Chapter 14
Functionalities and Approaches of Multi-cloud Environment

A. Vijayalakshmi and Hridya

14.1 Introduction to Cloud Computing

Cloud computing is an evolving paradigm where various resources and applications are moved to the Internet so that the applications can be remotely shared among different resources. It enables ubiquitous network access to a pool of shared resources [1]. National Institute of Standards and Technology (NIST) defines cloud computing as a model that enables access to the shared pool with various configurable computing resources like networks, servers, applications, and services [2]. In this technological era cloud computing is considered as a very prevailing network architecture that performs complex computations. The various characteristics of cloud computing include infrastructure sharing where a virtualized software model is used in sharing the services and storage, providing services based on demand of the users by allowing access through Internet for PCs, laptops, etc. as shown in Fig. 14.1.

While using the shared resources, users are charged based on their usage in the particular billing period. The advantage of using cloud from a user's perspective is that it is inexpensive and very convenient as application need not be installed in the personal system; rather it can be accessed through the Internet. The various vital components of cloud computing are:

1. Cloud computing provides services for the needy on time. Any consumer who is in need of computing resources, namely, software resources, CPU time, etc., for a particular timeslot can access cloud services without any human interaction with cloud providers.

A. Vijayalakshmi (✉) · Hridya
CHRIST (Deemed to be University), Bangalore, India
e-mail: vijayalakshmi.nair@christuniversity.in; hridya@btech.christuniversity.in

R. Nagarajan et al. (eds.), *Operationalizing Multi-Cloud Environments*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-74402-1_14

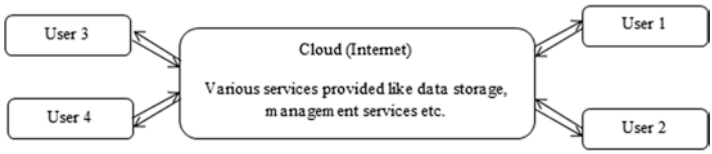

Fig. 14.1 Cloud characteristics

2. The services provided by cloud are accessible over the Internet by applications with diverse platforms that are at the consumer side.
3. The resources in a cloud service provider are pooled together so that multiple consumers are benefitted [3].

14.1.1 Architecture of Cloud

Basic 3 Tier cloud architecture is depicted in Fig. 14.2. The three Tiers in this architecture includes Load balancer server as the top layer, Application server in the second layer, and Database server in the bottom layer. Each of the Tier consists of dedicated server.

14.1.2 Service Models

Cloud computing is a model that is developed with the objective of convenient on demand access and usage of computing resources from a shared pool with minimalizing the interaction from the service provider [4]. The service from cloud server is categorized into three parts as shown in Fig. 14.3.

14.1.2.1 Cloud Infrastructure as a Service (IaaS)

This is a service offered by cloud computing in which the users access servers, storage, and networking resources as shown in Fig. 14.4. The advantage of using this service is that users need not purchase hardware and instead can pay for IaaS on demand and hence saving the cost of purchase and maintenance of hardware resources.

Servers: IaaS providers function to manage physical machines in various data centers around the world for powering the various layers of abstraction so that the services of these machines are made available to end users over the Internet.

Storage: The types of storage provided by cloud are block storage, file storage, and object storage. Block storage is where data files are stored in the cloud server for a fast and efficient data transfer. File storage help in application to access data

