Hindawi
Applied Computational Intelligence and Soft Computing
Volume 2021, Article ID 1843671, 16 pages
https://doi.org/10.1155/2021/1843671

Review Article

A Review of Evolutionary Trends in Cloud Computing and Applications to the Healthcare Ecosystem

Mbasa Joaquim Molo,[1,2,3] **Joke A. Badejo**,[1,2] **Emmanuel Adetiba**,[1,2,4] **Vingi Patrick Nzanzu**,[1,2,3] **Etinosa Noma-Osaghae**,[1] **Victoria Oguntosin**,[1] **Mushage Olivier Baraka**,[3] **Claude Takenga**,[3,5] **Sadeeq Suraju**,[2] **and Ezekiel F. Adebiyi**[2]

[1]*Department of Electrical and Information Engineering, Covenant University, Ota, Ogun State, Nigeria*
[2]*Covenant Applied Informatics and Communication African Center of Excellence, Covenant University, Ota, Ogun State, Nigeria*
[3]*Génie Electrique et Informatique, Université Libre des Pays des Grands Lacs, BP 360 Goma, Goma, Democratic Republic of the Congo*
[4]*HRA, Institute for Systems Science, Durban University of Technology, P.O. Box 1334, Durban, South Africa*
[5]*Infokom GmbH, Entreprise NTIC, Neubrandenburg, Germany*

Correspondence should be addressed to Emmanuel Adetiba; emmanuel.adetiba@covenantuniversity.edu.ng

Received 16 April 2021; Revised 2 July 2021; Accepted 25 August 2021; Published 20 September 2021

Academic Editor: Aniello Minutolo

Cloud computing is a technology that allows dynamic and flexible computing capability and storage through on-demand delivery and pay-as-you-go services over the Internet. This technology has brought significant advances in the Information Technology (IT) domain. In the last few years, the evolution of cloud computing has led to the development of new technologies such as cloud federation, edge computing, and fog computing. However, with the development of Internet of Things (IoT), several challenges have emerged with these new technologies. Therefore, this paper discusses each of the emerging cloud-based technologies, as well as their architectures, opportunities, and challenges. We present how cloud computing evolved from one paradigm to another through the interplay of benefits such as improvement in computational resources through the combination of the strengths of various Cloud Service Providers (CSPs), decrease in latency, improvement in bandwidth, and so on. Furthermore, the paper highlights the application of different cloud paradigms in the healthcare ecosystem.

1. Introduction

Cloud computing has made the dream of scalable computational resources real and is now on the verge of being considered in several usage models. The IT domain recognizes cloud computing as an emerging technology because it finds application in all disciplines. The prominent roles of cloud computing include hosting and delivering diverse software and services using the Internet [1, 2]. Cloud computing is a critical infrastructure for many organizations. After more than ten years of development, cloud computing has achieved great success and has significantly modified the history of the economy, society, industries, and science. With the fast development of mobile Internet and big data technology, most online services and data services are built on top of cloud computing. Thus, cloud computing has found applications in business, education, marketing, and medical and research fields [3].

Rather than providing a product via the Internet, cloud computing also provides IT solutions as a service. More than $1 trillion has been invested in cloud computing systems actively or passively. Leading CSPs such as Amazon, Microsoft, Salesforce, and Google are in intense competition [4] in terms of number of clients, reliability, and innovative service delivery.

With its unique properties such as rapid elasticity, on-demand self-service, and resource pooling, the cloud allows clients to rent online IT resources, platforms, and software services when necessary. Thus, cloud customers can integrate

their business applications on a pay-per-use basis, store data, and process and run analytics through the Internet [5].

Besides cloud computing technology, another paradigm has emerged by allowing a single CSP to grow beyond capacity. Due to the tremendous demand for online businesses requests, a single CSP can be overwhelmed so that its computing capacity becomes inadequate to fulfil the customer's requirement. This issue has led CSPs to put their resources together based on Service Level Agreement (SLA) to ensure that the Quality of Service (QoS) meets customer's requirement. An architecture called "Cloud Federation or Inter Cloud or Federated Cloud" is advantageous in terms of interoperability and financial benefits for both the customer who needs computational resources and the CSPs that, apart from having extra resources, need to keep their customers [6].

IoT devices generate and deliver a massive amount of data for analysis and decision-making. Applications such as remote surgery and smart cities require minimal response time. Therefore, it has become critical to bring computing power to the edge of the network. Both edge and fog computing efficiently help to obtain a certain satisfaction in terms of quality of service (in IoT applications that demand low latency), high bandwidth, and mobility service that a cloud environment itself cannot offer due to its centralized nature [7–9].

This paper reviews evolutionary trends in cloud computing (beginning from federated cloud through edge computing and finally to fog computing) by developing and describing the primary concept around each technology and the revolution that each technology has brought to the IT domain. We also discuss the novelty in each technology application and present the opportunities and challenges of these technologies to guide research in the healthcare ecosystem. This is not to downplay the relevance of cloud computing in other application domains such as self-driving cars, autonomous air vehicles, nuclear power plant control, and air traffic management [10].

