IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 August 2024, accepted 6 September 2024, date of publication 11 September 2024, date of current version 23 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3458829

TOPICAL REVIEW

A Systematic Literature Review of Cloud Brokers for Autonomic Service Distribution

MOHD HAMZAH KHAN, MOHAMED HADI HABAEBI, (Senior Member, IEEE), AND MD. RAFIQUL ISLAM, (Senior Member, IEEE)
Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur 53100, Malaysia
Corresponding author: Mohamed Hadi Habaebi (habaebi@iium.edu.my)

ABSTRACT In recent years, cloud computing has become an essential distributed computing platform and has achieved enormous popularity. Within cloud computing, the Cloud service broker creates an abstraction layer between provider and consumer so that customers notice the cloud service providers' offered services' solitary view. The brokers of cloud service help connect the cloud's substantial resources and select the data centers of the cloud that meet the user's requirement while maximizing the entire response time and reducing cost. The landscape of autonomic cloud brokers has been reviewed in this systematic literature review study, while the PRISMA approach is used to analyze the literature. This comprehensive review of cloud brokerage mechanisms is tailored towards the autonomic distribution of services. To emphasize autonomic computing and cloud-access security brokers, the evolving paradigms of cloud service selection are detailed and critically analyzed to enhance service distribution efficiency. Further, the role of cloud brokers in load-balancing services is also highlighted in this study. A new taxonomy for the structured framework of cloud brokerage mechanisms is introduced based on functionalities, deployment models, and architecture for the autonomic service distribution. Finally, the study offers valuable insights for future research challenges and best practices in cloud security.

INDEX TERMS Cloud broker, cloud service broker, data center, cloud computing, load balancing, virtual machines.

I. INTRODUCTION

In the technological era, cloud computing is becoming an essential distributed computing platform and has achieved immense popularity [1]. Additionally, cloud computing has changed the IT environment by providing on-demand and scalable computing resources [2]. Furthermore, it allows companies to access different services such as applications, processing power and storage without the necessity of remarkable investment in infrastructure. Besides, cloud computing has some core benefits, such as scalability and flexibility, as resources are adjusted based on demand, allowing companies to respond to evolving market conditions [3]. It delivers services through the pay-per-use model to its users. In addition, their layered architecture enables cloud service providers to process users' requests in a fault-tolerant, scalable, and flexible manner [4]. The CC(Cloud Computing) field continues to develop speedily due to the growing demand for the services' remote provisioning over a highly high-speed network [5]. Through practical resource applications for cloud service providers, cloud computing is characterized.

Similarly, for large organizations and entrepreneurs, it delivers cost-effective solutions. Furthermore, the rapid growth of CC-based businesses requires effective strategies for operating the requests of users with a minimum response time [6]. For multi-cloud developers, these strategies become crucial when deploying multiple private or public clouds and applying various virtual machines (VMs) to deliver better services to their end users [7]. The data centers of the cloud, which are multiple providers of cloud service, are equipped with extensive storage and high-performance servers integrated with efficient communication infrastructure. To user requests, the fault-tolerance, reliability, and response time are thereby maximized similarity or corresponding [8].

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

Furthermore, cloud service brokers (CSB) have a considerable role in maintaining a good relationship between cloud service consumers and providers [9]. Additionally, they focused on facilitating cloud services' management, integration, and selection. Moreover, it also ensures that companies use the most cost-effective and suitable solutions to achieve their requirements. Apart from that, brokers offer value through different primary functions, including handling intricate integration, governance and security, minimizing the businesses' administrative burden, managing "service-level agreements (SLAs)" [10], as well as confirming compliance with the requirements of the firms. Similarly, they compare and aggregate services from various providers that generate a single-entry point for different cloud offerings.

Subsequently, CSBs, by offering practical recommendations depending on particular cost considerations, performance metrics and business needs, increase the cloud experience. Moreover [11]. In addition, brokers become vital in handling these complex situations as firms increasingly adopt hybrid cloud and multi-cloud strategies. However, it ensures maximizing the advantages and seamless interoperability of cloud computing. So, CSBs are mandatory for maintaining operational efficiency, driving innovation, and achieving strategic IT goals in the cloud.

Moreover, for effective real-time response, the cloud's interoperability is necessary, along with adequate data center selection that helps fulfil the users' demand for resources. Through cloud brokering, cloud interoperability is accomplished by focusing on managing the services of users by serving as an intermediary between cloud service providers and cloud users [12]. Cloud service brokers help connect the cloud's substantial resources and choose the cloud's data centers that meet the user's requirements while maximizing the entire response time and reducing cost. Through load balancing and mapping among cloud service providers, these mechanisms confirm cloud resources' adequate utilization [13].

For cloud-based businesses, the utilization of resources is met since resources' underutilization and over-provisioning are mitigated by cloud brokering. The maximum load balancing approaches and cloud service brokering implement the evolutionary algorithm [14]. Both these integer algorithms or programming depend on heuristic approaches [15]. However, the approach's performance relies heavily on running runtime activities that are incurred to discover the appropriate solution. The optimization problem for evolutionary algorithms is mitigated using fundamental genetic operations like selection, crossover, mutation, and initialization [16]. Furthermore, the procedure of fitness evaluation then appeals to continuity until some particular criterion is achieved, including the objective function's minimum threshold value.

To identify an optimal solution, integer programming applies objective constraints and functions while mapping the issues [17]. Additionally, with many limitations and restrictions, the complications imposed on input data and objectives make it unproductive for usages that need real-time response. On the other hand, while avoiding the significant overhead of tasks, including measuring the brokering of optimized hybrid service for the multi-cloud solution that perfectly fits the necessities, exhaustive search, and maximization. Finally, low-overhead activities develop the load balancing and cloud-brokering's overall performance to generate a better time to respond to the clouds' running applications. Concerning the significance of the present context of issues, the research aims to systematically review the cloud broker for autonomic service distribution.

This study aims to identify the role of cloud brokers in autonomic service distribution. Therefore, it sets four objectives. These are:

- To categorize and identify cloud brokers' key features and capabilities that facilitate autonomic service distribution.
- To assess the performance and efficiency of various cloud brokers in autonomic service distribution, highlighting strengths and areas for development.
- To investigate the integration strategies cloud brokers, use to distribute autonomic services across diverse cloud environments seamlessly.
- To evaluate the security measures and compliance protocols implemented by cloud brokers in autonomic service distribution, ensuring regulatory adherence and data protection.

Based on these objectives, this study has established four research questions. These are:

- What are cloud brokers' significant features and capabilities that support autonomic service distribution successfully?
- How do different cloud brokers compare concerning performance and efficiency in the distribution of autonomic service?
- What integration strategies are applied across diverse cloud environments by cloud brokers to enable seamless autonomic service distribution?
- What compliance protocols and security measures are implemented by cloud brokers to ensure data protection and regulatory adherence in autonomic service distribution?

The rest of the paper is organized as follows. Section II introduces the motivation, novelty, and contributions of this work. Section III provides the details of the methodology followed throughout this study. Section IV explores cloud service brokers. Section V introduces the paradigm of Cloud Service Selection. Section VI introduces autonomic computing for Cloud Service Brokers, while section VII presents Cloud Access Security Brokers. Section VIII discusses the autonomic cloud brokers, while a taxonomy based on Autonomic Computing is presented in section IX. Section X presents the challenges and best practices for Cloud Service Broker, and the article concludes in section XI.

II. MOTIVATION, NOVELTY, AND CONTRIBUTION

The motivation behind this paper lies in enhancing the growing demand for autonomic service distribution and cloud environment complexity. Many companies highly leverage cloud resources for handling service selection and management. Hence, there is a huge demand for automated mechanisms. Further, valuable insights, challenges, open issues, and best practices for achieving autonomic service distribution must be highlighted and investigated. A comparison of the previous literature review studies, presented below, emphasizes further the need for a systematic literature review on cloud brokers for the autonomic distribution of services.

The novelty of this study lies in the critical approach used to analyze the different cloud brokers in providing autonomic distribution of services with load balancing supported by a new taxonomy of the structured framework of cloud brokering for the autonomic distribution of services.

III. METHODOLOGY

This research applied an effective methodology based on PRISMA. Significantly, an implicit search strategy was applied across multiple databases, using some keywords associated with autonomic service distribution and cloud brokers. Apart from that, all relevant studies are identified through a "two-phase screening process" with abstract, initial title review and full-text evaluation. Simultaneously, using an organized form, data extraction was conducted successfully. Additionally, with established tools, a quality assessment was performed with clear inclusion and exclusion criteria. Finally, the results of this systematic review were reported leveraging the PRISMA model to confirm methodological rigor. The PRISMA guidelines state the individual process processed in the "identification, screening, eligibility, and inclusion". This search strategy gathers all the topic-relevant articles from notable sources, including the Scopus database, Google Scholar, Science Direct, IEEE, Springer, Wiley, MDPI, and Elsevier. The existing literature was identified using keywords such as "autonomic computing", "cloud computing", "cloud access security brokers", "Cloud Broker", "Cloud Service Broker", "Data Center", "load balancing", "virtual machines" and "autonomic cloud broker".

Figure 1 explains the documents published from 2015 to 2024 in Scopus, while the overall document classification over the "Cloud Broker" is shown in Figure 2. The database analysis provided results from over 45% of full-text research articles, 45% of conference papers, 5% of book chapter articles, and 5% of publications from other categories (Conference review articles, books, editorial, and erratum).

Figure 3 shows the proposed research's PRISMA framework, including identification, screening, eligibility, and inclusion and exclusion criteria.

Inclusion Criteria:

- The articles considered in the research are peer-reviewed journals, systematic review articles, meta-analysis articles, and conference articles.

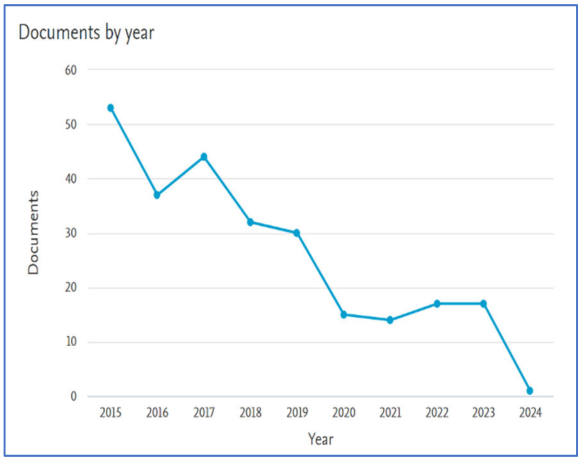

FIGURE 1. Documents published from 2015 to 2024 in Scopus.

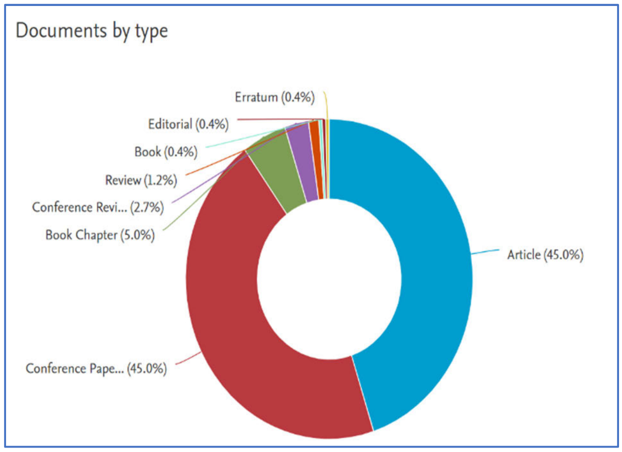

FIGURE 2. Documents classification from 2015 to 2024 in Scopus.

- The articles that directly related to the research context of cloud brokers were selected.
- The articles were chosen over the range of 2015 to 2024, more focused on (2020-2024).
- The chosen articles are published only in English.
- Articles are chosen based on the in-depth technical content related to the research context.

Incorporating various sources from different contexts and domains enriches the study by providing a detailed view of CSBs for "autonomic service distribution". Furthermore, it allows insights to be incorporated across several application scenarios, technological advancements, and industries, indicating broader challenges and trends. Subsequently, this diversity increases the study's relevance and depth, confirming that findings highlight various viewpoints and experiences, ultimately offering a more nuanced and robust insight into the field.

Exclusion Criteria:

- Research articles that do not directly relate to the research context are excluded.

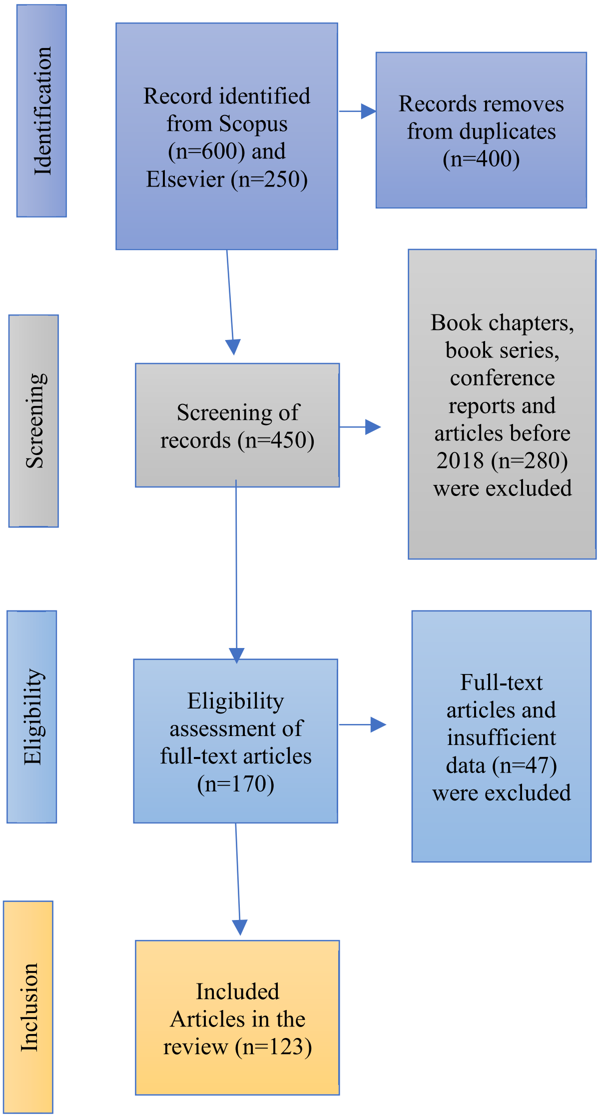

FIGURE 3. PRISMA framework.

- Book chapters, book series, conference reports, and non-peer-reviewed articles are excluded.
- The articles published before the year 2015 are excluded.
- Articles published in other languages are excluded from the research.
- Duplicate research articles from clone journals are excluded.