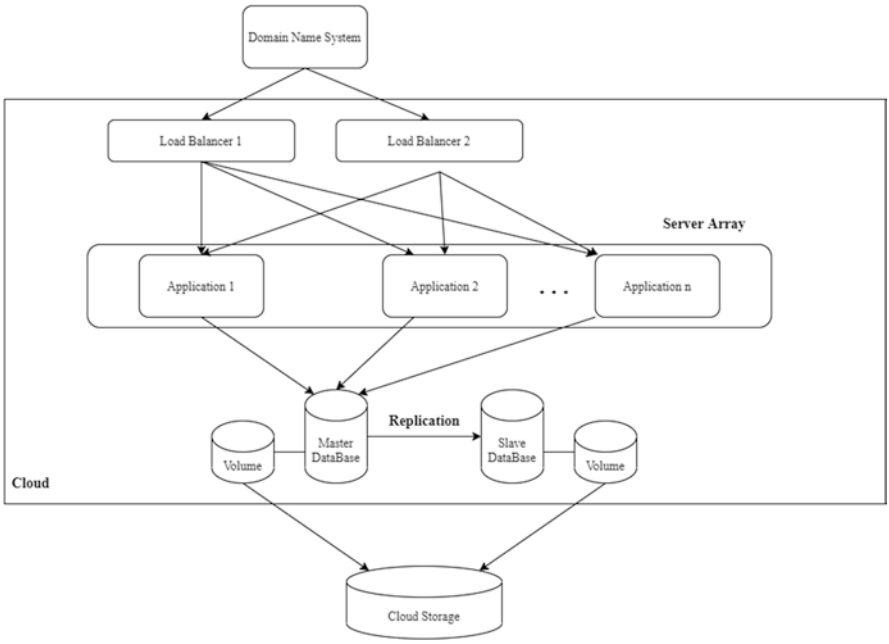

Fig. 14.2 Cloud architecture

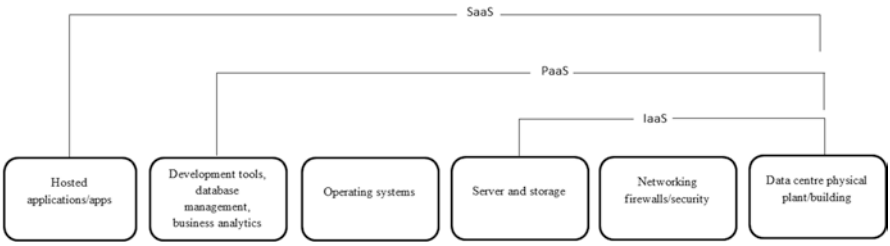

Fig. 14.3 Cloud services

through shared files. Object storage is highly distributed and is the most common mode of storage in cloud.

Network: In networking, the networking hardware like routers and switches are made available through APIs.

14.1.2.2 Cloud Platform as a Service (PaaS)

This is a service where cloud offers consumers with an environment where they can develop and manage various applications as shown in Fig. 14.5. PaaS provides platform for developing and testing applications, hence helping users not to worry on

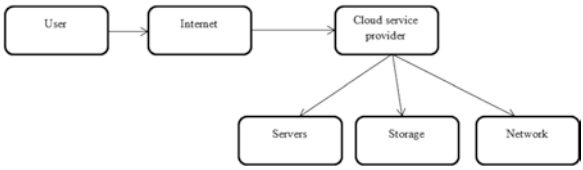

Fig. 14.4 Cloud resources

Fig. 14.5 Platform as a service

the infrastructure for the development of applications. This facility accomplishes the management of operating system and security by assisting team work.

14.1.2.3 Cloud Software as a Service (SaaS)

This is a feature offered by cloud server where the consumers can access cloud-based software. The applications that are installed in the cloud networks could be accessed by the users through web or an API. This is provided by the vendors through subscription, and use of resource is completely depending on the need as depicted in Fig. 14.6.

14.1.3 Deployment Models

Cloud community has defined the following deployment models [4].

Private cloud: Here the cloud server is solely operated and managed by a particular organization which can be located at the premise of the organization or outside. Security of data is one of the major concerns of building a private cloud. Apart from security, the cost incurred in transferring data from local system to public cloud is also a factor in developing a private cloud by organizations.

Community cloud: In this model several organizations with common objective jointly construct and share the same cloud infrastructure. Thus developed cloud infrastructure may be maintained and managed internally or by a third party vendor.