Safety-critical systems are present in medical applications and devices such as heart-lung machines, mechanical ventilation systems, radiation therapy machines, and robotics surgery machines. All of these machines must meet stringent requirements [11]. In addition, other safety-critical systems are exhibited in other healthcare-related technological areas such as fire alarm and life support systems. These systems use either the cloud or one of its related aforementioned technologies to process the large amount of data generated by various IoT sensors.

The contribution of this review is the provision of good understanding of the evolutionary trends in cloud computing by illustrating each technology using the healthcare ecosystem as a case study. An overview of the different evolutionary trends with specific focus on the health industry, including the drawbacks and opportunities available in each paradigm, is fully presented in this work.

2. Related Works

There have been substantial contributions in terms of literature survey of emerging trends of cloud computing. This section presents related works in literature survey of cloud computing vis-à-vis their limitations.

A detailed fog computing architecture together with its levels and a survey of the various computing paradigms and features are discussed in [12]. The paper presents an in-depth analysis of fog computing and a systematic analysis of the challenges of fog computing in relation to IoT. However, this work presents neither the application of fog computing to show the opportunities it brings to the IT domain nor the application of the related paradigm that may lead the end-users to opt for fog computing in various fields.

In [13], the authors present the architecture, characteristics, challenges, and need of fog computing. However, it does not relate fog computing to other cloud paradigms to show how the technology fits into user requirements as against the other paradigms. This work also does not present the application of fog computing in various domains.

The benefits, problems, and drawbacks of edge-to-cloud computing are discussed in [14]. It also looked at edge architecture and other applications suitable for current and future edge and cloud computing opportunities. However, the work does not consider the overall trends of cloud computing as a whole. Consequently, no information on the opportunities and challenges of the emerging trends of cloud computing was presented in the work.

A review of IoT technology and its impact on big data, followed by a demonstration of how fog computing, as a new approach, may aid IoT expansion was undertaken in [15]. The paper presented the integration of big data with IoT in various applications and the advantages and drawbacks of fog computing.

The authors in [16] proposed a taxonomy of tangible indicators for evaluating cloud, fog, and edge computing performance. The authors conducted a literature review to identify common indicators and applications. The open challenges these paradigms bring in the evolution were discussed. Unfortunately, this paper did not present the utility of the emerging trend as an incredible tool that brings tremendous opportunities to the IT domain.

Thus, to address some of the highlighted gaps in the foregoing works, the study at hand provides a comprehensive survey of the emerging trends of cloud computing with specific emphasis on the healthcare ecosystem, which is a safety-critical domain. Safety-critical systems are systems where time delay, security breach, lack of computational resources or resource availability, and so forth can lead to catastrophe. The drawbacks and opportunities of these safety-critical systems as applied to the trends in cloud computing are also discussed. We also highlight the open challenges from both the end-users and CSPs perspectives in order to guide future research in the field.

3. Cloud Computing Overview

This section presents, in general, the cloud computing paradigm and its architecture and illustrates its utilization in healthcare.

3.1. Cloud Computing Architecture. Cloud computing as an on-demand delivery and pay-as-you-go technology provides scalable, flexible, and manageable resources by virtualizing

existing resources [17–20]. Cloud computing is composed of different deployment models that declare how customers access cloud services. These models are Private Cloud, Public Cloud, Hybrid Cloud, and Community Cloud. Criteria such as ownership, scale of the system, regulation of the infrastructure, and where the infrastructure resides distinguish the implementation of each model [21–24].

After establishing the cloud, its services are deployed in business models that may vary depending on the user's specifications. The cloud service model is mainly divided into three types, namely, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) [25–27].

Cloud computing is also called the "Layered Computing Model" [28]. Its architecture can be spliced into two components, which are front end and back end. The front end represents what the end-users see, while the back end describes what the end-users cannot see, which is otherwise called the cloud section of the system [29]. On the other hand, the architecture of cloud computing can be divided into four different layers, which are the (i) hardware layer, (ii) infrastructure layer, (iii) platform layer, and (iv) application layer, as shown in Figure 1. These four layers are hereafter described:

(1) Hardware layer: it is also referred to as "server or physical layer." The hardware layer is responsible for handling all physical resources such as servers, switches, routers, and cooling system, which are implemented in a data center. This layer is the lowest layer of the infrastructure, where servers are interconnected through switches and routers [21, 30, 31].

(2) Infrastructure layer: it is also known as the "virtualization layer." This layer allows full access and control of infrastructure responsible for setting up active directory and protocols. The infrastructure layer is an essential part of cloud computing because it provides virtualization of the physical resources. This layer also consists of multiple sublayers such as virtual network, virtual storage, and Virtual Machine (VM). This layer pools storage and computational resources to deliver services according to users or business requirements. Also, it necessitates a thorough understanding of load balancing as well as all other hardware virtualization concepts [21, 30, 31].

(3) Platform layer: it provides the Application Programming Interface (API) for the implementation of application frameworks. This layer offers API support for implementing database, storage, and business logic of web applications, for example, Google App Engine (Python framework). The platform layer comprises an operating system and application framework [21, 30, 31].