Figure 3 explains the PRISMA framework of the proposed systematic literature review. In the identification process, the overall records identified from the database are 850 documents (600 from the Scopus database and 250 from the Elsevier database). From the 850 papers, 400 records concerning duplicates were removed, and 450 articles were processed into the screening section. In the records screening, 450 articles were included; 280 articles have been excluded concerning the book chapters, book series, conference reports, and erratum, and the associated exclusion criteria were excluded. In the eligibility criteria, the overall studies processed are 170 documents, and 47 articles have been excluded concerning the language and insufficient criteria. And finally, the review included 123 papers relating to the cloud broker in the present research.

In addition, the PRISMA established results by offering a structured and precise approach to data synthesis and selection. Significantly, it assisted in systematically documenting the review at each stage. Therefore, identifying key trends and themes was accessible for this study. Notably, by following the guidelines of PRISMA, this review effectively analyses and categorizes the data, indicating pinpoint gaps and recurring patterns in the existing research. Moreover, this structured methodology confirms an unbiased and detailed overview, facilitating a better insight into the field's future directions and current state.

Based on the analysis and review of existing literature, this article aims to answer the following research questions.

1. How do the cloud brokerage frameworks address the privacy concerns in multi-cloud?
2. How do cloud brokers impact overall reliability and efficiency?
3. What existing frameworks are proposed in the literature for evaluating cloud broker effectiveness in autonomic service distribution and load balancing?
4. What are the best practices for managing cloud brokerage architectures in real-world applications?
5. What are the potential future developments in the cloud brokerage field, mainly in the context of autonomic computing?

IV. CLOUD SERVICE BROKER (CSB)

In cloud computing, cloud brokering is a pivotal concept that facilitates the efficient management of cloud resources. "Cloud Service Broker (CSB)" indicates an intermediation between cloud service providers and consumers. Among cloud consumers and cloud service providers, the term cloud brokering acts as a facilitator [18]. The cloud service performance is enhanced by dynamically allocating resources, managing interactions among multiple cloud environments, and negotiating contracts. The CSB creates an abstraction layer between provider and consumer so that customers notice the cloud service providers' offered services' solitary view [13].

Thus, CSB provides value addition and consolidation services and brokerage services to its users. Besides these, the modern cloud platforms are fitted with data centers that provide high performance, and these data centers are distributed over various locations. However, to offer the best services to its users, these data centers include fruitful storage and computational resources. It becomes inevitable for users to be placed in such a situation to consider data centers' capability along with incurred monetary costs. The CSB, while attempting to reduce the financial cost and response time for end users, chooses data centers for request processing for utilization [19], [20]. The significant roles of CASB are mentioned in figure 4.

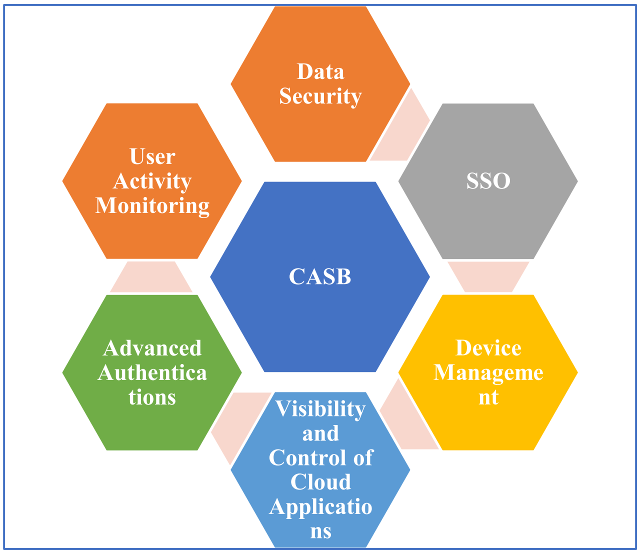

FIGURE 4. Role of CASB.

A. CHARACTERISTICS AND SERVICES OF CSB

1) PROVIDING EXPERTISE

CSBs have an influential role in mitigating issues related to cloud services' customization, management, and adoption [21]. These issues have been mitigated by identifying the lack of skills and knowledge that exist among users. It is essential to mention that brokers continuously emphasize furnishing consumers with proper guidance about cloud services to drive digital innovation and evaluate services provided by different vendors.

With a suggested vendor's thorough compilation, the customers and the broker can learn the services' details and the cloud services' mitigation [22]. The process has been completed by providing a detailed analysis of "service level agreements (SLAs)", pricing breakdowns, service features, and other essential factors. The brokers' utilization of knowledge and toolkits facilitates the decision-making processes that are well-informed, accurate, and objective.

2) NEGOTIATION

The authority of the cloud brokers is granted occasionally to participate in the negotiations of contracts with the providers of cloud service in support of their clients [9]. Apart from that, when engaging in service contracts with many vendors, the broker is endowed with remarkable power, presenting an essential method for reducing costs. CSBs, it is natural to possess formed affiliations with different vendors. These vendors can already have prior contractual agreements in some cases. By CSBs, the advantageous environment facilitates the vendors' expeditious acquisition.

3) IMPROVED COMPLIANCE AND SECURITY

The different cloud environments' applications increase security measures by data distribution across diverse platforms [23]. Furthermore, some cloud providers offer increased compliance and security measures with particular standards. All these standards are necessary for specific sectors of business.

4) SPECIALIZATION

By using specialized services provided by different cloud providers, CSBs increase their infrastructures' efficiency for specific workloads. A corporation applies an appropriate cloud service that delivers remarkable bandwidth to process extensive data sets [24]. The practical utilizations that enforce an excellent level of accessibility and dependability, another service has been followed. Moreover, this service allows companies to maximize the advantages generated by individual providers based on their workloads' exceptional demands.

5) SIMPLIFYING OPERATIONS

CSBs have a significant role in allowing the IT department to effectively manage the expense of cloud consumption, increase resource efficiency, and mitigate redundancies. In addition, a real-time integrated viewpoint's incorporation of both public and on-premise cloud resources creates an advantage for the company in minimizing errors related to several cloud platforms' management throughout the business [25].

6) VENDOR LOCK-IN AVOIDANCE

By hiring huge cloud providers, firms can reduce the extreme dependency risk on "single cloud providers" [26]. In resource allocation and contract negotiation, this technique offers enhanced adaptability that protects the business against possible modifications and price fluctuations invoked through a single provider of services.

7) COST EFFICIENCY

To increase the optimization of cost, the enterprises' ability is facilitated by CSBs. For their services, cloud providers show different terms and pricing structures. However, depending on their current financial resources and requirements, companies choose from these suppliers [27]. Besides that, CSBs can adopt expensive, dependable services for significant product applications and non-essential workloads, and the acceptance of cost-effective services can be made possible by CSBs. The various essential features of the CSB are mentioned in figure 5.

B. TYPES OF CSB

1) CLOUD AGGREGATOR

The cloud aggregator is a mediator that combines and consolidates several service catalogues into an integrated user interface and the cloud interface framework [28]. While confirming that the clients are obliged only to send a single amount to the broker, the client notably fails to select a different service number related to their specific requirements of businesses. Primarily for clients, the model of cloud

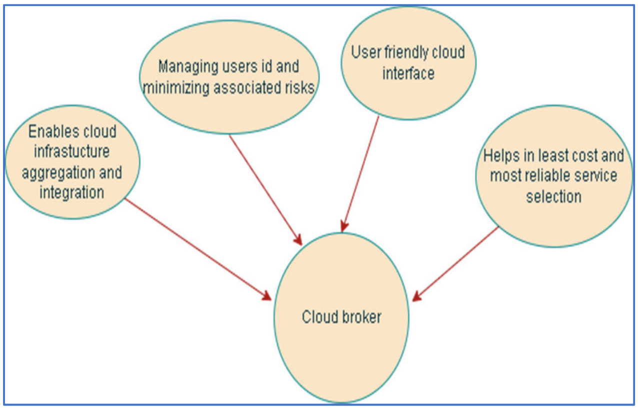

FIGURE 5. Features of CSB.

aggregator is regarded as an efficient and cost-effective strategy compared with each service's procurement. Within their ability as resellers, aggregators fulfil an essential role in managing the services and partnerships of cloud providers.

Besides the cloud services, the broker provides supplementary offerings, including governance and security. These aggregators' fundamental purpose is to structurally organize a proper services collection that offers an integrated association for all IT services and businesses. While yielding time and cost savings, this approach also increases adaptability and flexibility. In cloud computing technologies integration, cloud integrators are intensely specialized. These specialized integrators integrate these technologies into existing processes and systems. Across hybrid environments, by incorporating automated workflows, integrators mitigate the risk of businesses and increase operational efficiency by applying an integrated orchestration system. Finally, after completing the migration process, the integrator offers continuous aid to the firms as per their needs.

2) CLOUD CUSTOMIZERS

Customization alters pre-existing cloud services for businesses' particular needs [9]. The broker also focused on developing the functionalities that need to be accomplished on the cloud based on the demands of the companies. In generating the comprehensive infrastructure of the cloud, these functions have a remarkable role specified by seamless basic IT operations' integration, conformity with regulatory standards, and increased visibility.

3) SERVICE INTERMEDIATION

The broker providing value-added services on the existing cloud is involved in the service intermediation. To ensure confidentiality, integrity, and data availability, the cloud broker offers additional security measures such as encryption and intrusion detection [29]. CSB can enhance the responsiveness and performance of cloud applications through content delivery networks, caching, and load balancing. To ensure compliance with regulatory requirements and data durability, the CSB provides archival services and data backup.

4) SERVICE ARBITRAGE

The selection of the best-suited cloud service provider (CSP) for reaching user requirements is involved under the service arbitrage. Based on user preferences and real-time data, the cloud providers evaluate the CSPs dynamically. A few factors, such as pricing models, resource availability, and service level agreements, are considered [29]. To leverage respective strengths and mitigate critical risks associated with vendor lock-in, several applications across multiple CSPs have been deployed by the CSBs.

5) SERVICE INTEGRATION

The service integration involves orchestrating interactions among various cloud services to ensure seamless integration across heterogeneous cloud platforms [30]. The cloud broker mediates the interaction among disparate cloud services by translating API calls and protocols to ensure compatibility.

C. ALGORITHMS USED

1) RESOURCE ALLOCATION ALGORITHMS

By considering factors like user preferences, workload characteristics, and resource availability, resource allocation algorithms can determine how the resources among competing demands are distributed [31].

2) COST OPTIMIZATION ALGORITHMS

While meeting quality of service constraints and user requirements, cloud service costs can be reduced by using cost optimization algorithms [31]. Cost optimization techniques like dynamic programming, linear programming, and genetic algorithms can be used.

3) LOAD BALANCING ALGORITHMS

These algorithms distribute the incoming network traffic across multiple cloud instances to prevent overload on individual servers and optimal resource utilization [32].

In load balancing, cloud brokers have a significant role in managing the workload distribution across different cloud resources to minimize latency, ensure high availability and optimize performance [33]. CSBs, by using sophisticated policies and algorithms, dynamically allocate resources depending on usage patterns and real-time demand. For instance, the incoming application traffic is distributed automatically by "AWS Elastic Load Balancing" across different Amazon EC2 cases [34]. Besides these, Google's Cloud Load Balancing provides worldwide load balancing capabilities, managing traffic to the most responsive and nearest backend servers, potentially maximizing system efficiency and user experience [35].

However, different case studies highlight CSBs' effectiveness in load balancing. For instance, according to Verma and Gautam [36], "Amazon Web Services (AWS)" is used by

Netflix, and it also uses its own "load balancing" algorithms to handle significant amounts of user requests and streaming data. Additionally, by traffic distribution across different regions and servers, Netflix maintains high availability and seamless service delivery despite fluctuating demand, whereas another instance is Dropbox. Significantly, Dropbox uses cloud-based and in-house load-balancing algorithms to manage its sharing services and extensive data storage. However, this technique assists Dropbox in maintaining its reliable performance and scaling its infrastructure efficiently [36].

Furthermore, load balancing presents many challenges or limitations in cloud environments, such as managing the intricacies of hybrid and multi-cloud environments, confirming consistent productivity across distributed resources and managing unpredictable traffic patterns [37]. Moreover, there are many solutions for these challenges, including incorporating advanced load balancing techniques like those applying auto-scaling features to adjust resource allocation automatically depending on real-time demand utilizing machine learning algorithms for predictive scaling [38]. Subsequently, integrating comprehensive analytics and monitoring tools is mandatory to address and detect performance issues properly. Finally, cloud brokers overcome these issues with robust solutions to increase overall service efficiency and confirm optimal load distribution.

D. TESTBEDS USED

1) CloudSim

For evaluating and modelling the cloud computing environments, the CloudSim can be used as a popular simulation framework [39].

2) OpenStack

OpenStack is recognized as the open-source cloud computing platform that ensures flexible infrastructure to establish both the public and private clouds [39].

3) EUCALYPTUS

For establishing hybrid and private clouds compatible with Amazon web services, eucalyptus can be used, and to evaluate performance under different workload scenarios, customizable testbeds can be created with the help of eucalyptus [39].

V. PARADIGMS OF CLOUD SERVICE SELECTION

A. CloudQual

The CloudQual is a "quality model", and it has six metrics of quality like elasticity, security, responsiveness, availability, usability, and reliability ("Mean Time To Failure (MTTF)" and "Mean Time Between Failure (MTBF)") [40]. Among these six metrics, usability only belongs to a subjective nature, whereas the other five metrics belong to an objective nature. Some techniques were applied, like discriminative power, consistency, and correlation, to validate the quality metrics. In traditional services, SERVQUAL is a related work and a model of service quality. It has five "quality dimensions", including empathy, assurance, responsiveness, reliability, and tangibility.

B. SMICloud

Through "CSMIC (Cloud Service Measurement Index Consortium)", this SMICloud was created. The primary aim of SMICloud is to rank and compare cloud providers. This framework developed a healthy atmosphere for comparing several cloud service providers and the SMI cloud broker over multiple operations [41].

This framework introduced seven attributes, such as usability, security, assurance, performance, cost, agility, and accountability, to evaluate the service offered by CSPs. In addition, the SMI cloud broker included elements like a ranking system, SMI calculator, and SLA management. The "AHP (Analytic Hierarchy Process)" mechanism was proposed to rank the CSPs. This framework was proposed for getting the services of "Infrastructure as a Service (IaaS)".

C. METER

In the computing cloud models and frameworks, the C-Meter was the easy-to-use, extensible, and portable framework to submit and generate test workloads [42]. Similarly, for Amazon EC2, a C Meter was used to check its wait and response time in the queue, which restricted declination with a doorstep of 1 second [43]. In addition, the cloud services' elasticity issues are discussed by C-meter, but it lacks several other cloud services' quality issues, including reliability and security. Without addressing the users of these metrics, they can be unwilling to accept the framework.