Public cloud: This form of infrastructure is used by normal public consumers whereas the service providers have complete ownership in managing the cloud with a detailed policy, cost, and charging, and hence this model is the most prevailing form of cloud deployment models.

Hybrid cloud: This model is a combination of two or more deployment models which is opted by organization to optimize the resources (Table 14.1).

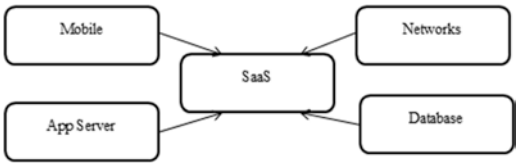

Fig. 14.6 Software as a service

Table 14.1 Pros and cons of various clouds

	Public cloud		Private cloud	Hybrid cloud
Pros	1.	Very simple to implement as well as use public cloud	Organization has a complete control over server updates and patches	Cost-efficient cloud strategy and flexible on utilization
	2.	Public clouds are bound to have negligible straightforward costs	Long-term expenditure is minimal	Hybrid clouds are less prone to extended services
	3.	Server virtualization can lead to utilization efficiency gains	Server virtualization can lead to utilization efficiency gains	Server virtualization can lead to utilization efficiency gains
	4.	Public clouds are widely accessible	–	Hybrid clouds are appropriate for large workloads
	5.	Public clouds do not need any space specifically dedicated for data center	–	–
Cons	1.	Public clouds are most expensive in long term	The upfront costs are large	Implementation is difficult as management schemes are complex
	2.	These types are susceptible to continued service outages	Private clouds are susceptible to continued service outages	Hybrid clouds require adequate space specially committed for data center
	3.	–	Access to the data is restricted	–
	4.	–	The space devoted to data center is large	–
	5.	–	Private clouds are not suited for handling large spikes in work load	–

14.2 Issues in Cloud Computing

Though cloud computing is a boon to the world of smart computing, there are few issues associated with cloud computing. Secure outsourcing of data is a major concern in cloud computing paradigm. The user making use of services provided by the cloud should be aware that the data sent to the cloud as well as the applications deployed in the cloud is controlled by the cloud provider. A strong trust should be

Table 14.2 Cloud computing issues – security strategies

Privacy model	Errors are difficult to find as well as correct System does not provide protection against attackers
Cloud computing privacy intrusion detection	Frequent update is necessary to avoid attackers There is a chance that non-intrusive information is incorrectly detected and terminated
Dirichlet reputation	Depends on complicated strategy that is difficult to implement Performance is dependent on user participation
Anonymous bonus point	The speed of data is reduced Intrusion protection is minimal Can be implemented in wireless application only
Network slicing	May be expensive while implemented in large network

formed between the user and the provider on the security of these data, and security plays a major issue in cloud computing [5–7]. The issues in cloud computing include various attacks on cloud interfaces as well as misusing the cloud services in order to attack other systems in the network [3]. Lists the difficulties in cloud computing with respect to various security strategies in Table 14.2.

Cloud computing provides different supports to the users through the Internet for storage, networking, software, and as server. Cloud storage helps in storing files and data in a remote storage that has access through the web. Cloud storage is preferred by people because it helps in saving the cost of resources for storage, high speed, and efficiency and increases the overall productivity. Cost saving and availability are the advantages of cloud computing. However, it carries along various challenges in terms of security of data. Cloud security is a major concern in people using cloud storage facility. It is very much necessary that proper security is provided to the sensitive data that are stored in cloud servers like credit card or debit card details, health information, etc. Cloud computing should take care of data breaches, loss of data, traffic attacks, distributed denial of service attacks, etc. The security concerns that are to be attended are data prevention, web security, location, identity and access management, recovery, data loss prevention, web and e-mail security, security assessments, regulatory compliance, violation management, event management, encryption, data segregation, business continuity, and disaster recovery. When data is stored in a remote database, the major concern is the security of data. Cloud service provides various security measures for the data stored in cloud [8].