(4) Application layer: the functionality of this layer is accessible via the Internet to deliver services such as Gmail and Zoom. It is the most utilized and most important layer because it is close to the end-users of cloud computing [30, 31].

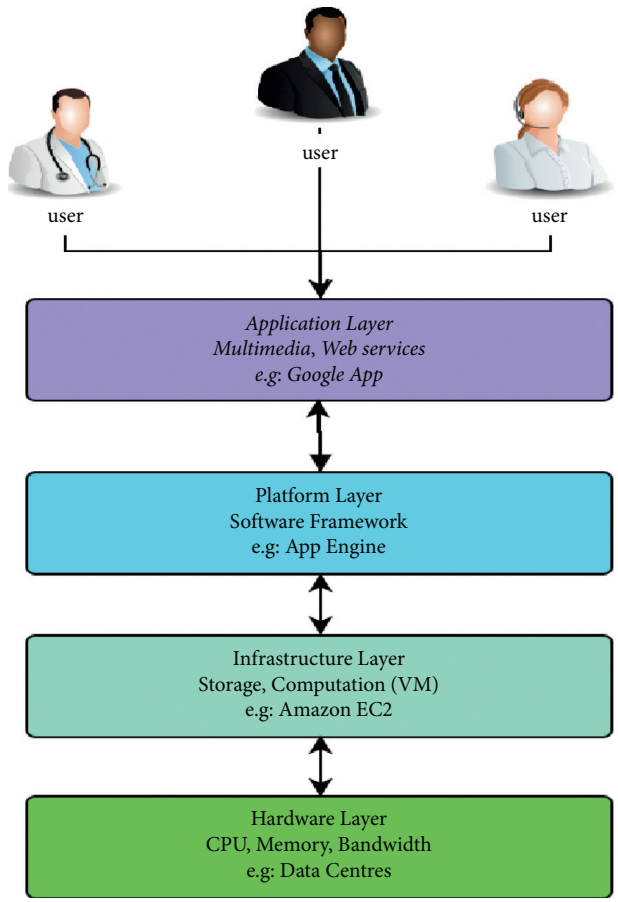

Figure 1: Cloud computing architecture and examples of different service providers.

3.2. Applications of Cloud Computing in Healthcare. In healthcare, wearable sensors are used to collect a considerable number of vital signs that monitor and diagnose illness using biological data from patients. These biological data can be used in diagnosis, interpretation, and proactive action in several scenarios through early prescription of medicine to patients. For instance, regularly evaluating glucose levels or heart rate after a clinical surgery is critical in assessing the recovery status of patients, particularly elderly patients [32].

Several works have been done in wearable health monitoring. For instance, the authors in [33] discuss the design of a Cloud-Based Intelligent Health Care Service (CBIHCS) that does real-time monitoring of blood glucose, weight, and heart rate for diagnosing chronic illnesses such as diabetes. In the work, fundamental body signs are collected with the help of body sensors and the collected data is sent and stored in the cloud to perform analysis and classification. In [34], the authors established a solid and proprietary privacy security system named Privacy-Preserving Disease Prediction (PPDP). Patient health records are encrypted in PPDP and uploaded to a cloud server. The risk of having a disease, which is based on AI prediction algorithms, was then reported for new clinical knowledge. A prediction of heart disease in cloud environment was provided in [35]. Attempts were made by the authors to propose

a suitable model based on patient information in order to help physicians predict heart disease. The paper presented different results of various models that were implemented with the heart disease dataset. The result revealed that the Naïve Bayes model provided the highest accuracy of 86.42% followed by the AdaBoost and boosted tree. Furthermore, the three models were combined to give an enhanced accuracy of up to 87.91%. The experiment was conducted on a cloud environment using 10,082 instances, which produced an overall effect of significantly reducing the execution time with a maximum accuracy.

The design and deployment of a genomic cloud were undertaken in [36] to enhance the computing capability and storage and provide more flexibility and easy analysis through the use of genomics software. The implementation of the genomic cloud infrastructure is based on multiple technologies, which includes Common Workflow Language/Workflow Description Language (CWL/WDL), Docker, Network Attached Storage (NAS), Database Availability Group (DAG), and Object Storage System (OSS). The developed cloud infrastructure also assists the user in generating high-performance clusters, managing tremendous genomic data files, and scripting genomics analysis pipelines.

3.3. Impact of the Utilization of Big Data in Cloud Computing for the Healthcare Ecosystem. Cloud computing and big data analytics in the healthcare ecosystem are two disciplines that are unexpectedly revolutionizing the field. These technologies have brought about powerful results and attractive benefits. Every second, a massive amount of healthcare data is generated, and, as such, tremendous computational resources are required to process these enormous data. Unfortunately, small and medium enterprises cannot afford the huge computational resources necessary to meet business needs [37, 38]. Nonetheless, there exist some factors that affect a cloud environment in the utilization of big data as hereafter presented [39]:

(1) Data storage: big data analytics require high-performance hardware for the analysis and storage of data. As data increase continuously, CSPs are supposed to increase the storage capacity to remain competitive.

