Security of Cloud Platform with Cloud Access Security Broker. In: Kaiser M.S., Xie J., Rathore V.S. (eds) Information and Communication Technology for Competitive Strategies (ICTCS 2020). Lecture Notes in Networks and Systems, vol 190. Springer, Singapore. https://doi.org/10.1007/978-981-16-0882-7_27 |
| S12      | S. Ahmad, S. Mehfuz and J. Beg, “Securely Work from Home with CASB Policies under COVID-19 Pandemic: A Short Review,” 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), 2020, pp. 109–114, https://doi.org/10.1109/SMART50582.2020.9337121 |
| S13      | S. Ahmad, S. Mehfuz and J. Beg, “Fuzzy Cloud Access Security Broker for Requirements Negotiation and Prioritization,” 2019 International Conference on Power Electronics, Control and Automation (ICPECA), 2019, pp. 1–6, https://doi.org/10.1109/ICPECA47973.2019.8975620 |
| S14      | Yahya Al-Dhuraibi, Fawaz Paraiso, Nabil Djarallah, and Philippe Merle. 2018. Elasticity in cloud computing: State of the art and research challenges. IEEE Transactions on Services Computing 11, 2 (March 2018), 430–447. https://doi.org/10.1109/TSC.2017.2711009 |
| S15      | Jyoti, A., Shirmali, M., Tiwari, S. et al. Cloud computing using load balancing and service broker policy for IT service: a taxonomy and survey. J Ambient Intell Human Comput 11, 4785–4814 (2020). https://doi.org/10.1007/s12652-020-01747-z |
| S16      | Kiranbir Kaur, Sandeep Sharma, and Karanjeet Singh Kahlon. 2017. Interoperability and portability approach in interconnected clouds: A review. Computing Surveys 50, 4, Article 49 (Oct. 2017), 1–49. https://doi.org/10.1145/3,092,698 |
| S17      | Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, and Joaquim Celestino Júnior. 2013. An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications 36, 1 (2013), 25–41. https://doi.org/10.1016/j.jnca.2012.08.007 |
| S18      | Amin Jula, Elankovan Sundararajan, and Zalinda Othman. 2014. Cloud computing service composition: A systematic literature review. Expert Systems with Applications 41, 8 (2014), 3809–3824. https://doi.org/10.1016/j.eswa.2013.12.017 |
| S19      | Ilia Iankoulova and Maia Daneva. 2012. Cloud computing security requirements: A systematic review. In Proceedings of the 6th International Conference on Research Challenges in Information Science (RCIS), 1–7. https://doi.org/10.1109/RCIS.2012.6240421 |
| S20      | Bandar Aldawsari, Thar Baker, and David England. 2015. Towards a holistic multi-cloud brokerage system: Taxonomy, survey, and future directions. In Proceedings of the IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 1467–1472. https://doi.org/10.1109/CTIT/UCUC/DASC/PICOM.2015.219 |
Table 17 Results of the quality scores of the selected studies

| Paper ID | QA1 | QA2 | QA3 | QA4 | QA5 | Score |
|----------|-----|-----|-----|-----|-----|-------|
| S1       | 0.5 | 1   | 0.5 | 1   | 0.5 | 3.5   |
| S2       | 0.5 | 0.5 | 0   | 0.5 | 1   | 2.5   |
| S3       | 0.5 | 0.5 | 1   | 1   | 1   | 4     |
| S4       | 0.5 | 1   | 0.5 | 0.5 | 1   | 3.5   |
| S5       | 1   | 1   | 0.5 | 1   | 0.5 | 4     |
| S6       | 1   | 1   | 0   | 1   | 0.5 | 3.5   |
| S7       | 0.5 | 0.5 | 0   | 0.5 | 1   | 2.5   |
| S8       | 1   | 1   | 0.5 | 1   | 1   | 4.5   |
| S9       | 0.5 | 0.5 | 0.5 | 1   | 0.5 | 3     |
| S10      | 1   | 0.5 | 0.5 | 0.5 | 1   | 3.5   |
| S11      | 1   | 1   | 0.5 | 1   | 1   | 4.5   |
| S12      | 0.5 | 0.5 | 1   | 0.5 | 1   | 3.5   |
| S13      | 1   | 1   | 0.5 | 1   | 0.5 | 4     |
| S14      | 0.5 | 0 | 0.5 | 0.5 | 1   | 2.5   |
| S15      | 0.5 | 1   | 0.5 | 0.5 | 0   | 2.5   |
| S16      | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 2.5   |
| S17      | 0.5 | 0   | 0.5 | 0   | 0.5 | 1.5   |
| S18      | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 2.5   |
| S19      | 0.5 | 1   | 0.5 | 0.5 | 0.5 | 3     |
| S20      | 1   | 1   | 0.5 | 1   | 1   | 4.5   |