14.3 Introduction to Multi-cloud

Cloud computing is a service provided to host applications and data in remote servers. The change in digital era has driven the companies toward multi-cloud architecture that enables shared services. Multi-cloud is a cloud computing approach made up of two or more cloud environments where applications are presented among the

heterogeneous networks. The transition from single cloud to multi-cloud data centers has always benefited the industry. This transition indicates the shift of traditional data centers to a pool of multiple private clouds on demand. Dedicated data servers from a private environment to hybrid and multi-cloud are deployment models that integrate more than one cloud. It differs from hybrid cloud in the cloud infrastructure. Hybrid cloud has a combination of two or more than two different types of clouds, whereas multi-cloud integrates different clouds of similar types. Hence, the term multi-cloud can be referred to as a cloud system where different cloud networks are combined to perform various roles. It is evident from the studies conducted that multi-clouds can address the security issues in cloud computing that are related to date integrity, intrusion, and service [9].

14.3.1 Single Cloud to Multi-cloud

NIST reported that services from different clouds can be used simultaneously or serially from one cloud to another [10]. Different multi-cloud use cases can be used to the maximum to provide flexibility and control over the workloads and cloud stored data. Since multi-cloud offers flexibility in cloud environment, the organizations are intended to meet the requirements of technical and commercial workload by adopting multi-cloud environment. Another advantage of multi-cloud is seen in the case geographical advantage in order to address the problems associated with latency issues. Also, there are times when the organizations use a certain cloud service for a short period in order to achieve their short-term goals. Apart from these, vendor lock-in problem is an issue which is a frequent concern in cloud computing that can be solved when multi-cloud strategy is used. Various multi-cloud use cases can be listed as follows [11].

- To access the services and resources based on various demands
- To improve the quality of service and optimize cost
- To use the services from various providers
- To avoid the dependency on a single provider
- To create backups of data so that disasters are dealt efficiently

14.3.2 Architecture of Multi-cloud

Multi-cloud architecture design is an appropriate solution for a reliable application being stored in cloud. Figure 14.7 shows a prominent multi-cloud architecture strategy where an application component can use different cloud services of other cloud platform and improve the overall performance.

To demonstrate cloudification, the Application-1 uses Amazon Web Service (AWS) for storage and Azure for computation. This improves availability and avoids