(2) Availability and reliability: CSPs have challenges in terms of delivering the service 24/7. Monitoring the provided service is crucial and, therefore, a critical evaluation of the SLA to ensure performance is essential.

(3) Performance and bandwidth cost: increasing the bandwidth size rather than purchasing hardware equipment so that the delivery of services becomes faster will lead to spending less money on hardware. However, big data requires both increased hardware and bandwidth; therefore, delivering a large amount of data every time, regardless of the location, can be expensive.

These few factors have led researchers to introduce new paradigms for enhancing computing capability by leveraging resources that are available from other CSPs or distributed nodes. This is to ensure that computational resources are close to the location of the user so as to reduce latency and improve bandwidth utilization.

4. Cloud Computing-Related Technologies

The different cloud computing paradigms that have been introduced in the IT domain to address the problems that traditional cloud computing faces include federated cloud (or cloud federation) and fog and edge computing.

4.1. Cloud Federation. In most cases, CSPs fail to fulfil customers' requirements due to growing demands for cloud services. Therefore, relying solely on a single cloud provider can stop users from having high-quality services whenever they need to. In this case, as the workload increases, the cloud federation assists CSPs to scale up by renting resources from other providers [40].

A cloud federation is a partnership between various entities in which companies can benefit by accessing resources hosted on another cloud environment [41, 42]. Efficient use of energy and resources are two crucial differentiators in the contemporary cloud computing marketplace. Regardless of how big cloud computing providers can be, they do have a finite capacity. Therefore, a federation of cloud computing infrastructure allows growing beyond the providers' capacity. Besides, it enables collaboration and resource sharing [31]. Cloud computing is built around an advanced orchestration model, which serves as a connecting point between the available and compatible resources and users' requests. This model allows the dynamic provision of resources to satisfy both the providers' and users' requirements. Thus, a generic end-user may transparently access any potential computational resource (e.g., CPUs, storage, and network) needed by moving freely from one CSP to another [43].

4.1.1. Cloud Federation Architecture. The fundamental architecture of a federated cloud is illustrated in Figure 2. It consists of several CSPs that offer services to different clients that can access the federated resources on demand [43]. The different components of the federated cloud are described as follows:

(1) *A front-end component* is a point that allows users to access the whole platform.

(2) *Cloud service broker component* is responsible for distributing resources according to user's requirement. This component is in charge of billing and metering of the federation platform.

(3) *The resource interface component* is the point that connects all the cloud computing platforms.

(4) *The user allocation table* contains the credentials of the user and the association between users and activated service.

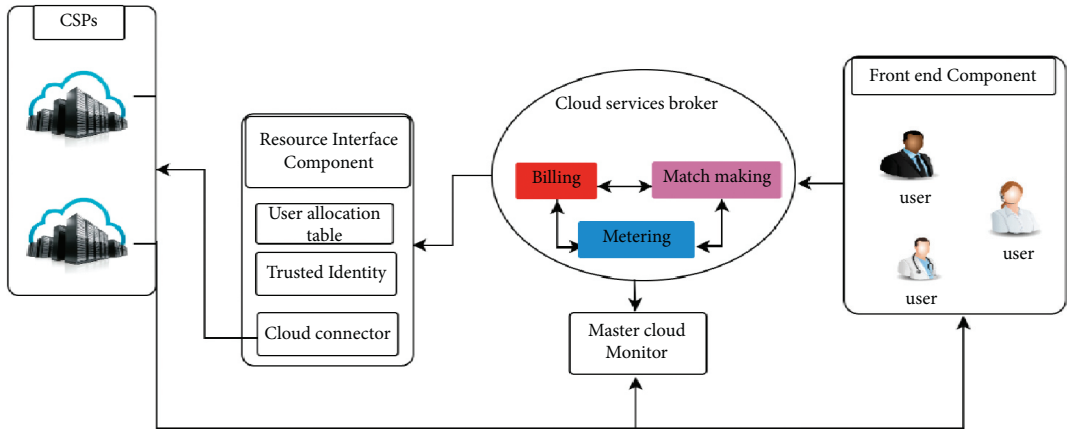

Figure 2: Architecture of a federated cloud environment.

(5) *The trusted identity component* is an interface that handles the credentials and encrypted data stored in the database, which the platform utilizes in order to authenticate the federation.

(6) *The cloud connector* is a module that works as an interface with the federation.

(7) *Master cloud monitor* is a module where cloud agents are set up in the federation to read specific metrics with greater precision than the resource interface component. The master cloud monitor (MCM) collects cloud agent relevant information to improve cloud interoperability.

The entity in charge of managing the use, performance, and delivery of cloud services is known as a cloud broker. This entity negotiates relations between cloud providers and cloud consumers. A cloud service broker can be defined as a "*cloud service partner that negotiates the relationship between Cloud Service Customers (CSUs) and Cloud Service Providers (CSPs)*." The two central cloud brokering stakeholders are CSPs and CSUs. CSUs can get economical solutions using a cloud broker, whereas CSPs can gain new ways to develop services and raise profit [44].