Author contribution SA, SM, FM-O and JB have the same contribution.

Funding None.

Data availability All data generated or analysed during this study are included in this published article.

Declarations

Conflict of interest All authors declares that they have no conflict of interest.

Informed consent None.

References

1. Rupa, C., Srivastava, G., Gadekallu, T.R., Maddikunta, P.K.R., Bhattacharya, S.: A Blockchain-Based Cloud Integrated IoT Architecture Using a Hybrid Design. In: Gao H., Wang X., Iqbal M., Yin Y., Yin J., Gu N. (eds) Collaborative Computing: Networking, Applications, and Worksharing. CollaborateCom 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, p. 350. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-67540-0_36
2. https://s3.amazonaws.com/files.technologyreview.com/p/pub/legacy/compaq_cst_1996_0.pdf.
process within the software engineering domain. J. Syst. Software 80(4), 571–583 (2007)
21. Vashishtha, M., Chouksey, P., Rajput, D.S., Reddy, S.R., Reddy, M.P.K., Thippa Reddy, G., Patel, H.: Security, and detection mechanism in IoT-based cloud computing using a hybrid approach. Int. J. Internet Technol. Secured Trans. 11(56), 436–451 (2021)
22. Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: State-of-the-art and research challenges. J. Internet Serv. Appl. 1(1), 7–18 (2010). https://doi.org/10.1007/s13174-010-0007-6
23. Manvi, S.S., Shyam, G.K.: Resource management for infrastructure as a service (IaaS) in cloud computing: a survey. J. Netw. Comput. Appl. 41, 424–440 (2014). https://doi.org/10.1016/j.jnca.2013.10.004
24. Zhan, Z.-H., Liu, X.-F., Gong, Y.-I., Zhang, J., Chung, H.S.-H., Li, Y.: Cloud computing resource scheduling and a survey of its evolutionary approaches. Comput. Surv. (2015). https://doi.org/10.1145/2788397
25. Aceto, G., Botta, A., de Donato, W., Pescape, A.: Cloud monitoring: a survey. Comput. Netw. 57(9), 2093–2115 (2013). https://doi.org/10.1016/j.comnet.2013.04.001
26. Jamshidi, P., Ahmad, A., Pahl, C.: Cloud migration research: a systematic review. IEEE Trans. Cloud Comput. 1(2), 142–157 (2013). https://doi.org/10.1109/TCC.2013.10
27. Jula, A., Sundararajan, E., Othman, Z.: Cloud computing service composition: a systematic literature review. Expert Syst. Appl. 41(8), 3809–3824 (2014). https://doi.org/10.1016/j.eswa.2013.12.017
28. Iankoulova, I., Daneva, M.: Cloud computing security requirements: a systematic review. In: Proceedings of the 6th International Conference on Research Challenges in Information Science (RCIS), pp. 1–7 (2012). https://doi.org/10.1109/RCIS.2012.6240421
29. Patel, A., Taghavi, M., Bakhtiyari, K., Celestino Júnior, J.: An intrusion detection and prevention system in cloud computing: a systematic review. J. Netw. Comput. Appl. 36(1), 25–41 (2013). https://doi.org/10.1016/j.jnca.2012.08.007
30. Gartner, R., By Analysts Craig Lawson, Riley, S.: Magic quadrant for cloud access security brokers. (2018)
31. Ahmad, S., Mehfuz, S., Beg, J.: A genetic algorithm based key management approach for enhancing data security in cloud environment. Int. J. Adv. Trends Comput. Sci. Eng. 9(5), 943–951 (2020)
32. Labati, R.D., Genovese, A., Piuri, V., Scotti, F., Vishwakarma, S.: Computational intelligence in cloud computing. In: Kivács L., Heidegger T., Szaka´l A. (eds) Recent Advances in Intelligent Science and Technology, NIST SP 500-292 (2011).https://doi.org/10.6028/NIST.SP.500-292.
33. Xiao, Z., Xiao, Y.: Security and privacy in cloud computing. IEEE Commun. Surv. Tutor. 15(2), 843–859 (2013). https://doi.org/10.1109/SURV.2012.060912.00182