VI. AUTONOMIC COMPUTING

The term autonomic computing is derived from the autonomic nervous system of the human body. Autonomic computing in computer science is inspired by the automated mechanisms that are identified in biological systems. Without constant human intervention, the systems can adapt and protect themselves by incorporating autonomic computing principles [44]. This approach can alleviate the management and complexity overhead in modern computing. Based on user requirements and environmental changes, these systems can be configured. For resource utilization and optimizing efficiency, autonomic systems can continuously monitor the performance metrics. The security measures are incorporated by autonomic systems to defend against vulnerabilities and cyber threats [45].

Additionally, cloud services' efficiency, scalability, and adaptability are significantly increased by autonomic computing through their self-management abilities. Furthermore, in the cloud brokers' context, for the distribution of autonomic services, the self-management principles are used by autonomic computing to automate primary functions, including performance optimization, fault detection, and resource allocation [46]. However, this automation enables cloud services to respond dynamically to changing conditions and workloads without any manual intervention that improves adaptability. Similarly, autonomic systems for scalability autonomously scale resources down and up depending on real-time demand, minimize costs, and confirm the practical application of computational resources. Apart from that, in autonomic computing self-healing mechanisms are present. These mechanisms allow cloud services to recover from and detect potential faults, maintaining better performance and availability [47]. Simultaneously, autonomic computing, by minimizing the necessity of human intervention and oversight, increases system efficiency, streamlines operations, and confirms that cloud services respond smoothly to evolving challenges and requirements [48]. Furthermore, it results in a more responsive and resilient cloud infrastructure that can support a broad range of services and applications with less manual management, associating with the cloud brokers' core objectives in optimizing the distribution of autonomic services. Figure 6 shows the objectives, properties, and meanings of autonomic computing.

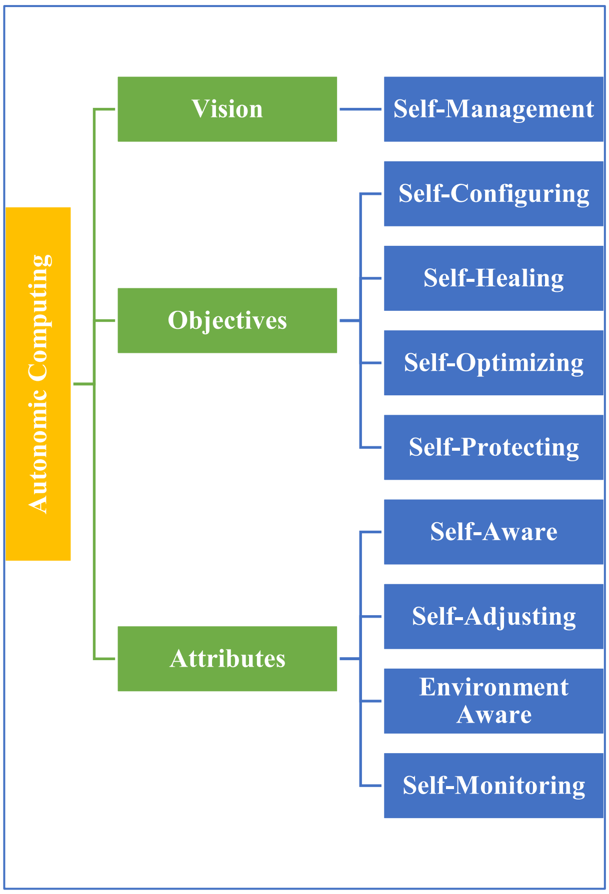

FIGURE 6. Objectives, properties, and attributes of autonomic computing.

Figure 6 illustrates the vision, objectives, and attributes of autonomic computing. This figure effectively outlines the fundamental aspects and goals of Autonomic Computing systems, which aim to manage themselves and adapt to changes with minimal human intervention.

A. TYPES OF AUTONOMIC COMPUTING

1) SELF-CONFIGURATION

Self-configuration is the system's ability to adjust configurations based on the requirements without human intervention. Software installation, network configuration, and system parameter tuning are involved as few of the tasks under self-configuration.

In autonomic computing, self-configuration indicates the systems' capability to automatically configure and set up themselves depending on high-level goals and policies without manual intervention [49]. Moreover, this procedure includes adjustments to operational factors, resource provisioning and initial setup in response to evolving conditions. Additionally, the classification of self-configuration comprises static and dynamic self-configuration. Significantly, static self-configuration involves pre-established infrastructure that is unable to change dynamically. On the other hand, dynamic self-configuration adapts in practical situations to operational demands and environmental changes. However, dynamic self-configuration using AI and machine learning confirms resource utilization, scalability and optimal performance, minimizing the necessity of continuous human intervention and oversight [50].

Besides these, assessing self-configuration's effectiveness and efficiency involves criteria including adaptability, accuracy and speed [51]. Additionally, key metrics such as configuration time can measure success rate, the ability of the system to set itself up, highlighting configurations' accuracy without adaptability and errors, and evaluating the ability of the system to respond to scale and changes. Similarly, benchmarks like human intervention's frequency and time-to-deploy also have a crucial role [52]. These benchmarks provide knowledge about performance. Moreover, system uptime and resource utilization are significant indicators, suggesting the efficiency of self-configuration in maintaining optimal operations while reducing manual oversight and downtime.

2) SELF-HEALING

To minimize downtime and ensure continuous operation, system detection is entailed by self-healing. Several techniques, such as error recovery and fault tolerance, are employed by self-healing mechanisms to maintain the system's reliability and integrity.

Moreover, in autonomic computing, self-healing indicates the ability of the system to repair, diagnose and detect faults automatically, confirming continuous operation without manual intervention. Furthermore, this capability increases the availability and reliability of the system by addressing challenges reactively and proactively [53]. However, proactive self-healing is one kind of self-healing which implements preventive measures and anticipates possible issues [54].

Similarly, reactive self-healing is another kind that focuses on responding to faults or problems as they happen, reinstalling regular activity [55]. In addition, self-healing by leveraging advanced technologies, including machine learning and AI, identifies anomalies and patterns, allowing effective and timely resolutions that reduce downtime and maintain optimal system performance.

Furthermore, examining self-healing's effectiveness and efficiency involves criteria including the success rate of fault resolution, recovery time and detection time. Moreover, key metrics are "mean time to repair (MTTR)" and "mean time to detect (MTTD)". These two metrics measured the system's efficiency in resolving and exploring issues [56]. Subsequently, an automatic repair success rate without manual interruption is also essential. Simultaneously, benchmarks such as system failures' frequency, system uptime and the influence on entire performance offer knowledge regarding self-healing capabilities. So, assessing the ability of the system to maintain stability and prevent recurring issues under different conditions is necessary for thorough evaluations.

3) SELF-OPTIMIZATION

For resource utilization and optimizing efficiency, the system analyzing performance metrics involves self-optimization [57]. The system metrics, such as network bandwidth, CPU usage, and memory utilization, are continuously monitored by self-optimization mechanisms.

Additionally, in autonomic computing, self-optimization indicates the ability of the system to adjust its operations automatically to increase resource utilization, efficiency and performance [58]. Significantly, this procedure involves continuous analysis and monitoring of system metrics to explore improvement opportunities. In general, self-optimization has two parts: local optimization and global optimization. Local optimization emphasizes optimizing individual subsystems or components. Similarly, global optimization concentrates on increasing the entire system's overall performance. However, using machine learning and AI dynamically, self-optimization mechanisms respond to changing conditions and workloads that reduce the necessity of manual intervention and tuning and ensure optimal functionality [59].

In addition, assessing self-optimization's effectiveness and efficiency involves criteria including adaptability, resource utilization and performance improvements [60]. Some key metrics are also there, such as throughput and response times. These two metrics measure enhancements in resource usage efficiency and system performance, highlighting optimal storage, memory and CPU utilization. Apart from that, different benchmarks, including the reduction in human interventions and "multitask Bayesian optimization (MTBO)", provide information about operational improvements [61]. Finally, assessing the adaptability of the systems to changing conditions and workloads and their capability to increase or maintain performance under different scenarios is essential for a detailed examination of self-optimization abilities.

4) SELF-PROTECTION

For shielding and identifying, it assesses malicious strikes, maintains integrity, and more extensive framework security. Self-protection is considered a strong ability of autonomic computing.

However, in autonomic computing, self-protection is the ability of the system to automatically recover from attacks and safeguard against security threats without manual intervention. Subsequently, self-protection involves implementing defensive measures, detecting potential threats and monitoring for vulnerabilities [62]. Moreover, there are two types of self-protection: reactive and proactive. Furthermore, proactive self-protection prevents and anticipates attacks by applying security patches and consistently scanning for vulnerabilities. In contrast, reactive self-protection mitigates and identifies threats during an attack in real time. Significantly, these mechanisms increase systems resilience utilizing machine learning and AI and can address security incidents promptly [63]. Moreover, in this way, these two classifications ensure the confidentiality and integrity of operations and data.

Some significant criteria have been followed to evaluate self-protection's effectiveness and efficacy, including resilience, response time, and threat detection accuracy. Similarly, two key metrics have also been highlighted in this study, such as "mean time to respond (MTTR)" and "mean time to detect (MTTD)". These two metrics measured the system's efficiency in resolving and exploring threats [64]. Subsequently, the number of false positives and the success rate of automated threat neutralization are vital indicators. Significantly, benchmarks, including reducing human interruption, system uptime and the severity and frequency of security breaches, offer knowledge about self-protection performance.

B. CHARACTERISTICS OF AUTONOMIC COMPUTING

1) SELF-AWARENESS

The term self-awareness refers to the systems possessing external environment, performance metrics, and internal state awareness through monitoring mechanisms. Informed decision-making can be facilitated, and a comprehensive understanding of current operating conditions can be developed by continuously monitoring these metrics.

2) SELF-REGULATION

Performance and stability with specified objectives are maintained by enabling self-regulation mechanisms. In response to environmental conditions and changing demands, the workload distribution and processing priorities are affected by self-regulation. Based on workload fluctuations, self-regulation mechanisms can dynamically scale resources up or down to ensure optimal performance.

3) SELF-OPTIMIZATION

To identify opportunities to enhance system performance, machine learning techniques and algorithms are employed by self-optimization mechanisms. The algorithm parameters, task scheduling optimization, and data storage layouts are included within the self-optimization.

4) ADAPTABILITY

The term adaptability refers to the ability of the system to reconfigure itself to maintain its performance and functionality. In dynamic computing environments, resilience can be fostered, and self-management capabilities can be exhibited by ensuring adaptability [57].

C. MAPE CONTROL LOOP

In an autonomic computing system, the MAPE (Monitor, Analyze, Plan, and Execute) is a fundamental concept that consists of four interconnected phases [65]. During monitoring, the system gathers data from several sources, including performance metrics, sensors, and logs, to access the current state. Once the data is collected, the system will analyze patterns and trends from desired states. The system formulates an effective plan based on analysis for optimizing performance and identifying issues. During the execution phase, the system implements a practical plan by executing prescribed actions such as reallocating resources and adjusting configurations. With continuous monitoring, analysis, planning, and execution, the MAPE control loop can be operated iteratively [65]. In dynamic environments, autonomic systems can be enabled to adapt and self-manage effectively. For self-management capabilities, the MAPE control loop can serve as a foundation in autonomic computing and help facilitate self-management capabilities to achieve desired system states. Figure 7 shows the MAPE control loop.

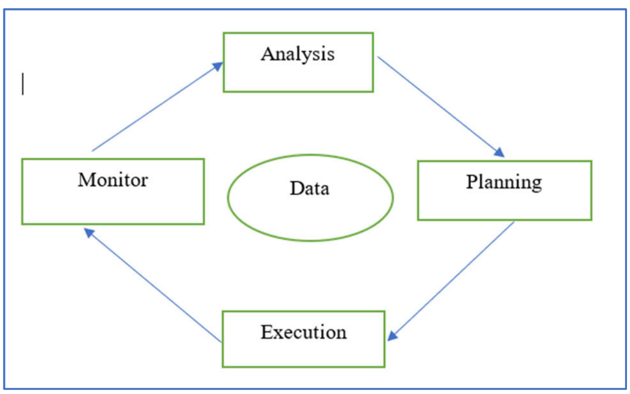

FIGURE 7. MAPE control loop.

D. CLOUD SERVICE MODELS

1) INFRASTRUCTURE AS A SERVICE (IaaS)

Including virtual machines, networking, and storage, the cloud providers offer virtualized computing resources over the internet in the IaaS model [66]. Based on the requirements, the users can scale up or down. When compared with traditional hosting methods, users are allowed to have great customization and can control the development frameworks. Without any investments in physical infrastructure, organizations can adjust their resources according to their requirements because it offers flexibility and scalability. Without experiencing any complexities of handling underlying hardware from simple web servers to critical enterprise applications, this level of control deploys a wide range of applications [8]. Additionally, load balancing, auto-scaling, and security controls are a few of the offerings under IaaS that are useful for establishing resilient applications in the cloud [67]. Cloud computing for infrastructure needs can be leveraged by providing a scalable solution for organizations.

2) PLATFORM AS A SERVICE (PaaS)

Developers can deploy and manage applications under the PaaS platform without any complexity in handling underlying infrastructure. The application development process can be streamlined by offering middleware, development tools, and other services [68]. Instead of handling infrastructure, they are deploying applications and coding to focus on enabling faster time-to-market. For managing applications over the internet, the required complete set of tools can be accessed by developers [8]. By allowing developers to focus more on establishing applications, the PaaS abstracts away the underlying infrastructure. This abstraction accelerates the development process by eliminating the requirement to handle networking, storage, and other components of infrastructure. The operational overhead associated with handling infrastructure is reduced by providing scalable solutions to accelerate the deployment processes.

3) SOFTWARE AS A SERVICE (SaaS)

On a subscription basis, the software applications over the internet are delivered by the software as a service. Without any requirement to maintain software locally, the applications through web browsers can be accessed by the users. SaaS providers can effectively handle cost-effectiveness, security, and updates [69]. The SaaS applications cover a wide range of functionalities, including project management, customer relationship management, and enterprise resource planning. The multi-tenancy architecture is also offered by SaaS applications, enabling multiple users to share a single application instance and handle data privacy [8]. For customers, cost-effective solutions can be delivered, and economies of scale can be achieved with the help of this architecture. Without worrying about infrastructure management, the core business activities focus on providing organizations with hassle-free and flexible access.

4) APPLICATION AS A SERVICE (AaaS)

Instead of entire software applications, the specific application functionalities are focused on the concept of an application as a service, which can be identified as an extension of the SaaS concept. Organizations can leverage third-party applications without any requirement for extensive development and controlling operational overhead. The API-based integrations, machine learning algorithms, and data processing services are included as a few of the offerings under the application as a service [8]. The application offers flexible pricing models like subscription-based pricing as a service. Without any infrastructure investment requirement, the application drives innovation and capability enhancement as a service.