Accumulation, integration, and customization of cloud brokerage services play a threefold role. Accumulation involves the collection and provision of different cloud services to the end-user. Integration refers to linking the cloud service as an intermediary with the internal system. Customization involves either adjusting the cloud service in compliance with the user's requirements or the creation of the cloud application. The threefold role of the cloud services broker resolves the limitations of a single cloud service. The threefold role addresses the limitation of data loss due to dependency on a single unique cloud and platform failure. It also allows easy management of data across multiple Cloud Service Providers [45].

4.1.2. Application of Cloud Federation in Healthcare. The relevance of cloud federation in healthcare is expressed by the fact that a single cloud may not be sufficient to process the huge amount of medical data being generated every second. Therefore, sharing resource among many CSPs is a major contribution of the federated cloud in the evolution of cloud computing. For instance, in African countries where computing capability is a tremendous concern, such facilities would allow the interchange of healthcare records, permitting access to expertise that is not locally available, and enable flexibility and cost-effective execution of tasks on computing resources [46].

For instance, the authors in [46] proposed a cloud federation system for healthcare using cooperative and competitive cooperation models. The work aimed at connecting multiple medical centers throughout Africa. Simulations were conducted using two new allocation strategies to assess the efficiency of the models using Genetic Algorithm-Based VM Allocation (GAVA) and Secure Roommate Allocation (SRA). In [47], the authors developed a Software-as-a-Service (SaaS) by leveraging the intrinsic security function of the Blockchain technology. This allowed a medical cloud to create a federation with others in order to coordinate a virtual healthcare team involving doctors from various federated hospitals who collaborate to conduct a healthcare workflow. Reference [48] proposed a cloud federation framework that allows the sharing of healthcare and medical resources among different CSPs with the ease of timely access that guarantees integrity and privacy of data. The approach used was validated by conducting a series of evaluation studies with the help of CloudSim toolkit.

4.2. Edge Computing. Internet-enabled applications such as virtual reality, surveillance, augmented reality, and real-time traffic monitoring require quick processing and rapid response time. End-users usually run such applications on their resource-limited mobile devices in most cases. However, the core operations and processing are carried out on cloud servers by moving the processing to the network's edge. Edge computing has proved to meet the mobile application requirement of fast response times [49]. The European Telecommunications Standards Institute (ETSI) described mobile edge computing as a technology that provides an environment for Internet services and cloud computing on the edge of networks, near radio access networks, and mobile users.

This model significantly reduces the delay in transmission and network burden and increases the density of nodes and the mobility support to bring the processing capability close to the user [49, 50]. Edge computing is a modern model for processing of part of the data at the network edge. There is controversy among researchers regarding the meaning and position of the edge. Some view "edge" as IoT-connected devices with limited resources that process the information gathered. Other researchers see "edge" as a concept that transfers data processing to the source [9]. For many scholars, edge computing collects devices, equipment, and network resources that produce, gather, and send data to remote cloud centers [51]. Different authors provide definitions of edge computing from various perspectives in terms of architecture, technology, capability, or characteristics, as shown in Table 1.

4.2.1. Main Differences between Cloud Computing and Edge Computing. Unlike the cloud computing paradigm, edge computing provides local and decentralized infrastructural services while taking the required resources closer to data sources and avoids data transfer requirements to a centralized node. Moreover, edge computing has the advantage of delivering real-time responses with very low latency, handling privacy issues, reducing data communication, improving bandwidth utilization, and reducing energy consumption [58]. Cloud computing has high latency, presents a slow response time, and has no offline mode. At the same time, cloud computing is scalable, processes big data, and has unlimited computational processing abilities. In contrast, edge computing is storage-limited, requires interconnection through proprietary networks, and is highly power-consuming [50, 51, 59, 60]. Moreover, edge computing can be combined with cloud computing to enhance the efficiency of both approaches yielding a hybrid edge-cloud computing model [58].

4.2.2. Architecture of an Edge Computing Platform. The basic structure on which an edge computing platform is built is summarized into three major parts, as shown in Figure 3. These components are hereafter explained:

Edge devices: these are on-premise edge equipment that gathers information or communicates with edge data, including video cameras, sensors, and other electronic components. Primary edge devices can gather data, transmit data, or both. Edge devices that are much more sophisticated have more computer capacity, enabling them to perform more operations. The ability to deploy and maintain applications on these edge network devices is vital.

(1) Edge node: the edge network layer and edge servers can be real or virtual servers located in different remote sites or merged in hyperconverged infrastructure. This layer of the edge computing architecture is divided into two sublayers: the edge server, which helps to store and perform small computation needs, and the edge data center that is responsible for delivering a portion of intensive data processing close to the user's location. The edge data center is usually connected to a more significant cloud data center that offers more storage capability and computational power.

(2) The cloud: this can run on premise or in a remote public cloud. It handles the processing that is not possible at other edge layers.