34. Dukes, C.: Committee on national security systems (CNSS) glossary (2015)
35. Lakhan, A., Mohammed, M.A., Kadry, S., Abdulkareem, K.H., Taha AL-Dhiief, F., Hsu, C.-H.: Federated learning enables intelligent reflecting surface in fog-cloud enabled cellular network (2021) https://doi.org/10.1109/7717. peerj-cs.758
36. Lakhan, A., Mohammed, M. A., Kozlov, S., Joel, Rodrigues, J.P.C.: Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enabled IoT system for healthcare workflows (2021). https://doi.org/10.1002/ett.4363
37. Lakhan, A., Memon, M.S., Mastoi, Qua et al.: Cost-efficient mobility offloading and task scheduling for microservices IoVT applications in container-based fog cloud network. Cluster Comput. (2021). https://doi.org/10.1007/s10586-021-03333-0
38. Lakhan, A., Mohammed, M.A., Rashid, A.N., Kadry, S., Panityakul, T., Abdulkareem, K.H., Thinnukool, O.: Smart-contract aware ethereum and client-fog-cloud healthcare system. Sensors 21(12), 4093 (2021). https://doi.org/10.3390/s21124093
39. Lakhan, A., Mastoi, Q.-U.-A., Elhoseny, M., Memon, M.S., Mohammed, M.A.: Deep neural network-based application partitioning and scheduling for hospitals and medical enterprises using IoT assisted mobile fog cloud. Enterprise Informat. Syst. (2021). https://doi.org/10.1080/17517755.2021.1883122
40. Stallings, W.: Cryptography and network security principles and practice. 7th edition, Pearson Education Limited (2017) ISBN 10: 0-13-444428-0
41. Liu, F., et al.: NIST cloud computing reference architecture. Recommendations of the National Institute of Standards and Technology, NIST SP 500-292 (2011). https://doi.org/10.6028/NIST.SP.500-292
42. CASB Best practices guide, ensuring secure and compliant cloud app use with symantec (2017)
43. Kitchenham, B., Charters, S. Guidelines for performing systematic literature reviews in software engineering. Technical Report, Ver. 2.3 EBSE Technical Report. EBSE, EBSE-2007- (School of Computer Science and Mathematics). (2007)
44. Lakhan, A., Mohammed, M.A., Ibrahim, D.A., Abdulkareem, K.H.: Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoT environment, Journal of King Saud University - Computer and Information Sciences, (2021), ISSN 1319-1578. https://doi.org/10.1016/j.jsuci.2021.11.009.
45. Shafiq, A., Mebarek-Oudina, F., Sindhu, T.N., Rasool, G.: Sensitivity analysis for Walters’ B nanoliquid flow over a radiative Riga surface by RSM, Sciencia Iranica (2021). https://doi.org/10.24200/SCI.2021.58293.5662
46. Khanna, P., Babu, B.V.: Cloud computing brokering service: a trust framework. in the third international conference on cloud computing, GRID’s Virtualiz. Nice (2012)
47. Patniotakis, I., Verginadis, Y., Mentzas, G.: PuSaR: preference-based cloud service selection for cloud service broker. J. Internet Serv. Appl. 6, 26 (2015)
48. https://pages.ciphercloud.com/rs/830-ILB-474/images/CipherCloud-CASB-Plus-Data-Sheet-v1.pdf.
49. Fittkau, F., Frey, S., Hasselbring, W.: CDOSim: Simulating cloud deployment options for software migration support. In: IEEE 6th International Workshop on the Maintenance and Evolution of Service-Oriented and Cloud-Based Systems, pp. 37–46. (2012)
50. Jararweh, Y., Akshara, Z., Jarrah, M., Kharbutli, M., Alsaleh, M.N.: TeachCloud: a cloud computing educational toolkit. In: IBM Cloud Academy Conference, pp. 1–19. (2012).