VII. CLOUD ACCESS SECURITY BROKERS (“CASB”)

Nowadays, the cloud is considered a new place that stores resources, applications, and data, but the cloud providers cannot confirm the cloud utilizations’ secure experience. Within the CC field, CASB emphasized surveying and recognizing all the applications of the cloud in use, tokenizing or encrypting sensitive information to maintain security and privacy, and potentially increasing the application of cloud companies over a few platforms of Cloud [70]. On the other hand, this CASB can be a gigantic field. Still, it is somehow ambiguous. In investigation papers, significant conflict is created among the expressions and commitments applied to depict them. According to Garner, CASB has four interconnected columns. These columns are ‘‘thereat protection’’, ‘‘data security’’, ‘‘compliance’’, and ‘‘visibility’’ [71].

Subsequently, CASBs act as intermediaries between providers and users of cloud services to increase the efficiency of service distribution and enforce security policies [72]. Additionally, CASBs, by offering visibility into threat prevention, data protection and cloud storage, ensure conformity with laws and address security gaps. Furthermore, by enforcing security controls and optimizing data flows without compromising performance, CASBs increase the efficiency of service distribution. However, they offer vital features, including real-time monitoring, identity management, encryption and ‘‘data loss prevention (DLP)’’ [73]. So, these characteristics assist firms in detecting anomalies, controlling access and securing sensitive data, and confirming efficient and safe cloud service distribution.

Moreover, in this section, this study has provided real-world examples regarding CASB implementation. The first one is CloudLock. It is one of the popular CASB solutions implemented by Cisco. This CloudLock significantly helped in improving compliance and data security for its clients. Subsequently, by integrating CloudLock, Cisco allowed firms to prevent unauthorized access, enforce data protection policies and monitor user activities across different cloud platforms, which enhanced operational efficiency and security [74].

‘‘Azure AD Conditional Access’’ with CASB implementation by Microsoft is another example [75]. In addition, this implementation enabled firms to execute adaptive access policies depending on the behaviour and context of the user, minimizing the unauthorized access risk and increasing overall service efficiency. Thus, securing and maintaining the environment of cloud service while improving service distribution confirms that firms use cloud advantages without compromising efficiency or security.

A. EVOLVING PARADIGMS OF CLOUD SERVICE SELECTION CONCERNING SECURITY AND AUTONOMIC COMPUTING

The cloud service selection’s evolving paradigm recently incorporates autonomic computing principles and advanced security measures to increase operational efficiency and decision-making [76]. Furthermore, security-focused paradigms focus on compliance, data protection, threat detection, and using tools like AI-generated security analytics and CASBs. Notably, autonomic computing principles drive self-configuring and dynamic systems that respond to changing security threats and workloads [77]. Moreover, this incorporation enables context-aware and real-time decisions, confirming that chosen cloud services encounter security requirements and performance. By automating these procedures, companies achieve greater adaptability, efficiency, and resilience in their selection of cloud services, overcoming evolving and complex security challenges.

B. CHALLENGES IN CASB

The crucial research concerns of CASB have not been properly and thoroughly investigated as the directions of further research [27]. Furthermore, for all CASBs, no proper support for the features of QoS and no support for the architectures of multiple cloud services like hybrid, community, private, and public cloud are common problems. The issues of CASB need to be explored sincerely to assist future designers in making them appropriate.

In CC, some particular challenges are- reduced costs of data centers, the processing time of Data and VM, and zero execution time achievement for AWS at the cloud scale, introducing the scenario of multi-user-multi-key. Finally, in understanding the intended outcomes of the person and identifying the assistance and resources to achieve these outcomes, CASB has an essential role.

C. RECOMMENDATION FOR THE BEST PRACTICES OF CASB

In cloud environments, ‘‘Cloud Access Security Brokers (CASBs)’’ have a significant role in securing applications and data [73]. In this section, some recommendations have been provided about the CASB’s best practices to increase security. It is essential to achieve complete visibility within organizations in all services and applications of the cloud that are used. All organizations need to confirm that the solution of CASB can monitor and discover both unsanctioned (shadow IT) and sanctioned applications [78]. Apart from that, applying the analytics of user behavior to explore suspicious and abnormal activities helps detect possible threats within the firms. To react to the user's abnormal behaviors, the companies must incorporate alerting mechanisms and anomaly detection.

Additionally, tokenization and encryption are a must for sensitive data. For unified control over the users' access to the cloud applications, integrating CASB is important with access and identity management systems [79]. With the "Application Programming Interfaces (APIs)" of cloud service providers, the CASB integration helps enforce security and real-time monitoring policies. In the APIs of cloud providers, regular updating of the connections of APIs with changes is essential [80]. Finally, organizations need to conduct regular simulations and drills to ensure an effective and swift reaction in a security incident. To correlate and centralize the security event data, organizations must integrate the solution of CASB with the "Security Information and Event Management (SIEM)" system.

VIII. AUTONOMIC CLOUD BROKERS

The comprehensive survey is conducted on the autonomic cloud broker by emphasizing self-management capabilities for optimizing cloud resources dynamically. With modern applications' evolving demands, both the scalability and resilience in cloud environments are ensured [44]. Self-optimization, self-protection, adaptability, and self-healing are a few of the characteristics of autonomic cloud brokers mainly focused on in this study. The concept of an autonomic broker is presented for managing services across multiple clouds. Including functionalities and components, the architectural design of an autonomic broker is mainly focused [81]. Across heterogeneous cloud environments, the cloud broker effectively manages and monitors the resources autonomously. For cloud service management, they ensure the autonomic approach results in experiencing huge benefits. By focusing on the challenges associated with traditional cloud brokerage models and the motivation behind autonomic cloud broker development the valuable insights into the emerging concept of autonomic cloud brokers can be provided [82]. For service optimization and dynamic resource allocation the autonomic computing principles can be leveraged.

The workload demands and evolving user requirements can be reached in dynamically composing cloud services by exploring the self-adaptive service composition mechanisms in autonomic cloud environments [83]. A multi-objective optimization approach is proposed for self-adaptive service composition to enhance resource efficiency and service quality in cloud environments. Cost efficiency, performance, and scalability can be optimized for the autonomic management of cloud resources [84]. For autonomic cloud bursting, a practical roadmap and conceptual model need to be proposed [85]. The sudden workload spikes can be accommodated by exploring the opportunities and challenges of dynamically expanding cloud resources. The resilience in a cloud environment can be enhanced by presenting a conceptual framework for autonomic cloud bursting. To meet the performance requirements and varying workload demands, the existing approaches are analyzed for the autonomic provisioning of cloud resources [86].

The resource allocation efficiency can be enhanced, and future research directions can be identified by focusing more on the current provisioning methods. For managing cloud-based services, both the opportunities and challenges of leveraging autonomic computing principles must be explored [87]. The reliability and efficiency of cloud services are enhanced by focusing more on the significance of self-management capabilities. To cover several degrees and applications, a foundational understanding of autonomic computing principles is required by highlighting the potential applications in diverse domains and the evolution of autonomic computing concepts necessary to be discussed in addressing complex adaptive systems [88]. While implementing autonomic cloud service brokerage systems, focus on both the opportunities and challenges is required. Resource utilization, cost-effectiveness in a cloud environment, and service quality should be enhanced to discuss challenges and opportunities [89].

A trade-off between cost and performance resource provisioning is entailed in the multi-cloud environment for autonomic cloud brokering. Similarly, the user requests within minimum delay can be scheduled by attempting the adequate load balancing mechanism. In recent days, in-depth research has been conducted on load balancing and autonomic cloud service brokering. The placement of the virtual machine in a multi-cloud environment can be done by ensuring the autonomic cloud brokering architecture [90]. The user-defined constraints for load balancing and the number of virtual machines are considered for the cloud environment. Later, the cloud environment uses integer programming to formulate the problem that aims to maximize infrastructure capacity within user-defined constraints. Using an integer linear programmer, the federated cloud environment is proposed as another approach for load balancing among several machines. Within QoS constraints, the cloud provider's profit is maximized by the approach integrated with the mechanism of virtual execution environment placement [91].

The cost-aware provisioning of resources is proposed, and in comparison, reducing cost through stochastic integer programming, the number of Virtual Machines (VM) and the number of VMs provisioned is determined by the two-phase model [92]. The cloud scheduling approach executes cost minimization within deadline-limited scenarios [93]. By using binary integer programming, the application execution time is minimized. Along with execution deadlines, the memory resources and CPU are characterized by the application mapping tasks, for instance, taking place within constraints. The multi-objective evolutionary algorithm is proposed for mapping every job in a hybrid cloud [94]. The GA search for four objectives related to resource utilization, income, number of processed employment, and energy consumption is performed by enabling the simulation framework to implement evolutionary algorithms.

To enhance cloud provider profits and customer satisfaction, another multi-objective evolutionary algorithm is the whale optimization algorithm [95]. The WOA technique evaluates the instance's response time, and cost reduction is included under customer satisfaction by choosing appropriate scheduling for the optimum location using energy resource allocation. The evolutionary algorithm-based approach is a way to choose a data center that can efficiently process user requests [14]. The population with parameters and the number of data centers to be optimized are initialized by the evolutionary algorithm-based approach. The data center with the best-fit value is selected for the next generation. The weighted difference of vectors related to the probability of crossover and data centers are utilized for recombination. Including clusters, grids, and clouds, the resources obtained from different environments are provided by describing an effective framework design [96]. For required resource estimation and time, the task execution time has been used by the resource provisioning approach in the framework.

Another autonomic cloud broker selection policy is suggested for the multiple grids that use the rank evaluation [70]. With the usage of average slowdown parameters and resource information, the ranks will be computed. Similarly, different dynamic and static approaches are proposed for scheduling resources [97]. The number of VMs required, considering VM costs, budget, and deadlines, is computed by providing dynamic online resources. The priority queues are used for dynamic scheduling, and in ideal virtual machines, the tasks are assigned. The proposed framework can evaluate the service broker within the multi-cloud environment [98]. By considering the service-level agreement (SLA) parameters, the autonomic cloud service broker searches for the appropriate cloud provider. The other approaches in the framework perform the cost-aware selection and random and region-based selection of cloud service providers.

Using heuristic-based approaches, the Cloud Analyst simulator implements the optimized response time (ORT) and the closest data center (CDC). The CDC service broker selects the data centers that incur minimal communication costs within neighboring regions. The optimized response service broker is selected through load balancing among the brokers, producing the closest data center and lowest estimated response time. Moreover, the load balancing using round-robin (RR) is spread equally by elaborating on the throttled approach in the next section. Similarly, cost-aware brokering is proposed by controlling the distribution load and cost among data centers [99]. The 5.5% cost reduction is enabled by the distribution of load-optimized hybrid service brokering for multi-cloud. However, compared with the closest data center (CDC)-based approach, services' response time increases gradually and is implemented in CloudAnalyst [100]. In contrast to these approaches, based on the static and dynamic selection of data centers, the runtime overhead by distributing load is reduced with the help of NHSB_TRR.

Moreover, there is more possibility for the normalization-based mechanism to control the monetary cost and enhance response time effectively. The dynamic load-balancing approach that includes both the load and performance for resource allocation [101] is proposed. By generating computing load on every server, the improvement of resource utilization is targeted by the dynamic load balancing approach. Considering RAM and CPU capacities, the resource utilization is computed. Including the number of physical machines, the weights are assigned to data centers.

Similarly, for choosing data centers, the two region-wise matrices that correspond to parameters are considered [102]. The first matrix uses the cost and distance parameters. In comparison, the second metric uses the availability and performance parameters for regions. By choosing individuals from these matrices, both sets are generated subsequently. The data centers are common for both sets; they are selected to process user requests.

Regarding bandwidth parameters and communication delay, proximity-based allocation is initially used in the proposed approach [13]. For choosing data centers, the processing capability is considered in the case of multiple data centers. Similarly, the round-robin-based selection is used during the multiple data center's existence in a region [11]. While considering the available data centers for allocation, the allocated data centers list is maintained effectively. Based on the speed of the data center, the priority for data centers is assigned [33]. By considering assigned priorities to data centers, the round-robin allocation takes place. Based on the number of data centers in the region, the number of processors, and the speed of processors, a similar approach [103]. For processing user requests and choosing a data center, the allocation policy of the round-robin is used subsequently.

Based on the load and cost, the practical approach for choosing a service broker is described by [104]. The virtual machines are arranged in sorted order by the proposed algorithm for processing speed and network latency. The requests are redirected by choosing the data center, which results in virtual machine matching and minimum cost. However, no specific mechanism for overall response time and cost reduction has been provided. The NHSB_TRR provides cloud users with highly efficient, cost-effective services and distributes load among data centers. This uses a low-overhead mechanism. The response time can be improved by controlling the normalized parameter values, and NHSB_TRR significantly minimizes the associated cost. Moreover, the hybrid selection mechanism, which consists of dynamic and static data center selection, has dramatically reduced the overhead.

By focusing on topics like load balancing, energy efficiency, scheduling algorithms, resource management in multi-cloud environments, cost-performance trade-offs,

TABLE 1. Comparison of related works.