4.2.3. Applications of Edge Computing in Healthcare. As mentioned earlier, the significant difference between cloud computing and edge computing resides in how and where data processing is involved. With cloud computing, the data is processed and stored in a centralized location, while with edge computing, the data is processed close to the source. Processing data near the source brings another connotation regarding response time, bandwidth, and real-time interaction. As technological development advances, the healthcare system needs specialized equipment that enables fast analysis and data processing, better security, cost-effectiveness, and so forth. Combined with IoT system, edge computing has brought a severe revolution in the healthcare ecosystem. For example, [61] used cognitive computing to monitor and examine users' physical health. It also changes the computational allocation of resources of the entire edge computing network in accordance with each user's health-risk level. The study shows that the edge cognitive computing-based healthcare system enhances customer experience, effectively allocates computational resources, and dramatically increases patient survival rates in emergency situations. The study in [62] introduced LiveMicro, a platform which provides the benefits of enabling edge computing-driven digital pathology computations, such as image processing on a live capture of a microscope and allowing remote pathologists to diagnose in real time in a single virtual microscope session. This allows for continuous medical education and remote consultation, which is vital in underserved and remote hospitals and private practices. The work in [63] proposes a healthcare system architecture for monitoring to allow remote communication with optimal bandwidth and short response time for a fast decision-making process for preliminary diagnosis in a virtual environment. The proposed system enables the filtering and compression of a patient's record with a functional algorithm. An open-source and low-cost approach to assist the triage in the emergency department is presented in [63]. The main objective of the study is the COVID-19 prescreening, fever, and cyanosis noncontact detection.

4.3. Fog Computing. A new paradigm called fog computing emerged in 2014. The paradigm of fog computing offers improvement in the usage of resources. It also suggests an improvement in terms of reducing the latency for latency-critical applications [64].

Cloud computing's centralized design prompted researchers to establish a distributed technology as a cloud computing extension, which is similar to providing consumers with services offered by cloud computing technology. Fog

Table 1: Definitions of edge computing.

Definitions	Authors
Edge computing is a method of delivering intelligent services at the network edge by combining the key technologies of networks, processing, storage, and applications. This technique facilitates meeting the critical criteria of the digital business for agile connectivity, security, data optimization, real-time services, and privacy protection close to the location of devices.	[52]
Edge computing consists of techniques that enable computation at the network's edge, close to the source of production of the information. In edge computing, the node not only gathers information but also generates it.	[53]
Edge computing is a recent trend of cloud computing wherein major storage and computational resources, alternatively termed as cloudlets, micro data centers, are located close to the end devices or sensors at the network edge.	[54]
Edge computing is a technology that performs computations near the source of information rather than sending them to a centralized processing system to capitalize in terms of speed, transmission time, and effectiveness.	[55]
Edge computing helps eliminate the necessity for centralized data processing by bringing the device's computational capability close to the source of information. This allows fast data transport and improves the effectiveness of the computing process.	[56]
Edge computing is a new processing paradigm that brings computing power and storage to the network's edge. It provides advanced analysis combined with cloud services.	[57]

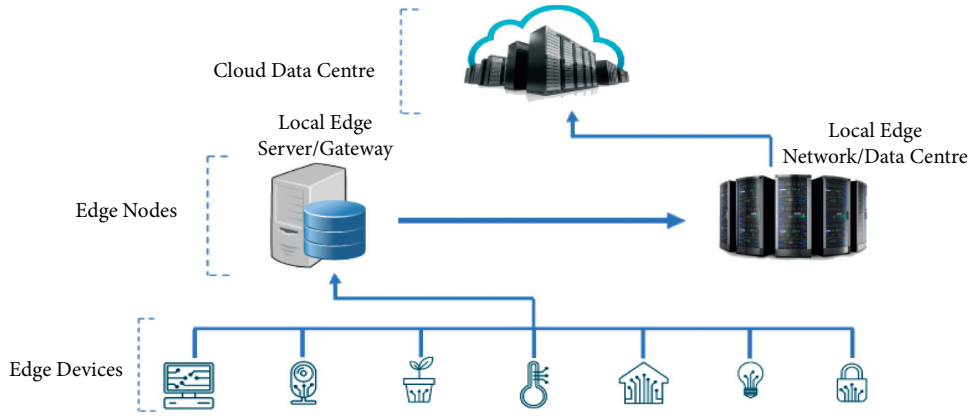

Figure 3: Structure of edge computing (each of these nodes is critical to the overall structure of edge computing).

computing helps to bring the computational resources closer to the source of the generated data. Fog computing allows storage, computing, and networking services between traditional cloud computing data centers and devices [65].

Due to the extreme limitations on the computing resources of IoT devices, it is common to discharge tasks requiring substantial computational resources to computer systems with sufficient computing resources such as High-Performance Computing (HPC), cloud systems, or data centers for processing [66, 67].

While massive data centers are typically used in cloud computing, fog computing uses small servers, routers, switches, set-top boxes, gateways, or access points since fog computing systems consume less space compared to cloud computing systems, thereby locating hardware closer to users [68]. Fog computing provides a significant improvement in cloud protection, efficiency, and accessibility by providing a robust and distributed communication system with a short delay of about 10 ms and high throughput in the order of 10 Gbps. Therefore, the fog computing environment complements cloud computing by allowing computing to be deployed immediately at the network's edge. Also, QoS is a fundamental fog service metric that should be considered in four aspects of delivering the fog services, which are connectivity, reliability, capacity, and delay [69, 70].