51. Li, X., Jiang, X., Huang, P., Ye, K.: DartCSim: an enhanced user-friendly cloud simulation system based on CloudSim with better performance. In: IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, pp. 392–396. (2012)
52. Li, X., Jiang, X., Ye, K., Huang, P.: DartCSim+: enhanced CloudSim with the power and network models integrated. In: IEEE Sixth International Conference on Cloud Computing, pp. 644–651 (2013)
53. Cai, Z., Li, Q., Li, X.: ElasticSim: a toolkit for simulating workflows with cloud resource runtime auto-scaling and stochastic task execution times. J. Grid Comput pp. 257–272 (2016)
54. Kohn, A., Spohr, M., Nagel, L., Spinczyk, O.: FederatedCloudSim: an SLA-aware federated cloud simulation framework. In: Proceedings of the 2nd International Workshop on CrossCloud Systems. pp. 1–5. (2014)
55. Zhou, A., Wang, S., Sun, Q., Zou, H., Yang, F.: FICloudSim: a simulation tool for cloud service reliability enhancement
mechanisms. In: Proceedings Demo and Poster Track of ACM/IFIP/SUSENIX International Middleware Conference. (2013)
56. Chen, W., Deelman, E.: WorkflowSim: a toolkit for simulating scientific workflows in distributed environments. In: IEEE 8th International Conference on E-Science. (2012)
57. Teixeira Sá, T., Calheiros, R.N., Gomes, D.G.: CloudReports: an extensible simulation tool for energy-aware cloud computing environments. Cloud Comput. pp. 127–142 (2014)
58. Higashino, W.A., Capretz, M.A.M., Bittencourt, L.F.: CEPSim: a simulator for cloud-based complex event processing. In: IEEE International Congress on Big Data. pp. 122–139 (2015)
59. Bux, M., Leser, U.: DynamicCloudSim: Simulating heterogeneity in computational clouds. Future Generat. Comput. Syst. pp. 85–99 (2015)
60. Jararweh, Y., Jarrah, M., kharbutli, M., Alshara, Z., Alsaleh, M.N., Al-Ayyoub, M.: CloudExp: a comprehensive cloud computing experimental framework. Simul. Model. Pract. Theory 180–192 (2014)
61. Alves, D.C., Batista, B.G., Filho, D.M.L., Peixoto, M.L., Reiff-Marganiec, S., Kuehne, B.T.: CM Cloud simulator: a cost model simulator module for Cloudsim.In: IEEE World Congress on Services. 99–102 (2016)
62. Jung, J., Kim, H.: MR-CloudSim: designing and implementing MapReduce computing model on CloudSim. In: International Conference on ICT Convergence pp. 504–509 (2012)
63. Sqalli, M.H., Al-saeedi, M., Binbeshr, F., Siddiqui, M.: UCloud: a simulated Hybrid Cloud for a university environment, IEEE 1st International Conference on Cloud Networking. pp.170–172 (2012)
64. Gupta, S.K.S., Gilbert, R.R., Banerjee, A., Abbasi, Z., Mukherjee, T., Varsamopoulos, G.: GDCSim: a tool for analyzing green data center design and resource management techniques. In International Green Computing Conference and Workshops pp. 1–8 (2011)
65. Cucinotta, T., Santoguidis, A.: CloudNetSim - simulation of real-time cloud computing applications. In: Proceedings of the 4th Embedded and Real-time Systems (2013).
66. Malik, A.W., Bilal, K., Aziz, K., Klizovich, D., Ghani, N., Khan, S.U., Buyya, R.: CloudNetSim++: a toolkit for data center simulations in OMNET++. In 11th Annual High Capacity Optical Networks and Emerging/Enabling Technologies. pp. 104–108 (2014)
67. Rehman, U.U., Ali, A., Anwar, Z.: secCloudSim: secure cloud simulator. In 12th International Conference on Frontiers of Information Technology, pp. 208–213 (2014)
68. Tian, W., Zhao, Y., Xu, M., Zhong, Y., Sun, X.: A toolkit for modeling and simulation of real-time virtual machine allocation in a cloud data center. IEEE Transactions on Automation Science and Engineering. pp.153–161 (2015)