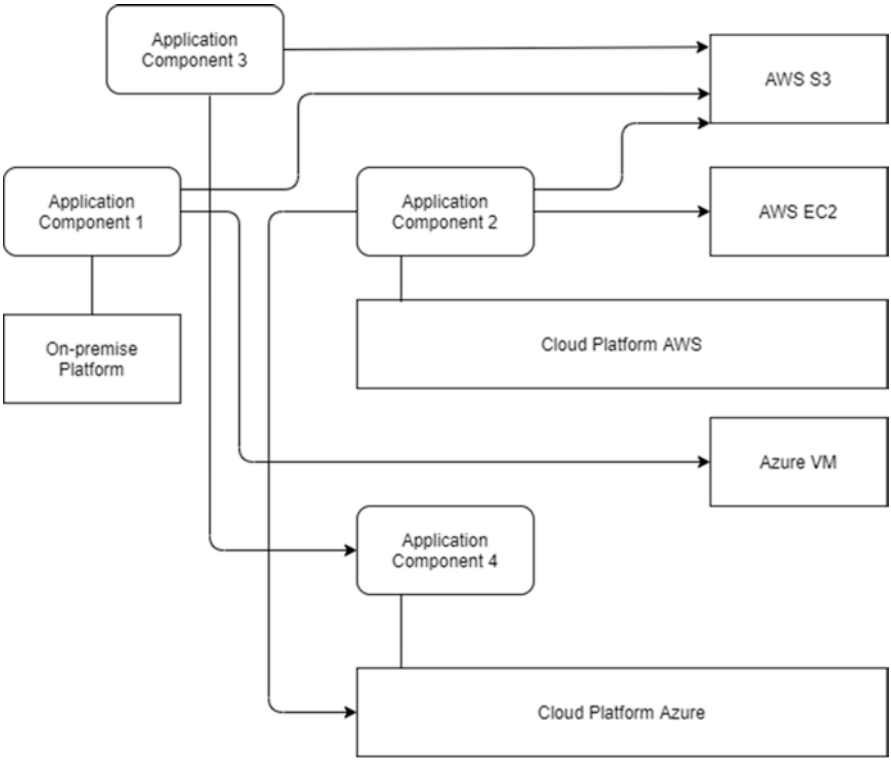

Fig. 14.7 Multi-cloud architecture

vendor lock-in. Application-2 demonstrates multi-cloud relocation where the application is re-hosted on AWS cloud platform and privilege is given to use environmental services provided by Azure. This method enhances the availability as the application that is re-hosted avoids vendor lock-in. Multi-cloud refactor is demonstrated using application component3 deployed on AWS using AWS3 and application4 on Azure so that the application can use any of the cloud service provided by Azure as per the requirement of the application. This method provides optimal performance and quickness to respond to changes [12].

14.3.3 Benefits of Multi-cloud

Multi-cloud offers various advantages and the most important of these is flexibility. With organizations adopting multi-cloud strategy, the organization has flexibility in choosing from various cloud service providers. Multi-cloud allows choosing varied set of services that are provided by various cloud providers. Managing deployment on various clouds is another important functionality of multi-cloud [11]. Ability in

distributing applications and services geographically is another benefit of multi-cloud computing. The user experience will increase as the app is closer to the target user [13]. Below are the advantages of multi-cloud listed as per [12].

Disaster recovery: It is difficult and risky when a particular organization has to manage its resources when it uses a cloud service. There can be cyber-attacks that can affect the end users to wait to access the data until the problem is solved. Using multi-cloud can help the users robust against such attacks as there are other clouds that can carry the workload when any one of them is affected.

Vendor lock-in: With multi-cloud, the various organizations have the privilege to choose the best service according to their objective of the organization. Hence while using multi-cloud, organizations can explore various providers and find the best match for each component of their operations.

Managing data: An organization can develop data that need to be accessed in varied intervals. There are cases in which some data may be stored in the database and not accessed for a long time, and some of them will be accessed in frequent intervals. In such cases, rather than storing these data in single cloud, you can make use of the right cloud for right function. An organization can also have data that are to be uploaded to the cloud, analyzed, and downloaded back. In such instances, the organization prefers a cloud service with speed and power. Hence, with multi-cloud, the organization has the privilege to access the right service depending on the frequency in which different data need to be accessed.

Cost optimization: The performance analysis of the workloads in various cloud platforms will help in saving the cost.

Low latency: In an environment with multi-cloud, the data center closest to the end user can serve the data requested from the end user with minimal delay. This can lead to unified experience for the user.

14.4 Security in Multi-cloud Architecture

The objective of cloud computing is to provide various resources to the end user as a service over the Internet. Security of data in cloud is an important aspect when quality of service of cloud is considered. Due to dynamic nature of cloud, various security threats emerge [14]. Cloud servers contain humongous confidential sensitive data. By using multiple distinct clouds and splitting data based on various components, threats associated with tampering of data can be brought down. Thus the confidentiality of data is maintained with multi-cloud strategy. When an organization uses multi-cloud strategy, it has the provision to use multiple distinct clouds at an instant of time so that it can reduce the risk of malicious data and tampering of data. The integration of distinct clouds makes it difficult for an attacker to tamper the data hosted in the cloud server [6, 9]. The concept of using multiple cloud was suggested by Bernstein and Celesti [15, 16] and various instances of cloud computing working together and further recommended grid capabilities in cloud computing.