Hence, fog computing is a model that enables low latency computing, where fog nodes provide partial validation of transaction which does not require considerable computational resources and cloud servers provide the final transaction validation when there is a need for substantial computing capability. This allows overcoming processing capability issues of IoT devices and helps in having short response time to ensure QoS [71].

4.3.1. Architecture of Fog Computing Platform. Fog computing architecture, as illustrated in Figure 4, is composed of three layers, namely, (i) IoT or user layer, (ii) fog layer, and (iii) the cloud layer [72], described as follows:

(1) *The IoT layer* incorporates a large number of heterogeneous and omnipresent devices that produce physical world information. It is a worldwide network of affiliated entities based on shared communication protocols [73].

(2) *The fog layer* is placed between the IoT layer and the cloud layer. The core service node in this architecture is the fog node. The fog layer consists of many elements, namely, gateway, routers, network edge server, access points, and other devices. This layer can process, transmit, and store data temporarily [74].

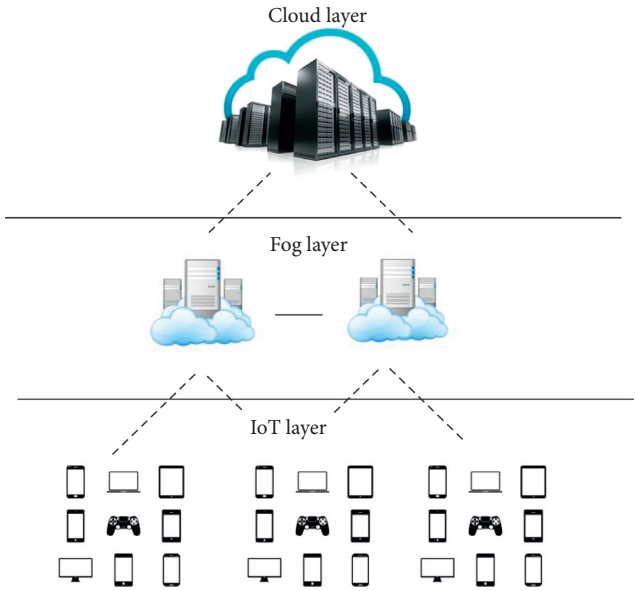

Figure 4: Fog computing architecture.

(3) *The cloud computing layer* offers the possibility of processing a large amount of data and gives a wide range of services.

Fog nodes are placed nearest to IoT units, ingesting data from them. Then, the fog node routes the collected data to the most suitable location for data processing. The fog node then collects, processes, analyzes, and stores the most sensitive data. Moreover, any indication of issues relating to faults can be detected by the sensors at the closest fog node and response time can be sent to the actuator. The fog node must support both the integration and environment of IoT devices with the cloud. To effectively handle IoT resources, a computing model that can help both ends, IoT and cloud, is needed. Furthermore, with the appearance of the sixth generation of wireless communication (6G), resource management in fog computing would be easier due to the larger communication channel it offers [75]. Therefore, fog computing is characterized by several factors specific to it such as low latency, real-time analysis, bandwidth conservation, high level of security, geographic distribution, proximity to users, business agility, overall service management, and redundancy [13].

4.3.2. Application of Fog Computing in Healthcare. In [76], the authors designed a system that involves a series of software modules that enable a phobia patient to engage in a therapy session with a remote specialist therapist. The victim and the therapist share the same virtual reality environment. The fog paradigm was used to satisfy the stringent Tactile Internet specifications, such as a 1 ms round trip latency. The architecture uses high-level interfaces for communicating with external software applications and a broad range of hardware devices. The work in [77] presents an automated technological analysis for telesurgery which was based on 5G, IoT, Tactile Internet, and Artificial Intelligence (AI). A fog assisted interactive model is used to reduce latency during the process. Furthermore, in the study in [78], the authors performed the assessment of a prototype that gathered the patient's electrocardiogram traces and utilized the user's smart device as the fog layer to safely share his data with certified parties. This allowed patients to share information with doctors.

5. Opportunities and Challenges in Cloud Computing

This section gives first the obstacles and opportunities in cloud computing, presents the challenges of each technology of the evolution of the cloud, and gives the challenges of the evolutionary trend in general.

5.1. Obstacle and Opportunities for Cloud Computing Development. The cloud computing field gives the IT industry tremendous opportunities. It offers an opportunity to innovate businesses and transform them into a more reliable and flexible business service. Cloud computing is at an early stage in many organizations [79].

Some opportunities that this technology provides are summarized in Table 2.