69. Sotiriadis, S., Bessis, N., Antonopoulos, N., Anjum, A.: SimIC: Designing a new inter-cloud simulation platform for integrating large-scale resource management. In: IEEE 27th International Conference on Advanced Information Networking and Applications. pp. 90–97 (2013)
70. Fernández-Cerero, D., Fernández-Montes, A., Jakóbik, A., Kołodziej, J., Toro, M.: SCORE: simulator for cloud optimization of resources and energy consumption. Simul. Modell. Pract. Theory. 82, 160–173 (2018)
71. Fernández-Cerero, D., Jakóbik, A., Fernández-Montes, A., Kołodziej,J.: GAME-SCORE: game-based energy-aware cloud scheduler and simulator for computational clouds. Simul. Model. Pract. Theory 93, 3–20 (2019)
72. Kececioglu, M.: DISSECT-CF: a simulator to foster energy-aware scheduling in infrastructure clouds. Simul. Modell. Pract. Theory. 188–218 (2015).
73. Liu, C., Wang, G., Han, P., Pan, H., Fang, B.: A cloud access security broker approach for encrypted data search and sharing. International conference on computing, and networking and communications (ICNC): Cloud Computing and Big Data, (2017)
74. Swarna Priya, R.M., Bhattacharya, S., Maddikunta, P.K.R., Somayaji, S.R.K., Lakshmanna, K., Kaluri, R., Hussien, A., Gadekallu, T.R.: Load balancing of energy cloud using wind-driven and firefly algorithms in the internet of everything. J. Parallel Distrib. Comput. 142, 16–26 (2020). https://doi.org/10.1016/j.jpdc.2020.02.010
75. Barr, J.: “Amazon EC2 Beta”. Amazon Web Services Blog. (2006)
76. Chauhan, S.S., Emmanuel, S.P., Joshi, R.C, Singh, G., Govil, M.C.: Brokering in interconnected cloud computing environments: a survey. J. Parallel Distrib. Comput. (2018)
77. Plummer, D.C., Smith, D.M., Bittman, T.J., Cearley, D.W., Mayank Kapoor (2011)
78. Konwinski, A., et al.: Above the clouds: a berkeley view of public and private cloud computing (2009) putingreport080307%5B1%5D.pdf.
79. Staten, J.: Is cloud computing ready for the enterprise? (2008) http://vu2aut.persiangig.com/ECCommerce/Forrester-Cloud-computingreporting8080307%5B1%5D.pdf.
80. Pradeep, D., Smith, D.M., Bitting, T.J., Cearley, D.W., Cappuccio, D.J., Scott, D., et al.: Five refining attributes of public and private cloud computing (2009) http://www.gartner.com/DisplayDocument?id=67182&refUrl=fromdoc
93. Vouk, M.A.: Cloud Computing-Issues, Research, and Implementations. J. Comput. Inf. Technol. 4, 235–246 (2008)
94. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud computing and emerging it platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Gener. Comput. Syst. 25(6), 599–616 (2009)
95. Vaquero, L., Rodero-Merino, L., Caeres, J., Lindner, M.: A break in the clouds: towards a cloud definition. SIGCOMM Comput. Commun. Rev. 39(1), 50–55 (2009)
96. Rosenthal, A., Mork, P., Li, M.H., Stanford, J., Koester, D., Reynolds, P.: Cloud computing: a new business paradigm for biomedical information sharing. J. Biomed. Inform. 43, 342–353 (2010)
97. Durkee, D.: Why cloud computing will never be free. Commun. ACM 8, 62–69 (2010)
98. Gartner (2008b) Gartner says contrasting views on cloud computing are creating confusion. Gartner press release, 29 September 2008.
99. Kusnetzky, D., Chalmers, R.: Partly Cloudy – Blue-Sky thinking about cloud computing, The 451 Group (2008)
100. Gens, F.: Defining “Cloud Services” and “Cloud Computing”. IDC eXchange (2008)
101. Rai, P.K., Bunkar, R.K.: Study of security risk and vulnerabilities of cloud computing. Int. J. Comput. Sci. Mobile Comput. 3, 490–496 (2014)