Reference	Year	Limitations	Importance
[4]	2013	Due to the simplifications and assumptions made in the simulation model, the simulation results do not perfectly reflect real-world cloud performance.	This study offers a practical method for evaluating cost-performance trade-offs in cloud applications.
[57]	2016	The latest advancements in autonomic management techniques are not covered.	The autonomic management techniques for cloud services and resources are well-discussed
[7]	2016	The proposed brokerage approach introduces the additional overhead for the cloud resource management process, which potentially impacts performance.	The novel approach is introduced for resource management in multi-cloud environments, and the challenges associated with resource allocations can be addressed.
[82]	2017	The architectural aspects are mainly focused on during this study, but an in-depth discussion of practical changes is lacking.	A systemic survey of the solutions and challenges in architecting cloud-enabled systems is provided.
[12]	2018	Based on the relevance of fuzzy rules, the effectiveness of enhanced service broker algorithms is dependent, and this could vary across different application domains.	The service brokerage algorithms in cloud environments are improved by presenting novel approaches, and fuzzy logic is leveraged for decision-making.
[6]	2018	Based on specific workload characteristics, the scheduling algorithm's performance is provided in the proposed study, and the characteristics of all cloud computing scenarios are not well generalized.	Optimized task scheduling algorithms are presented for improving resource utilization in cloud environments, and for cloud service providers, practical benefits are provided.
[5]	2019	All the performance management aspects in cloud environments are not covered under the proposed taxonomy, and to accommodate evolving technologies, the proposed taxonomy requires necessary updates.	A structured framework is provided during this study to help practitioners understand the performance management issues in cloud computing and aid them in addressing relevant challenges.
[83]	2019	The emerging trends and recent advancements in autonomic computing are not covered.	Along with future directions, valuable insights into the current state of autonomic computing research are provided.
[89]	2019	Limited discussion is provided on the challenges of	By laying the groundwork for practical implementation, a

TABLE 1. *(Continued.)* Comparison of related works.

		practical implementation.	comprehensive overview of autonomic computing concepts is offered.
[14]	2019	Based on the dynamics of the fog/cloud environment, the optimized service broker routing policy effectiveness is dependent, and under various workloads, the performance implications are not entirely captured.	The requirement for efficient resource allocation in a distributed computing environment is addressed, and a potential solution is offered to enhance system performance.
[19]	2019	The different service broker scheduling approach suitability for cloud data centers is provided based on factors like user requirements, workload characteristics, and system architecture. Across deployments, this could be varied.	A different service broker scheduling approach is introduced to enhance system efficiency and improve resource allocation.
[90]	2020	The discussed optimization techniques do not cover all the scenarios, and adaptation is a massive requirement for specific contexts.	For multi-cloud architectures, the optimized hybrid service brokering is presented.
[13]	2020	The taxonomy does not cover all the load-balancing	A comprehensive survey of load balancing in

TABLE 1. *(Continued.)* Comparison of related works.

		aspects of cloud computing, and this study potentially overlooks specific techniques.	cloud computing is provided during this study, and by facilitating informed decision-making, valuable insights into current trends are offered.
[16]	2020	Based on specific characteristics, the proposed meta-heuristic algorithm's effectiveness for cloud resource provisioning is provided so that this can be varied across deployments.	The autonomic approach to cloud resource provisioning has been introduced to leverage meta-heuristic algorithms.
[17]	2021	Based on factors like problem size, the applicability of the proposed cutting plane algorithms for integer programming is limited.	For integer programming with linear objectives, the finite cutting plane algorithm is presented, and to resolve optimization problems, it offers a potentially efficient approach.
[15]	2021	The systematic review does not include all the relevant studies on meta-heuristic scheduling approaches.	Valuable insights into the strengths and weaknesses of different algorithms are offered.
[105]	2021	The opportunities are primarily focused, and the lack of potentially	The opportunities in autonomic cloud computing are explored by

TABLE 1. *(Continued.)* Comparison of related works.

		overlooking challenges is noticed.	guiding research initiatives in leveraging automation.
[96]	2023	There is limited coverage of specific approaches and challenges	Practical guidance is provided for industry efforts towards self-management and automation.
[106]	2023	Not all the potential challenges are covered during this study, and adaptation is required for specific contexts.	The performance evaluation of load-balancing algorithms with different service broker policies is discussed for cloud computing.
[8]	2023	This survey does not cover all existing software technologies for improving energy efficiency in cloud data centers, and the emerging, well-known solutions are overlooked during this study.	A comprehensive overview of software-based approaches is provided to improve energy efficiency in cloud data centers, and this study serves as a valuable resource for researchers.
[1]	2023	The empirical data is lacking during this analysis, and the study heavily depends on the existing literature and theoretical frameworks.	This study provides a comprehensive overview of the defences and challenges of enterprise cloud computing. For practitioners, this is a valuable resource.

service brokerage algorithms, and autonomic management techniques, the comprehensive analysis of several studies on cloud computing is offered by contributing review paper to the existing literature in table 1. Some previous reviews have overlooked certain advancements and practical challenges. However, current research meticulously addresses these aspects by providing valuable insights into recent advancements and emerging trends. The current review has also acknowledged the gaps and limitations in the existing research. The holistic view of the field is offered by analyzing a wide range of studies from different years. The areas for further investigation are identified, and the informed decisions in cloud computing technologies implementation and the current state of the art are effectively understood by analyzing a wide range of studies. However, certain limitations are noticed in the existing literature, and periodic updates are required to address new challenges.

IX. CLOUD SERVICE LOAD BALANCING AND BROKERING

The optimal selection can be considered by the environment for service provision, with multiple cloud service providers having locations and diverse pricing models. The processing capabilities, parameters reckoning, and user request allocation for data centers are required for the cloud service providers. Within different geographic regions, the generated user requests are placed by user bases. The areas are connected to the data centers through high-speed networks or the Internet. For processing user requests, the cloud data center is selected using the algorithms of cloud service brokering. With virtual machines, every data center is equipped, and for processing user requests, these are allocated by the data center controller [13].

The requests arriving at the data center must be distributed among virtual machines, and load-balancing algorithms accomplish the tasks. Load-balancing algorithms require queue implementation, allowing them to cope with multiple requests. As the virtual machines allocated or de-allocated are triggered, the load balancing algorithms must be implemented for throttled load balancing [106]. After user requests are processed, the output response is returned to the user base. For multi-cloud, the hybrid service brokering is optimized. To compare performance in this paper, the load balancing approaches and cloud service brokering approaches are implemented within the CloudAnalyst simulator. Below is a succinct description of the working mechanism of load-balancing approaches and service brokering.

A. CLOSEST DATA CENTER (CDC) SERVICE BROKERING

User requests are generated from user bases in different regions. To choose the closest data center, the nearest service brokering uses the core responding latencies and data transfer parameters [105].

B. THROTTLED (THR) LOAD BALANCING

The specific task to virtual machines is allocated by throttled load balancing, and until the virtual machine becomes free, this waits for the next allocation. While searching for the next free VM for allocation, the throttled load balancer traverses the VM indexes in ascending order [107].

C. OPTIMIZED RESPONSE TIME (ORT) SERVICE BROKERING

To minimize the response time corresponding to every user request, optimized response time service brokering is attempted. The response time is estimated through the processing capabilities of data centers, availability time, and request size computation [108]. The data center is selected to process the request with a minimum estimated response time.

D. EQUALLY SPREAD (ES) LOAD BALANCING

An equally spread load balancing approach is attempted to balance the allocations among available virtual machines. The Virtual Machines in the free state are allocated initially, and then with the minimum number of allocations, the algorithm selects Virtual Machines [109].

E. ROUND-ROBIN (RR) LOAD BALANCING

While distributing requests in a round-robin fashion, the virtual machines are selected dynamically using the round-robin load-balancing approach [110]. Regardless of VM status, the computation of the VM index continues as the new request arrives. For VM index computation, round-robin load balancing is characterized by low runtime overhead.

Table 2 can be referred to when comparing the review paper with existing ones. The unique contributions are highlighted within the table, and the existing review limitations are discussed well, emphasizing the requirement for future contributions. They are selected to support the points and provide credibility to compare the relevant references from the provided list.

X. TAXONOMY

A taxonomy of cloud brokerage mechanisms is presented based on functionalities, deployment models, and architecture.

The taxonomy presents the structured framework for the distribution of autonomic service in a cloud environment. In the context of autonomic service distribution, the in-depth understanding of functionalities, deployment, and architecture has been facilitated by delineating these dimensions.

Figure 8 introduces a taxonomy for cloud brokers, emphasizing the possible implementation of autonomic computing. The IaaS, PaaS, and the SaaS are identified as the three cloud service models. Self-protecting, self-healing, self-optimizing, and self-scaling brokers are the four essential features of autonomic cloud brokers. Every model has its unique capabilities, which this taxonomy figure mentions. Using these models, autonomic cloud brokers can focus on cost optimization, deployment management, and performance monitoring.

Significantly, cloud brokerage mechanisms' new taxonomy classifies techniques depending on the models of cloud service they support: "Software as a Service (SaaS)", "Platform as a Service (PaaS)", and "Infrastructure as a

TABLE 2. Comparison of cloud service load balancing and cloud brokering works.

Load Balancing Approach	Description	Current Review Benefits	Existing review drawbacks
Closest Data Center service brokering	The closest data centre for user requests can be selected by utilizing data transfer parameters and core responding latencies.	The response time can be minimized, and the resources can be utilized efficiently for users.	The availability factors are not considered, and the cloud brokering depends on the network proximity[105].
Optimized Response Time (ORT) service brokering	Based on processing capabilities and request size computation, the data centre with the lowest estimated response time is selected by minimizing the response time.	By prioritizing response time, the user experience will be improved. Multiple factors can be considered when making effective decisions.	An accurate response time estimation is required, which might be challenging in a few scenarios[19].
Throttled (THR) Load Balancing	Specific tasks are allocated for virtual machines, and until the current virtual machine becomes free, this might wait for the next allocation.	The overload on individual virtual machines can be prevented, and the fair allocation of resources can be ensured.	If the virtual machines are loaded heavily, latency can be introduced. This may not be suitable for real-time applications with latency requirements [107].
Equally Spread (ES) load balancing	The allocations among available virtual machines can be balanced by initially allocating free virtual machines.	The specific virtual machine overloading can be prevented, and the workload is distributed evenly across resources.	The differences in resource capabilities may not be considered, and if some virtual machines are underutilized, inefficient resource utilization might be experienced[109].
Round-Robin (RR) load balancing	The virtual machines are selected dynamically to distribute requests in a round-robin fashion.	The requests are distributed relatively among available resources and can be easily implemented.	Factors like resource availability might not be considered, and the overhead might be introduced due to continuous virtual machine index computation [110].

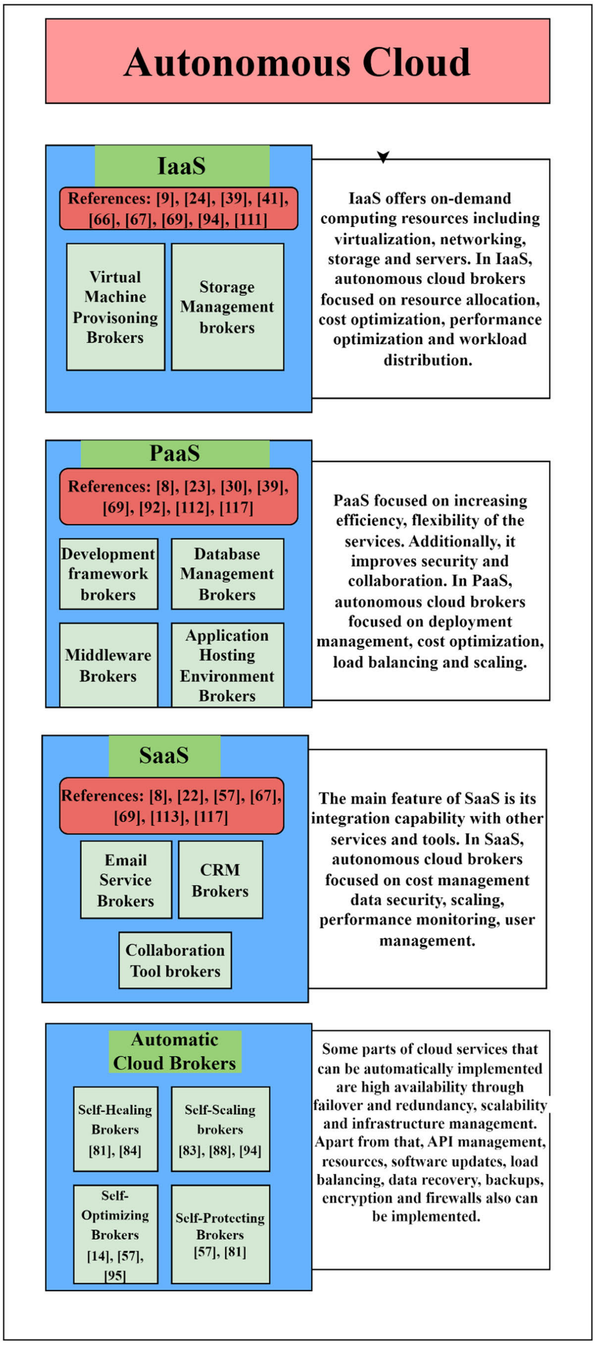

FIGURE 8. Taxonomy for cloud brokers.

Service (IaaS)''. Additionally, mechanisms for IaaS Brokerage concentrate on improving resource provisioning such as networking, storage and computing with criteria like cost management, load balancing and resource allocation efficiency [111]. Similarly, PaaS Brokerage addresses application platforms' management and deployment, highlighting development lifecycle support, application scaling, and service composition [112]. In contrast, SaaS Brokerage focuses on maintaining cloud-based software applications with criteria such as user access management, integration and service discovery [113]. However, this taxonomy is planned to align the brokerage mechanisms with the particular requirements of each cloud service model. SaaS concentrates on seamless user experience and application integration; PaaS demands fruitful platform support, and IaaS needs effective resource management. Moreover, this systematic approach confirms a better solution for appropriate cloud service management and distribution.

XI. CHALLENGES AND BEST PRACTICES OF CLOUD SECURITY

A. CHALLENGES

There are a few challenges associated with cloud security [27]. While developing a cloud approach, the mark for frequently including business units and executive staff is missed by many IT organizations. For cloud services used all over the organization, many enterprises are not conscious, and before estimating, they would have 20 times more applications. Even though cloud services are known, many enterprises fail to encrypt/decrypt the handling of sensitive data and granularly control access and compliance-related data in these applications. Many enterprises have no idea how to detect cloud threats like account compromise, malware, and data destruction. Most companies apply the same controls for all cloud-sensitive data and compliance requirements. Risky user behavior and cloud data loss prevention are disproportionately focused on, and for threat detection, the sensitive needs are managed by many organizations. Including resource management in a multi-cloud context, a few key issues are highlighted [9]. Among different cloud service providers, the challenges arose from the variations in reporting procedures and pricing structures. The challenging undertaking is managing the encryption keys in a multi-cloud context. By guaranteeing secure storage simultaneously, essential accessibility across several cloud platforms is required.

B. DATA SECURITY AND PRIVACY

Due to the increased sensitive data volume stored remotely, significant challenges are posed when ensuring data security in a cloud computing environment. Implementing a robust data encryption mechanism is included as one of the open issues in this area, as it requires data to be secured to establish granular access control policies for regulating data access based on individual roles [70]. The open issues can be addressed by addressing the concerns related to data sovereignty and ensuring compliance with evolving requirements like CCPA, GDPR, and HIPAA. Additionally, when choosing data storage locations and cloud providers, the organization must consider the data residency requirements.

C. INTEROPERABILITY AND VENDOR LOCK-IN

For organizations seeking to leverage multiple cloud environments, one of the ongoing challenges is achieving interoperability among different cloud platforms. The data portability across heterogeneous cloud environments and the APIs to facilitate seamless integration are identified as a few open issues that include massive efforts. Organizations must develop effective strategies to mitigate the risks associated with vendor lock-in and handle vendor dependencies [73]. Additionally, collaboration among cloud providers is needed to ensure compatibility among the cloud services and promote vendor-neutral solutions.

D. SCALABILITY AND PERFORMANCE

To ensure the utilization of cost-effective resources and reach user demands, scalability optimization in cloud resources is essential. The minimal bandwidth constraints and network latency are a few challenges in a cloud environment. Based on requirements, the scale of resources and fluctuating demand patterns can be accommodated [70]. Organizations must consider caching strategies, data locality and distributed computing techniques to enhance the scalability in distributed cloud environments.