Considering shared environment like cloud, giving maximum protection to the privacy of data and identity of clients is very necessary. Amazon S3 and Microsoft Azure which provide data as a service (DaaS) are the two very important and widely used cloud service where organizations can store data and can retrieve whenever needed based on various policies for gaining access. XACML is an access control model that specifies identity attributes like an individual's email address, age, location access, etc. to provide fine-grained data access. With cloud computing, data theft and privacy breach is not limited to the circle of an organization [17].

14.4.1 Algorithm for Data Security in Cloud

14.4.1.1 Encryption Algorithm

Encryption algorithms like RSA (Rivest, Shamir, Adleman), AES (Advanced Encryption Standard), XOR (Exclusive OR), and DES (Data Encryption Standard) have been a great advantage while considering security of data in cloud [18]. AES is an encryption standard, where the operation speed is fast and offers high safety on the data. This is a symmetric encryption algorithm which performs both encryption and decryption. The encryption procedure changes with respect to the key that changes the operation of AES algorithm. The encryption formula for AES is

$C = E(K, P)$where C is the cipher text, K is the key, E is the encryption function, and P is the plaintext.

The AES algorithm executes for Nr-1 loops on a 128-bit block of data. Nr (10,12 or 14) depends on the key length which can be 128, 192, or 256 bits in length. The steps in encryption are listed below.

Step 1: Sub Bytes.

This step is known as substitute bytes transformation which includes a 16×16 matrix as a table look called s-box. The matrix has the combination of 8 bits sequence. The left most 4 bits are used, the leftmost nibble of the byte is used to specify a particular row of the s-box, and the rightmost 4 bits indicate a column.

Step 2: Shift Row Transformation.

In this step, the rows of a particular state are shifted in a circular way toward left.

Step 3: Mixing of column transformation.

In this stage, a substitution takes place where columns are individually operated and every byte of a particular column is mapped with a new value that is a function of all the four bytes in the column.

14.4.1.2 Data De-duplication Technology

Data De-duplication is the process in which all the duplicate data are eliminated to reduce the storage required for these data. This in turn reduces the bandwidth for transfer of data across the network. This technique is a great benefit to the cloud

users in managing their data without duplication and it saves the storage. For secure data de-duplication, Rabin block algorithm is used which involves block-wise de-duplication of data.

14.4.1.3 Cloud Storage Technology

Cloud storage is a file server with complex functionality that can be helpful in storing and accessing stored data as and when required. The end user or the organizations upload the data and store the same on cloud servers that ensure security of these data. If there is a server failure, accessing the stored data will be difficult. To solve this, all the data nodes are added to the node at the backup to make sure data is available.

14.4.2 Good Practices in Multi-cloud Strategy

Organizations are increasingly adopting multi-cloud strategy with the fast development in the field [19]. If multi-cloud strategy is used with identical operations on two clouds, security settings should be the same across both the clouds. This is achieved by synchronizing policies across the cloud providers:

- If an organization is making use of varied workloads, independent security policies have to be created for every service.
- Automate various tasks of an organization to reduce the risk factor and ensure security.
- Choose the appropriate tool such that it allows to synchronize the security protocols across various cloud service providers.
- Create a strategy to monitor security that can consolidate logs and alerts from various platforms in one location.

14.5 Conclusion

The Internet has emerged into accumulation of humongous amount of data all around the world. Cloud computing has been of great advantage in order to store these data and access when in need. Data stored in cloud can be accessed from a remote server with the help of various services offered by cloud service providers. Transition from single cloud to multi-cloud is a smart venture for the organizations to achieve greater performances. This chapter discusses the transition of cloud computing from single cloud toward multi-cloud. It also drives into the benefits of using multi-cloud strategy.