102. Sun, L., Dong, H., Hussain, F.K., Hussain, O.K., Chang, E.: Cloud service selection: state-of-the-art and future research directions. J. Netw. Comput. Appl. 45, 134–150 (2014). https://doi.org/10.1016/j.jnca.2014.07.019
103. Aldawari, B., Baker, T., England, D.: Towards a holistic multi-cloud brokerage system: taxonomy, survey, and future directions. In: Proceedings of the IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 1467–1472 (2015). https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.219
104. Grozev, N., Buyya, R.: Inter-cloud architectures and application brokering: taxonomy and survey. Software 44(3), 369–390 (2014). https://doi.org/10.1002/spe.2168
105. Assis, M.M., Bittencourt, L.F.: A survey on cloud federation architectures: identifying functional and non-functional properties. J. Netw. Comput. Appl. 72, 51–71 (2016). https://doi.org/10.1016/j.jnca.2016.06.014
106. Al-Dhuraibi, Y., Paraiso, F., Djarrallah, N., Merle, P.: Elasticity in cloud computing: state of the art and research challenges. IEEE Trans. Serv. Comput. 11(2), 430–447 (2018). https://doi.org/10.1109/TSC.2017.2711009
107. Zhang, Z., Wu, C., Cheung, D.W.L.: A survey on cloud interoperability: taxonomies, standards, and practice. SIGMETRICS Perform. Evaluat. Rev. 40(4), 13–22 (2013). https://doi.org/10.1145/2479942.2479945
108. Kaur, K., Sharma, S., Kahlon, K.S.: Interoperability and portability approach in interconnected clouds: a review. Comput. Surv. 50(4), 1–49 (2017). https://doi.org/10.1145/3092698
109. Jyoti, A., Shrimali, M., Triwari, S., et al.: Cloud computing using load balancing and service broker policy for IT service: a taxonomy and survey. J. Ambient Intell Human Comput 11, 4785–4814 (2020). https://doi.org/10.1007/s12652-020-01747-z
110. Gartner, plan and manage successful CASB deployment. Match security with agility and elasticity of the cloud. Tata Communication (2018)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
Javed Beg (Director of Product Manager-Oracle IAM and Cloud Security, Oracle-India) received the B.Tech. degree in Mechanical Engineering from Jamia Millia Islamia, India, in 1999, the MS degree in computer integrated manufacturing from IIT Madras, in 2001. Currently, he has been working in Oracle-India as a director of the product manager, for the past 3 years. He worked in different esteemed organizations like Oracle, TCS, IIT Madras, Wipro Technologies, Outworx, Saviynt, Inc. at different posts. He worked (July 1999-May 2001) as a research scholar at the manufacturing Engineering section, Hindustan Motor Ltd. He joined TCS (Jul 2001-Sep 2001) as an assistant engineer. Furthermore, he worked (Oct 2001-Jul 2003) in Wipro Technologies as a senior system engineer. After that, he joined Outworx(Aug 2003-Oct 2008) as a technical architect. He worked (Oct 2008- Sep 2016) in different posts like principal member technical staff, principal product manager, and group product manager in Oracle-India. Further, he worked (Oct-2016-May 2019) as a director of product management and sales engineering in Saviynt, Inc. He has published more than 5 articles in international journals and conferences.

**Authors and Affiliations**

Shahnawaz Ahmad¹ • Shabana Mehfuz¹ • Fateh Mebarek-Oudina² • Javed Beg³

¹ Department of Electrical Engineering, Jamia Millia Islamia, New Delhi 110025, India
² Department of Physics, Faculty of Sciences, University of 20 aout 1955 - Skikda, B.P 26 Road El-Hadaiek, 21000 Skikda, Algeria
³ Oracle, Noida, India