E. RESOURCE ALLOCATION AND MANAGEMENT

Careful planning and coordination are required to efficiently manage the resources across multiple cloud providers. The development of dynamic resource provisioning mechanisms for allocating resources based on user demand is an open issue under resource management for defining the resource allocation policies to prioritize critical workloads and enable robust monitoring tools to track resource utilization and the workload distribution required to be optimized. Additionally, while designing resource management strategies to achieve optimal performance in dynamic cloud environments, factors like resilience, cost optimization, and elasticity must be considered [73]. For making informed decisions about resource optimization, robust analytic tools help track real-time performance metrics. The inefficiencies can be identified, and corrective actions can be considered to enhance resource utilization by monitoring key performance indicators like network throughput and memory usage.

F. COMPLIANCE AND GOVERNANCE

For organizations operating in the cloud, reaching regulatory compliance requirements for governance policies is recognized as one of the significant challenges. The risks associated with data breaches can be managed, and the open issues in this area demonstrate compliance with industry standards. Governance controls are integrated into the cloud deployment pipelines to enforce best practices throughout the software development lifecycle. Additionally, to maintain cloud-based system security, the organization must address emerging threats like zero-day exploits and insider threats [73]. Organizations are required to stay vigilant to address emerging threats in cloud computing environments. The attack vectors that pose risks to cloud-based systems can be identified by including the monitoring industry trends. Cloud environments can be protected against evolving security risks by staying informed about adopting proactive security measures.

G. FUTURE RESEARCH CHALLENGES AND OFFER POTENTIAL DIRECTIONS

In this study, different future research challenges have been identified. Firstly, advanced techniques are lacking to manage increasingly dynamic and complex cloud environments, optimizing autonomic service distributions' accuracy and efficiency [16]. Secondly, companies have experienced challenges integrating emerging technologies, including machine learning and AI, to increase their real-time decision-making and predictive capabilities [114]. Besides these, in "autonomic cloud brokerage", addressing privacy and security concerns remains critical, especially as access control and data handling become more sophisticated. Additionally, research must investigate cloud brokers' scalability in hybrid and multi-cloud environments, confirming they can easily manage distributed and diverse resources. So, some standardized benchmarks and metrics are needed to assess autonomic service distribution instruments' performance, facilitating improvement and comparison across different cloud platforms.

In "autonomic cloud brokerage", this study has provided some notable recommendations to address research limitations, such as developing advanced techniques that use machine learning and AI for adaptive and more accurate service distribution. In addition, research needs to emphasize incorporating effective security frameworks to solve emerging privacy issues and confirm seamless scalability across hybrid and multi-cloud environments. Furthermore, establishing standardized benchmarks and metrics will assist in comparing and assessing autonomic mechanisms [115]. Subsequently, exploring novel techniques will further increase performance for automating resource management and real-time predictive analytics [116]. So, these directions will improve autonomic cloud service distribution's reliability and efficiency and drive innovation.

H. BEST PRACTICES

However, depending on the findings of this study, best practices in this field include incorporating a solid security framework that implements real-time threat detection, access and identity management, and encryption. Apart from that, to mitigate vulnerabilities, regularly patching and updating systems is essential. Simultaneously, for the efficiency of service distribution, applying auto-scaling and dynamic load balancing aids in improving resource allocation depending on real-time demand. However, employing AI and advanced algorithms for predictive analytics confirms scalability and optimal performance. Finally, adopting continuous monitoring and standardized metrics facilitates performance improvements and evaluation. So, these practices strongly increase resilience, efficiency and security in cloud environments.

The team education concept is imperative to encompass the intricacies associated with operating on diverse cloud platforms and possesses a profound comprehension of multi-cloud security principles. The unique characteristics of every cloud environment are considered in comprehensive incident response plan development. These plans must encompass specific methods to minimize and identify the problems effectively, including Platform as a Service (PaaS), Infrastructure as a Service (Iaas), and Software as a Service (Saas). By considering the nature of service provision, the delineation of security responsibilities among cloud providers and corporations must be established explicitly. Additionally, careful consideration should be provided for service-level agreement contracts.

To achieve consistency across all cloud environments, the consolidation of security tools needs to be considered, and this was imperative to corresponding usage rules and establishing uniformity in security tools. Consistent security policy implementation is recognized as one of the significant aspects of maintaining a secure environment. Security is identified as the first concern in the cloud environment. The first stages of deployment and development procedures should be considered when choosing cloud providers. For data protection and information security, Identity and access management are considered an essential aspect [117]. Data integrity and confidentiality can be guaranteed by implementing encryption methods across all data lifecycle stages, including data processing, storage, and transmission. To provide data accessibility as required, the study aims to enable solutions for encryption key management.

XII. CONCLUSION

This study aims to gain vast knowledge in the rapidly developing industry of cloud brokerage. A systematic literature survey is conducted during this study to guarantee comprehensive coverage of such solutions. The research study is done effectively by highlighting the significant achievements as well as unresolved issues and depicting the current state of cloud brokerage. The best platform for deploying and managing applications should be selected based on the growing number of cloud providers. The cloud service broker assists the cloud consumer in choosing the appropriate cloud service provider. During the study, the core roles of cloud service brokers, such as service arbitrage, service aggregation, and service intermediation, are explained efficiently. The study's principal objective is to conduct an effective literature survey on the paradigms of cloud service selection and cloud service brokers. The regulations and standards consider the potential for redundancy and high complexity.

Additionally, this review explores major findings, such as significant cloud brokerage mechanisms' identification and their responsibilities in increasing service distribution. The new taxonomy's introduction also categorizes brokerage tools by different service models such as SaaS, PaaS and IaaS. These three improving and understanding models offer a systematic framework for improving and understanding cloud service management. Moreover, this taxonomy offers targeted development and research by clarifying challenges and needs related to each service model. Furthermore, it applies to future studies such as addressing emerging scalability and security issues, advancing algorithmic innovations, and allowing more precise evaluations.

The consideration of established standard models, best practices, patterns, and architectures is required to manage the complexities associated with overlaps, compliance complexities, and uncertainties. It is necessary to make specific efforts to identify the instances of overlap and examine regulatory policies. Due to a lack of initiative in improving software architecture precision at an advanced level, providing practical guidance for implementation and design endeavors is necessary. The security, compliance, and overall software quality can be enhanced within cloud systems by enabling standardized methodologies. To manage growing complexities, this study investigates the extent to which industries consider certain features. As an essential feature, the correct architecture utilization is prioritized even though several factors influence compliance. By entering new service specifications, the contract between two parties or users is established if the facilities of the broker agent search for the optimal data center as per user requirements.

Among several stakeholders in the architecture field, including service providers, developers, and business owners, the utilization of architectural patterns serves as a shared communication column. For the automated system execution utilized in the testing realm and compliance verification, the utilization of architectural patterns served as a reference point. By focusing on services, regulations, and policy-based systems, more research areas (RAs) must be developed to improve the overall software quality. Enhanced flexibility is offered using abstract compliance architecture for emerging rules that are important in persuading the sector. Based on compliance that enhances security, the integration efforts should focus on establishing a cohesive approach encompassing both facets. Further studies are required to focus more on assisting the CSCs in specifying application requirements and making effective decisions related to cloud provider selection.

In summation, the findings of this review have remarkable utilization in cloud computing. It offers a practical taxonomy for the mechanisms of cloud brokerage. Additionally, it increases security and service distribution efficiency. Furthermore, this taxonomy enables firms to customize their cloud techniques to particular models, including SaaS, PaaS and IaaS, resulting in more effective security and fault management, improved load balancing and optimized resource management. So, companies can achieve more cost-effective, scalable and reliable solutions by addressing identified challenges and adopting the recommended strategies. However, these advancements improve whole service delivery, streamline cloud operations and drive innovations, positively influencing the cloud computing field.

ACKNOWLEDGMENT

This work was conducted at the IoT and Wireless Communication Protocols Laboratory, ECE Department, International Islamic University Malaysia.

REFERENCES

[1] A. R. Kunduru, "The perils and defenses of enterprise cloud computing: A comprehensive review," *Central Asian J. Math. Theory Comput. Sci.*, vol. 4, no. 9, pp. 29–41, Sep. 2023.

[2] A. Sunyaev, "Cloud computing," in *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, A. Sunyaev, Ed., Cham, Switzerland: Springer, 2020, pp. 195–236, doi: 10.1007/978-3-030-34957-8_7.

[3] C. P. Amajuoyi, L. K. Nwobodo, and M. D. Adegbola, "Transforming business scalability and operational flexibility with advanced cloud computing technologies," *Comput. Sci. IT Res. J.*, vol. 5, no. 6, pp. 1469–1487, Jun. 2024.

[4] M. Rak, A. Cuomo, and U. Villano, "Cost/performance evaluation for cloud applications using simulation," in *Proc. Workshops Enabling Technol., Infrastruct. Collaborative Enterprises*, Jun. 2013, pp. 152–157, doi: 10.1109/WETICE.2013.36.

[5] N. Fareghzadeh, M. A. Seyyedi, and M. Mohsenzadeh, "Toward holistic performance management in clouds: Taxonomy, challenges and opportunities," *J. Supercomput.*, vol. 75, no. 1, pp. 272–313, Jan. 2019, doi: 10.1007/s11227-018-2679-9.

[6] A. Jindal, "Optimized task scheduling algorithm for cloud computing," in *Information and Communication Technology for Sustainable Development*, D. K. Mishra, M. K. Nayak, and A. Joshi, Eds., Singapore: Springer, 2018, pp. 431–439, doi: 10.1007/978-981-10-3932-4_45.

[7] L. Heilig, E. Lalla-Ruiz, and S. Voß, "A cloud brokerage approach for solving the resource management problem in multi-cloud environments," *Comput. Ind. Eng.*, vol. 95, pp. 16–26, May 2016, doi: 10.1016/j.cie.2016.02.015.

[8] A. Katal, S. Dahiya, and T. Choudhury, "Energy efficiency in cloud computing data centers: A survey on software technologies," *Cluster Comput.*, vol. 26, no. 3, pp. 1845–1875, Jun. 2023, doi: 10.1007/s10586-022-03713-0.

[9] B. Cinar, "The role of cloud service brokers: Enhancing security and compliance in multi-cloud environments," *J. Eng. Res. Rep.*, vol. 25, no. 10, pp. 1–11, Oct. 2023.

[10] R. Sissodia, M. S. Rauthan, and V. Barthwal, "Service level agreements (SLAs) and their role in establishing trust," in *Analyzing and Mitigating Security Risks in Cloud Computing*. Hershey, PA, USA: IGI Global, 2024, pp. 182–193, doi: 10.4018/979-8-3693-3249-8.ch009.

[11] S. Al-E'mari, Y. Sanjalawe, A. Al-Daraiseh, M. B. Taha, and M. Aladaileh, "Cloud datacenter selection using service broker policies: A survey," *Comput. Model. Eng. Sci.*, vol. 139, no. 1, pp. 1–41, 2024, Accessed: Aug. 5, 2024. [Online]. Available: https://www.researchgate.net/profile/Salam-Al-Emari/publication/377057309_Cloud_Datacenter_Selection_Using_Service_Broker_Policies_A_Survey/links/6597f8820bb2c7472b3603f1/Cloud-Datacenter-Selection-Using-Service-Broker-Policies-A-Survey.pdf

[12] R. Jain, N. Sharma, and T. Sharma, "Enhancement in performance of service broker algorithm using fuzzy rules," in *Proc. 2nd Int. Conf. Inventive Syst. Control (ICISC)*, Jan. 2018, pp. 922–925, doi: 10.1109/ICISC.2018.8398934.

[13] A. Jyoti, M. Shrimali, S. Tiwari, and H. P. Singh, "Cloud computing using load balancing and service broker policy for IT service: A taxonomy and survey," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 11, pp. 4785–4814, Nov. 2020, doi: 10.1007/s12652-020-01747-z.

[14] A. M. Manasrah, A. Aldomi, and B. B. Gupta, "An optimized service broker routing policy based on differential evolution algorithm in fog/cloud environment," *Cluster Comput.*, vol. 22, no. S1, pp. 1639–1653, Jan. 2019, doi: 10.1007/s10586-017-1559-z.

[15] J. K. Konjaang and L. Xu, "Meta-heuristic approaches for effective scheduling in infrastructure as a service cloud: A systematic review," *J. Netw. Syst. Manage.*, vol. 29, no. 2, p. 15, Jan. 2021, doi: 10.1007/s10922-020-09577-2.

[16] M. Kumar, S. C. Sharma, S. Goel, S. K. Mishra, and A. Husain, "Autonomic cloud resource provisioning and scheduling using meta-heuristic algorithm," *Neural Comput. Appl.*, vol. 32, no. 24, pp. 18285–18303, Dec. 2020, doi: 10.1007/s00521-020-04955-y.

[17] M. Conforti, M. De Santis, M. Di Summa, and F. Rinaldi, "Scanning integer points with lex-inequalities: A finite cutting plane algorithm for integer programming with linear objective," *4OR-Q J. Oper. Res.*, vol. 19, no. 4, pp. 531–548, Dec. 2021, doi: 10.1007/s10288-020-00459-6.

[18] F. Folgado, D. Calderón, I. González, and A. Calderón, "Review of Industry 4.0 from the perspective of automation and supervision systems: Definitions, architectures and recent trends," *Electronics*, vol. 13, no. 4, p. 782, Feb. 2024, doi: 10.3390/electronics13040782.

[19] R. Valarmathi and T. Sheela, "Differed service broker scheduling for data centres in cloud environment," *Comput. Commun.*, vol. 146, pp. 186–191, Oct. 2019, doi: 10.1016/j.comcom.2019.08.007.

[20] *CASB: Cloud Access Security Brokers Explained in Detail*. Accessed: Apr. 22, 2024. [Online]. Available: https://spin.ai/blog/api-casb-cloud-access-security-broker/

[21] A. Premchand, M. Sandhya, and S. Sankar, "Simplification of application operations using cloud and DevOps," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 13, no. 1, p. 85, Jan. 2019.

[22] R. Bose, S. Sengupta, and S. Roy, *Interpreting SLA and Related Nomenclature in Terms of Cloud Computing: A Layered Approach to Understanding Service Level Agreements in the Context of Cloud Computing*. Saarbrücken, Germany: Lambert Academic Publishing, 2023. Accessed: Mar. 28, 2024. [Online]. Available: http://111.93.178.142:25000/jspui/bitstream/123456789/323/1/978-620-2-19960-5_Interpreting%20SLA%20and%20related%20nomenclature%20in%20terms%20of%20Cloud%20Computing_Sandip%20Roy.pdf

[23] A. Abbas. (2023). *Cloud Access Security Brokers (CASBs): Enhancing Cloud Security Posture*. Accessed: Mar. 28, 2024. [Online]. Available: https://osf.io/zsv7d/download

[24] W. Qi, M. Sun, and S. R. A. Hosseini, "Facilitating big-data management in modern business and organizations using cloud computing: A comprehensive study," *J. Manage. Org.*, vol. 29, no. 4, pp. 697–723, Jul. 2023, doi: 10.1017/jmo.2022.17.