References

1. Ferry, N., Rossini, A., Chauvel, F., Morin, B., & Solberg, A. (2013, June). Towards model-driven provisioning, deployment, monitoring, and adaptation of multi-cloud systems. In 2013 IEEE sixth international conference on cloud computing (pp. 887–894). IEEE.
2. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
3. Hu, F., Qiu, M., Li, J., Grant, T., Taylor, D., McCaleb, S., … Hamner, R. (2011). A review on cloud computing: Design challenges in architecture and security. *Journal of Computing and Information Technology, 19*(1), 25–55.
4. Dillon, T., Wu, C., & Chang, E. (2010, April). Cloud computing: Issues and challenges. In 2010 24th IEEE international conference on advanced information networking and applications (pp. 27–33). IEEE.
5. Hong, J., Dreibholz, T., Schenkel, J. A., & Hu, J. A. (2019, March). An overview of multi-cloud computing. In *Workshops of the international conference on advanced information networking and applications* (pp. 1055–1068). Springer.
6. Bohli, J. M., Gruschka, N., Jensen, M., Iacono, L. L., & Marnau, N. (2013). Security and privacy-enhancing multicloud architectures. *IEEE Transactions on Dependable and Secure Computing, 10*(4), 212–224.
7. Singh, Y., Kandah, F., & Zhang, W. (2011, April). A secured cost-effective multi-cloud storage in cloud computing. In 2011 IEEE conference on computer communications workshops (INFOCOM WKSHPS) (pp. 619–624). IEEE.
8. Liu, W. (2012, April). Research on cloud computing security problem and strategy. In 2012 2nd international conference on consumer electronics, communications and networks (CECNet) (pp. 1216–1219). IEEE.
9. AlZain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012, January). Cloud computing security: From single to multi-clouds. In 2012 45th Hawaii international conference on system sciences (pp. 5490–5499). IEEE.
10. Sokol, A. W., & Hogan, M. D. (2013). NIST cloud computing standards roadmap.
11. Petcu, D. (2013, April). Multi-cloud: Expectations and current approaches. In Proceedings of the 2013 international workshop on Multi-cloud applications and federated clouds (pp. 1–6).
12. 6 Multi-Cloud Architecture Designs for an Effective Cloud Strategy. *sim*. https://www.sim-form.com/multi-cloud-architecture/.
13. Akinrolabu, O., New, S., & Martin, A. (2019, June). Assessing the security risks of multicloud saas applications: A real-world case study. In 2019 6th IEEE international conference on cyber security and cloud computing (CSCloud)/2019 5th IEEE international conference on edge computing and scalable cloud (EdgeCom) (pp. 81–88). IEEE.
14. Pawar, P. S., Sajjad, A., Dimitrakos, T., & Chadwick, D. W. (2015, May). Security-as-a-service in multi-cloud and federated cloud environments. In *IFIP international conference on trust management* (pp. 251–261). Springer.
15. Bernstein, D., Ludvigson, E., Sankar, K., Diamond, S., & Morrow, M. (2009, May). Blueprint for the intercloud-protocols and formats for cloud computing interoperability. In 2009 fourth international conference on internet and web applications and services (pp. 328–336). IEEE.
16. Celesti, A., Tusa, F., Villari, M., & Puliafito, A. (2010, July). How to enhance cloud architectures to enable cross-federation. In 2010 IEEE 3rd international conference on cloud computing (pp. 337–345). IEEE.
17. Singhal, M., Chandrasekhar, S., Ge, T., Sandhu, R., Krishnan, R., Ahn, G. J., & Bertino, E. (2013). Collaboration in multicloud computing environments: Framework and security issues. *Computer, 46*(2), 76–84.
18. Yao, J., & Jiang, X. (2020, March). Research on multi cloud dynamic secure storage technology. In 2020 International conference on computer engineering and application (ICCEA) (pp. 72–78). IEEE.
19. 8 Best Practices for Multi-Cloud Security. https://blog.checkpoint.com/2019/12/20/8-best-practices-for-multi-cloud-security/.