[25] M. H. Ghahramani, M. Zhou, and C. T. Hon, "Toward cloud computing QoS architecture: Analysis of cloud systems and cloud services," *IEEE/CAA J. Autom. Sinica*, vol. 4, no. 1, pp. 6–18, Jan. 2017, doi: 10.1109/JAS.2017.7510313.

[26] D. Harauzek. (2022). *Cloud Computing: Challenges of Cloud Computing From Business Users Perspective—Vendor Lock-in*. Accessed: Mar. 28, 2024. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-115089

[27] S. Ahmad, S. Mehfuz, F. Mebarek-Oudina, and J. Beg, "RSM analysis based cloud access security broker: A systematic literature review," *Cluster Comput.*, vol. 25, no. 5, pp. 3733–3763, Oct. 2022, doi: 10.1007/s10586-022-03598-z.

[28] L. Liu, J. Zhang, S. H. Song, and K. B. Letaief, "Client-edge-cloud hierarchical federated learning," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6. Accessed: Mar. 28, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9148862/

[29] E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas, and A. Rekeraho, "Enhancing cloud security-proactive threat monitoring and detection using a SIEM-based approach," *Appl. Sci.*, vol. 13, no. 22, p. 12359, 2023.

[30] V.-N. Pham, M. D. Hossain, G.-W. Lee, and E.-N. Huh, "Efficient data delivery scheme for large-scale microservices in distributed cloud environment," *Appl. Sci.*, vol. 13, no. 2, p. 886, Jan. 2023.

[31] L. Yin, J. Liu, Y. Fang, M. Gao, M. Li, and F. Zhou, "Two-stage hybrid genetic algorithm for robot cloud service selection," *J. Cloud Comput.*, vol. 12, no. 1, p. 95, Jun. 2023, doi: 10.1186/s13677-023-00458-y.

[32] J. Zhou, U. K. Lilhore, P. M, T. Hai, S. Simaiya, D. N. A. Jawawi, D. Alsekait, S. Ahuja, C. Biamba, and M. Hamdi, "Comparative analysis of metaheuristic load balancing algorithms for efficient load balancing in cloud computing," *J. Cloud Comput.*, vol. 12, no. 1, p. 85, Jun. 2023, doi: 10.1186/s13677-023-00453-3.

[33] D. A. Shafiq, N. Z. Jhanjhi, A. Abdullah, and M. A. Alzain, "A load balancing algorithm for the data centres to optimize cloud computing applications," *IEEE Access*, vol. 9, pp. 41731–41744, 2021, doi: 10.1109/ACCESS.2021.3065308.

[34] G. Fernandez and J. A. Renjith, "An approach on performance monitoring in cloud application," in *Proc. 5th Int. Conf. Sci. Technol. Eng. Math. (ICONSTEM)*, Mar. 2019, pp. 201–207. Accessed: Aug. 6, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8918800/

[35] J.-B. Lee, T.-H. Yoo, E.-H. Lee, B.-H. Hwang, S.-W. Ahn, and C.-H. Cho, ''High-performance software load balancer for cloud-native architecture,'' *IEEE Access*, vol. 9, pp. 123704–123716, 2021.

[36] V. K. Verma and P. Gautam, ''Evaluations of distributed computing on auto-scaling and load balancing aspects in cloud systems,'' *Int. J. Appl. Math., Comput. Sci. Syst. Eng.*, vol. 2, pp. 1–7, Jan. 2020, Accessed: Aug. 6, 2024. [Online]. Available: https://wseas.com/journals/amcse/2020/amcsejournal2020-006.pdf

[37] R. S. S. Dittakavi, ''Evaluating the efficiency and limitations of configuration strategies in hybrid cloud environments,'' *Int. J. Intell. Autom. Comput.*, vol. 5, no. 2, pp. 29–45, 2022.

[38] S. Verma and A. Bala, ''Auto-scaling techniques for IoT-based cloud applications: A review,'' *Cluster Comput.*, vol. 24, no. 3, pp. 2425–2459, Sep. 2021, doi: 10.1007/s10586-021-03265-9.

[39] V. A. Leal Sobral, J. Nelson, L. Asmare, A. Mahmood, G. Mitchell, K. Tenkorang, C. Todd, B. Campbell, and J. L. Goodall, ''A cloud-based data storage and visualization tool for smart city IoT: Flood warning as an example application,'' *Smart Cities*, vol. 6, no. 3, pp. 1416–1434, May 2023.

[40] C. Giovanoli, ''Cloud service quality model: A cloud service quality model based on customer and provider perceptions for cloud service mediation,'' in *Proc. 9th Int. Conf. Cloud Comput. Services Sci.*, 2019, pp. 241–248. [Online]. Available: https://www.academia.edu/download/78664095/75875.pdf

[41] R. Khurana and R. K. Bawa, ''Quality based cloud service broker for optimal cloud service provider selection,'' *Int. J. Appl. Eng. Res.*, vol. 12, no. 18, pp. 7962–7975, 2017.

[42] N. Yigitbasi, A. Iosup, D. Epema, and S. Ostermann, ''C-meter: A framework for performance analysis of computing clouds,'' in *Proc. 9th IEEE/ACM Int. Symp. Cluster Comput. Grid*, May 2009, pp. 472–477. Accessed: Mar. 28, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5071907/

[43] A. Choudhary, ''A walkthrough of Amazon elastic compute cloud (Amazon EC2): A review,'' *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 9, no. 11, pp. 93–97, Nov. 2021.

[44] M. S. Al-Asaly, M. A. Bencherif, A. Alsanad, and M. M. Hassan, ''A deep learning-based resource usage prediction model for resource provisioning in an autonomic cloud computing environment,'' *Neural Comput. Appl.*, vol. 34, no. 13, pp. 10211–10228, Jul. 2022, doi: 10.1007/s00521-021-06665-5.

[45] M. Kaur and H. Kaur, ''Autonomic computing for sustainable and reliable fog computing,'' in *Proc. Int. Conf. Sustain. Comput. Sci., Technol. Manag. (SUSCOM)*, Rochester, NY, USA, Feb. 2019, p. 11, doi: 10.2139/ssrn.3363069.

[46] M. Mangla, S. Deokar, R. Akhare, and M. Gheisari, ''A proposed framework for autonomic resource management in cloud computing environment,'' in *Autonomic Computing in Cloud Resource Management in Industry 4.0*, T. Choudhury, B. K. Dewangan, R. Tomar, B. K. Singh, T. T. Toe, and N. G. Nhu, Eds., Cham, Switzerland: Springer, 2021, pp. 177–193, doi: 10.1007/978-3-030-71756-8_10.

[47] P. Dehraj and A. Sharma, ''A review on architecture and models for autonomic software systems,'' *J. Supercomput.*, vol. 77, no. 1, pp. 388–417, Jan. 2021, doi: 10.1007/s11227-020-03268-0.

[48] S. S. Gill, ''Modern computing: Vision and challenges,'' *Telematics Informat. Rep.*, vol. 13, Mar. 2024, Art. no. 100116, doi: 10.1016/j.teler.2024.100116.

[49] D. P. Sharma, B. K. Singh, A. T. Gure, and T. Choudhury, ''Autonomic computing: Models, applications, and brokerage,'' in *Autonomic Computing in Cloud Resource Management in Industry 4.0*, T. Choudhury, B. K. Dewangan, R. Tomar, B. K. Singh, T. T. Toe, and N. G. Nhu, Eds., Cham, Switzerland: Springer, 2021, pp. 59–90, doi: 10.1007/978-3-030-71756-8_4.

[50] R. S. M. L. Patibandla, V. L. Narayana, and A. P. Gopi, ''Autonomic computing on cloud computing using architecture adoption models: An empirical review,'' in *Autonomic Computing in Cloud Resource Management in Industry 4.0*, T. Choudhury, B. K. Dewangan, R. Tomar, B. K. Singh, T. T. Toe, and N. G. Nhu, Eds., Cham, Switzerland: Springer, 2021, pp. 195–212, doi: 10.1007/978-3-030-71756-8_11.

[51] P. Zhou, D. Zuo, K. M. Hou, Z. Zhang, J. Dong, J. Li, and H. Zhou, ''A comprehensive technological survey on the dependable self-management CPS: From self-adaptive architecture to self-management strategies,'' *Sensors*, vol. 19, no. 5, p. 1033, Feb. 2019, doi: 10.3390/s19051033.

[52] M. Klymash, A. Luntovskyy, M. Beshley, I. Melnyk, and A. Schill, *Emerging Networking in the Digital Transformation Age: Approaches, Protocols, Platforms, Best Practices, and Energy Efficiency*, vol. 965. Cham, Switzerland: Springer, 2023. Accessed: Aug. 6, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=tdy0EAAAQBAJ&oi=fnd&pg=PR5&dq=self-configuration+key+benchmarks+human+intervention%E2%80%99s+frequency+and+time-to-deploy,++in+cloud+computing+&ots=-Ftdu2TTsc&sig=G29bvIW-b_2plfzLswuPj0NeEeE

[53] V. Shahane, ''Towards real-time automated failure detection and self-healing mechanisms in cloud environments: A comparative analysis of existing systems,'' *J. Artificial Intell. Res. Appl.*, vol. 4, no. 1, Art. no. 1, Feb. 2024.

[54] O. Adeniyi, A. S. Sadiq, P. Pillai, M. A. Taheir, and O. Kaiwartya, ''Proactive self-healing approaches in mobile edge computing: A systematic literature review,'' *Computers*, vol. 12, no. 3, p. 63, Mar. 2023.

[55] J. P. Dias, T. B. Sousa, A. Restivo, and H. S. Ferreira, ''A pattern-language for self-healing Internet-of-Things systems,'' in *Proc. Eur. Conf. Pattern Lang. Programs (EuroPLoP)*. New York, NY, USA: Association for Computing Machinery, Dec. 2020, pp. 1–17, doi: 10.1145/3424771.3424804.

[56] S. Harsha and F. Sreeharsha, ''Data privacy and security considerations in self-healing networks: Balancing automation and confidentiality,'' *Int. Res. J. Eng. Technol. (IRJET)*, vol. 11, no. 5, pp. 1–11, May 2024.

[57] M. Ghobaei-Arani, S. Jabbehdari, and M. A. Pourmina, ''An autonomic approach for resource provisioning of cloud services,'' *Cluster Comput.*, vol. 19, no. 3, pp. 1017–1036, Sep. 2016, doi: 10.1007/s10586-016-0574-9.

[58] P. Gupta, S. S. Patra, M. K. Gourisaria, A. Mishra, and N. S. Goje, ''Resource management issues and challenges in autonomic computing,'' in *Autonomic Computing in Cloud Resource Management in Industry 4.0*, T. Choudhury, B. K. Dewangan, R. Tomar, B. K. Singh, T. T. Toe, and N. G. Nhu, Eds., Cham, Switzerland: Springer, 2021, pp. 123–147, doi: 10.1007/978-3-030-71756-8_7.

[59] J. Sekar and L. L. C. Aquilanz, ''Autonomous cloud management using AI: Techniques for self-healing and self-optimization,'' *J. Emerg. Technol. Innov. Res.*, vol. 11, pp. 571–580, Jan. 2023.

[60] E. Henrichs, V. Lesch, M. Straesser, S. Kounev, and C. Krupitzer, ''A literature review on optimization techniques for adaptation planning in adaptive systems: State of the art and research directions,'' *Inf. Softw. Technol.*, vol. 149, Sep. 2022, Art. no. 106940.

[61] P. Q. Velasco, K. Hippalgaonkar, and B. Ramalingam. (2024). *Emerging Trends in Multi-Objective Optimization of Organic Synthesis Leveraging High-Throughput Tools and Machine Learning Methods*. Accessed: Aug. 6, 2024. [Online]. Available: https://chemrxiv.org/engage/chemrxiv/article-details/6686407501103d79c5f811aa

[62] V. Jain, Chitra, N. Batra, J. Marriappan, and P. K. Kaithal, ''Autonomic computing system: Threats, security issues and an efficient approach for self protection,'' *Mater. Today, Proc.*, vol. 80, pp. 2951–2955, Jan. 2023.

[63] B. Maati and D. E. Saidouni, ''CIoTAS protocol: CloudIoT available services protocol through autonomic computing against distributed denial of services attacks,'' *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 11, pp. 15175–15204, Nov. 2023, doi: 10.1007/s12652-020-02556-0.

[64] S. R. Sindiramutty, ''Autonomous threat hunting: A future paradigm for AI-driven threat intelligence,'' 2023, *arXiv:2401.00286*.

[65] L. Malburg, M. Hoffmann, and R. Bergmann, ''Applying MAPE-K control loops for adaptive workflow management in smart factories,'' *J. Intell. Inf. Syst.*, vol. 61, no. 1, pp. 83–111, Aug. 2023, doi: 10.1007/s10844-022-00766-w.

[66] S. Kansal, H. Kumar, S. Kaushal, and A. K. Sangaiah, ''Genetic algorithm-based cost minimization pricing model for on-demand IaaS cloud service,'' *J. Supercomput.*, vol. 76, no. 3, pp. 1536–1561, Mar. 2020, doi: 10.1007/s11227-018-2279-8.

[67] I. Lee, ''Pricing and profit management models for SaaS providers and IaaS providers,'' *J. Theor. Appl. Electron. Commerce Res.*, vol. 16, no. 4, pp. 859–873, Feb. 2021, doi: 10.3390/jtaer16040049.

[68] K. O. Shakerkhan and E. T. Abilmazhinov, ''Development of a method for choosing cloud computing on the platform of paas for servicing the state agencies,'' *Int. J. Modern Educ. Comput. Sci.*, vol. 11, no. 9, pp. 14–25, Sep. 2019, doi: 10.5815/ijmecs.2019.09.02.

[69] F. Wulf, T. Lindner, M. Westner, and S. Strahringer, "IaaS, PaaS, or SaaS? The why of cloud computing delivery model selection—Vignettes on the post-adoption of cloud computing," in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, 2021, pp. 6285–6294. Accessed: Apr. 22, 2024. [Online]. Available: https://opus4.kobv.de/opus4-oth-regensburg/frontdoor/index/index/docId/791

[70] G. Tricomi, G. Merlino, A. Panarello, and A. Puliafito, "Optimal selection techniques for cloud service providers," *IEEE Access*, vol. 8, pp. 203591–203618, 2020.

[71] S. Ahmad, S. Mehfuz, and J. Beg, "Securely work from home with CASB policies under COVID-19 pandemic: A short review," in *Proc. 9th Int. Conf. Syst. Modeling Advancement Res. Trends (SMART)*, Dec. 2020, pp. 109–114. Accessed: Mar. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9337121/

[72] B. Collier, "Considerations for selecting and implementing cloud security solutions using cloud access security brokers," Ph.D. thesis, Dept. Inf. Technol., Marymount Univ., Arlington, VA, USA, 2023. Accessed: Aug. 6, 2024. [Online]. Available: https://search.proquest.com/openview/52d7a6fea5f9b55f7db20b628c5721ed/1?pq-origsite=gscholar&cbl=18750&diss=y

[73] S. Kaur and R. Gupta, "Enhancing features of cloud computing using cloud access security brokers to avoid data breaches," *Eur. J. Eng. Technol. Res.*, vol. 4, no. 10, pp. 185–189, Oct. 2019.

[74] F. Pires, O. R. Pacheco, and R. T. Martins, "Why you should care about GDPR in IoT enterprises & solutions," in *Proc. 16th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Jun. 2021, pp. 1–9. Accessed: Aug. 6, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9476614/

[75] M. Howard, S. Curzi, and H. Gantenbein, *Designing and Developing Secure Azure Solutions*. Redmond, WA, USA: Microsoft Press, 2022. Accessed: Aug. 6, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=jtfPEAAAQBAJ&oi=fnd&pg=PT23&dq=Azure+AD+Conditional+Access+with+CASB+implementation+by+Microsoft.&ots=MHVB4ghDZC&sig=fLqTojBDGABUDa2m9xTEBXiReiU

[76] N. A. Angel, D. Ravindran, P. M. D. R. Vincent, K. Srinivasan, and Y.-C. Hu, "Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies," *Sensors*, vol. 22, no. 1, p. 196, Dec. 2021.

[77] M. A. N. Saif, S. K. Niranjan, and H. D. E. Al-Ariki, "Efficient autonomic and elastic resource management techniques in cloud environment: Taxonomy and analysis," *Wireless Netw.*, vol. 27, no. 4, pp. 2829–2866, May 2021, doi: 10.1007/s11276-021-02614-1.

[78] M. Brouwer and A. Groenewegen, "Cloud access security brokers (CASBs)," Univ. Amsterdam, Amsterdam, The Netherlands, Tech. Rep. SNE/OS3.nl, pp. 2020–2021, 2021.

[79] X. Ou, "Research on data access security agent technology in cloud computing security," *J. Phys., Conf. Ser.*, vol. 1693, no. 1, Dec. 2020, Art. no. 012013. Accessed: Mar. 29, 2024. [Online]. Available: http://dx.doi.org/https://iopscience.iop.org/article/10.1088/1742-6596/1693/1/012013/meta

[80] W. Hassan, T.-S. Chou, X. Li, P. Appiah-Kubi, and T. Omar, "Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks," *Int. J. Informat. Commun. Technol. (IJ-ICT)*, vol. 8, no. 3, p. 162, Dec. 2019.

[81] D. Petcu, "Consuming resources and services from multiple clouds," *J. Grid Comput.*, vol. 12, no. 2, pp. 321–345, Jun. 2014, doi: 10.1007/s10723-013-9290-3.

[82] *Architecting Cloud-Enabled Systems: A Systematic Survey of Challenges and Solutions-Chauhan–2017—Software: Practice and Experience–Wiley Online Library*. Accessed: Mar. 29, 2024. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.2409

[83] V. Hayyolalam, B. Pourghebleh, A. A. Pourhaji Kazem, and A. Ghaffari, "Exploring the state-of-the-art service composition approaches in cloud manufacturing systems to enhance upcoming techniques," *Int. J. Adv. Manuf. Technol.*, vol. 105, nos. 1–4, pp. 471–498, Nov. 2019, doi: 10.1007/s00170-019-04213-z.

[84] A. S. Alahmad, H. Kahtan, Y. I. Alzoubi, O. Ali, and A. Jaradat, "Mobile cloud computing models security issues: A systematic review," *J. Netw. Comput. Appl.*, vol. 190, Sep. 2021, Art. no. 103152, doi: 10.1016/j.jnca.2021.103152.

[85] A. Elhabbash, F. Samreen, J. Hadley, and Y. Elkhatib, "Cloud brokerage: A systematic survey," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–28, Jan. 2019, doi: 10.1145/3274657.

[86] M. Kumar, A. Kishor, J. Abawajy, P. Agarwal, A. Singh, and A. Y. Zomaya, "ARPS: An autonomic resource provisioning and scheduling framework for cloud platforms," *IEEE Trans. Sustain. Comput.*, vol. 7, no. 2, pp. 386–399, Apr. 2022, doi: 10.1109/TSUSC.2021.3110245.

[87] L. Hadded and T. Hamrouni, "Optimal autonomic management of service-based business processes in the cloud," *Soft Comput.*, vol. 26, no. 15, pp. 7279–7291, Aug. 2022, doi: 10.1007/s00500-022-07124-6.

[88] M. C. Huebscher and J. A. McCann, "A survey of autonomic computing—Degrees, models, and applications," *ACM Comput. Surv.*, vol. 40, no. 3, pp. 1–28, Aug. 2008, doi: 10.1145/1380584.1380585.

[89] R. Buyya, "A manifesto for future generation cloud computing: Research directions for the next decade," *ACM Comput. Surv.*, vol. 51, no. 5, pp. 1–38, Nov. 2018, doi: 10.1145/3241737.

[90] M. A. Khan, "Optimized hybrid service brokering for multi-cloud architectures," *J. Supercomput.*, vol. 76, no. 1, pp. 666–687, Jan. 2020, doi: 10.1007/s11227-019-03048-5.

[91] Q. M. Ashraf, M. H. Habaebi, M. R. Islam, and M. Tahir, "Autonomic computing in Internet of Things for resource management," *J. Next Gener. Inf. Technol.*, vol. 6, no. 4, p. 47, 2015.

[92] S. K. Addya, A. Satpathy, B. C. Ghosh, S. Chakraborty, S. K. Ghosh, and S. K. Das, "CoMCLOUD: Virtual machine coalition for multi-tier applications over multi-cloud environments," *IEEE Trans. Cloud Comput.*, vol. 11, no. 1, pp. 956–970, Jan. 2023.

[93] M. I. Alghamdi, "Optimization of load balancing and task scheduling in cloud computing environments using artificial neural networks-based binary particle swarm optimization (BPSO)," *Sustainability*, vol. 14, no. 19, p. 11982, Sep. 2022.

[94] A. Quarati and D. D'Agostino, "MOEA-based brokering for hybrid clouds," in *Proc. Int. Conf. High Perform. Comput. Simulation (HPCS)*, Jul. 2017, pp. 611–618. Accessed: Mar. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8035135/

[95] S. Goyal, S. Bhushan, Y. Kumar, A. U. H. S. Rana, M. R. Bhutta, M. F. Ijaz, and Y. Son, "An optimized framework for energy-resource allocation in a cloud environment based on the whale optimization algorithm," *Sensors*, vol. 21, no. 5, p. 1583, Feb. 2021.

[96] Q. M. Ashraf, M. Tahir, M. H. Habaebi, and J. Isoaho, "Towards autonomic Internet of Things: Recent advances, evaluation criteria and future research directions," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14725–14748, Aug. 2023, doi: 10.1109/JIOT.2023.3285359.

[97] M. Malawski, G. Juve, E. Deelman, and J. Nabrzyski, "Algorithms for cost- and deadline-constrained provisioning for scientific workflow ensembles in IaaS clouds," *Future Gener. Comput. Syst.*, vol. 48, pp. 1–18, Jul. 2015.

[98] I. Haddar, B. Raouyane, and M. Bellafkih, "Service broker-based architecture using multi-criteria decision making for service level agreement," *Comput. Inf. Sci.*, vol. 13, no. 1, p. 20, Dec. 2019.

[99] R. K. Naha and M. Othman, "Cost-aware service brokering and performance sentient load balancing algorithms in the cloud," *J. Netw. Comput. Appl.*, vol. 75, pp. 47–57, Nov. 2016.

[100] M. Tahir, Q. Mamoon Ashraf, and M. Dabbagh, "Towards enabling autonomic computing in IoT ecosystem," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2019, pp. 646–651. Accessed: Apr. 26, 2024.

[101] S. Acharya and D. A. D'Mello, "Energy and cost efficient dynamic load balancing mechanism for resource provisioning in cloud computing," *Int. J. Appl. Eng. Res.*, vol. 12, no. 24, pp. 15782–15790, 2017.

[102] D. Sugumaran and C. R. Bharathi. *Efficient Data Center Scheduling for Big Information Application Using Effective Client Handling Management Technique (ECHMT) in Cloud Computing*. Accessed: Mar. 29, 2024. [Online]. Available: https://www.academia.edu/download/67622460/IJARET_11_12_078.pdf

[103] A. I. El Karadawy, A. A. Mawgoud, and H. M. Rady, "An empirical analysis on load balancing and service broker techniques using cloud analyst simulator," in *Proc. Int. Conf. Innov. Trends Commun. Comput. Eng. (ITCE)*, Feb. 2020, pp. 27–32, doi: 10.1109/ITCE48509.2020.9047753.

[104] P. M. Rekha and M. Dakshayini, "Dynamic cost-load aware service broker load balancing in virtualization environment," *Proc.Comput. Sci.*, vol. 132, pp. 744–751, Jan. 2018, doi: 10.1016/j.procs.2018.05.086.

[105] M. A. Shahid, M. M. Alam, and M. M. Su'ud, ''Performance evaluation of load-balancing algorithms with different service broker policies for cloud computing,'' *Appl. Sci.*, vol. 13, no. 3, p. 1586, Jan. 2023, doi: 10.3390/app13031586.
[106] A. Katangur and S. Chowdhury, ''DEThresh: Enhancing cloud computing performance with differential evolution-driven datacenter selection and threshold-based load balancing optimization,'' Missouri State Univ., Springfield, MO, USA, Tech. Rep., Mar. 2024, doi: 10.21203/rs.3.rs-3929293/v1.
[107] M. Hashemi and A. Masoud, ''Load balancing algorithms in cloud computing analysis and performance evaluation,'' *IEEE*, vol. 3, no. 4, pp. 1–7, 2020.
[108] V. Priya, C. S. Kumar, and R. Kannan, ''Resource scheduling algorithm with load balancing for cloud service provisioning,'' *Appl. Soft Comput.*, vol. 76, pp. 416–424, Mar. 2019, doi: 10.1016/j.asoc.2018.12.021.
[109] G. A. P. Princess and A. S. Radhamani, ''A hybrid meta-heuristic for optimal load balancing in cloud computing,'' *J. Grid Comput.*, vol. 19, no. 2, p. 21, May 2021, doi: 10.1007/s10723-021-09560-4.
[110] G. Sinha and D. Sinha, ''Enhanced weighted round Robin algorithm to balance the load for effective utilization of resource in cloud environment,'' *EAI Endorsed Trans. Cloud Syst.*, vol. 6, no. 18, Sep. 2020, Art. no. 166284, doi: 10.4108/eai.7-9-2020.166284.
[111] A. K. Samha, ''Strategies for efficient resource management in federated cloud environments supporting infrastructure as a service (IaaS),'' *J. Eng. Res.*, vol. 12, no. 2, pp. 101–114, Jun. 2024.
[112] A. Mimidis-Kentis, J. Soler, P. Veitch, A. Broadbent, M. Mobilio, O. Riganelli, S. Van Rossem, W. Tavernier, and B. Sayadi, ''The next generation platform as a service: Composition and deployment of platforms and services,'' *Future Internet*, vol. 11, no. 5, p. 119, May 2019.
[113] A. Oluwabukola and A. Adebowale, ''An architectural model for SLA negotiation between SaaS and customers,'' *Int. J. Eng. Appl. Sci. Technol.*, vol. 5, no. 5, pp. 30–36, Sep. 2020.
[114] S. Kanungo, ''Edge-to-cloud intelligence: Enhancing IoT devices with machine learning and cloud computing,'' *International Peer-Reviewed Journal*, vol. 2, no. 12, pp. 238–245, 2019.
[115] M. S. Aslanpour, S. S. Gill, and A. N. Toosi, ''Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research,'' *Internet Things*, vol. 12, Dec. 2020, Art. no. 100273.
[116] D. Soni and N. Kumar, ''Machine learning techniques in emerging cloud computing integrated paradigms: A survey and taxonomy,'' *J. Netw. Comput. Appl.*, vol. 205, Sep. 2022, Art. no. 103419.
[117] C. Singh, R. Thakkar, and J. Warraich, ''IAM identity access management—Importance in maintaining security systems within organizations,'' *Eur. J. Eng. Technol. Res.*, vol. 8, no. 4, pp. 30–38, Aug. 2023, doi: 10.24018/ejeng.2023.8.4.3074.

MOHD HAMZAH KHAN received the bachelor's and master's degrees in computer science and engineering from Jamia Hamdard University, India, in 2015 and 2017, respectively. He is currently pursuing the Ph.D. degree in computer science and engineering with International Islamic University, Malaysia. He then worked as a Research Analyst for a year and half in a cybersecurity company. His active research interests include cloud brokers, autonomic cloud computing, autonomic load distribution, and load-balancing optimization.

MOHAMED HADI HABAEBI (Senior Member, IEEE) received the first degree from the Civil Aviation and Meteorology High Institute, Libya, in 1991, the M.Sc. degree in electrical engineering from Universiti Teknologi Malaysia, in 1994, and the Ph.D. degree in computer and communication system engineering from Universiti Putra Malaysia, in 2001. He is currently a Professor with the Department of Electrical and Computer Engineering, International Islamic University Malaysia. His research interests include wireless communication protocols, the Internet of Things, edge and cloud computing, wireless sensor and actuator networks, cognitive radio, small antenna systems, radio propagation, and engineering applications of artificial intelligence. He is a member of IET. He also serves as an active reviewer and is on the editorial board of several international journals. He is a C.Eng.

MD. RAFIQUL ISLAM (Senior Member, IEEE) received the B.Sc. degree in electrical and electronic engineering from BUET, Dhaka, in 1987, and the M.Sc. and Ph.D. degrees in electrical engineering from the University of Technology Malaysia, in 1996 and 2000, respectively. He is currently a Professor with the Department of Electrical and Computer Engineering, International Islamic University Malaysia. Over the course of his academic career, he has published more than 300 research papers in international journals and conferences. His research interests include antenna design, wireless channel modeling, RF and FSO propagation measurement, and modeling. He is a Life Fellow of the Institute of Engineers Bangladesh. He is a member of IET.