Cloud computing reflects a tremendous transition in ICT and aims to offer immense benefits to many organizations and businesses. Cloud infrastructure aims to significantly reduce ICT running costs [80, 81]. It also promises to deliver scalability [82], reliability and availability [83], agility [84], and flexibility [85]. Besides, it promises to offer many other advantages to businesses to enable organizations to concentrate on business processes while leaving the IT business to the cloud provider. However, while cloud infrastructure has several advantages, many problems need to be tackled as a feasible ICT solution, especially in developing countries. According to [86], in general, cloud-based issues have been divided into six main categories, namely, data management and allocation of resources, security and privacy, load balancing, scalability and availability, server migration and compatibility, and interoperability and communication between clouds. Each of these problems has influenced the reliability and performance of their principles in cloud-based environments. In summary, the main challenges in cloud computing are provided in Table 3.

5.2. Challenges in Cloud Federation. A federated cloud computing system is a dynamic distributed system consisting of pooled computational resources. The unexpected user requests and the consequences of external events that are beyond user and system administrator control may cause several challenges, such as the following:

(1) Reliability and interoperability: since a cloud federation is a partnership between several CSPs [94], the heterogeneity of the entire federation may affect its performance. Ensuring the compatibility of the shared resources within the federation and avoiding any type of anomaly so that user's request will be

Table 2: Obstacle and opportunities for cloud computing development.

SN	Obstacles	Opportunities
1	Availability/business continuity/ interoperability/scalable storage	Use multiple cloud providers to ensure that user's requirements are met by providing federated computational resources and storage
2	Data confidentiality and auditability	Deploy encryption, VLANs, firewalls
3	Performance unpredictability	Improve VM support, flash memory, gang schedule VMs
4	Bugs in large distributed system	Invent debugger that relies on distributed VMs
5	Scaling quickly	Invent autoscaler that relies on machine learning; snapshots for conservation
6	Reputation fate sharing	Offer reputation-guarding services like those for e-mail
7	Software licensing	Pay-for-use licenses

Table 3: Cloud computing challenges.

Challenge	Description	Reference
Security concern	The reliable third party offers several cloud services and faces new security risks. The cloud supplier provides its services over the Internet and uses several web technologies, which generate new security problems.	[87, 88]
Regulations issues	Lack of benchmarks and relevant patterns makes compliance more complicated than it should be.	[89, 90]
Reliability	Lack of reliability and high cloud service availability is becoming a big problem. Research has shown that about $285 million have been lost yearly due to cloud service failure.	[83]
Loss of control	Control loss occurs when CSPs are unable to offer full authority to customers in handling their resources. Due to the absence of authentication and access protection, loss control exposes the cloud computing security concerns.	[91]
Privacy concern	Data protection for some organizations and individuals is a critical feature of their business. Indeed, their confidential data (health, finance, personal knowledge, etc.) plays a significant role in their companies.	[92]
Data flow management	Considering the huge stream of data being generated by CSPs and IoT devices continuously, the cloud computing capability becomes simply unable to process such data, which in turn alters the quality of service.	[93]

efficiently treated regardless of the technology that CSPs use is a very challenging task [95]. The need for automated ways of detecting anomalies in the federation is critical to avoid the SLA violation among CSPs and also between CSPs and users. Thus, the detection of an anomaly in an automated way would be helpful for disaster management.

(2) Resource pricing: customers and providers of cloud resources are rational and willing to increase their interest as much as possible while consuming and sharing resources. Since the user's requests are handled within the federation, the pricing mechanism is then used to control the individual rationality of customers and suppliers. Therefore, the need for dynamic pricing strategies is crucial [96].

(3) Load balancing: it is usual to have more than one provider to process the user request in the federated cloud environment. In such situations, the strategy needed to allocate the user request equally between CSPs using load balancing methods becomes complicated for sharing the workload transparently [97].

5.3. Challenges in Edge Computing. Several technological challenges have resulted from the complexities of edge computing, such as reliability, mobility management, heterogeneity, security and privacy, scalability, and resource management. Also, edge computing faces other significant open challenges, such as the following:

(1) User trust in edge computing systems: the success of all innovations is positively related to its acceptance by customers. Trust is considered as one of the significant factors in the endorsement and adoption by users of edge systems. As customer confidence is closely related to the protection and privacy of technology, if the user's data are not adequately handled, the consumer trust will certainly be broken down. Therefore, the technical advantage of these systems/technologies is not accepted. Therefore, research efforts to build customer confidence models for edge computing systems must be undertaken [98].

(2) Agile and dynamic pricing models: a challenging task is developing dynamic and agile pricing models, as one pricing model may not be successful for multiple consumer interactions. With best-fit pricing models that can offer mutual gains for service providers and consumers, heterogeneous edge computing systems are also difficult to include. However, for the development of dynamic pricing models for edge computing systems, the pricing model for cloud services such as "pay-as-you-go" may be utilized [99].

(3) Discovery, delivery of service, and mobility: service discovery in distributed edge computing systems is challenging considering the rising number of mobile devices that need services simultaneously and uninterruptedly. Since the delay involves identifying

and choosing the other available facilities and resources, this task becomes more difficult. In heterogeneous edge computing systems, the automated and user-transparent discovery of suitable edge computing nodes according to necessary resources also presents a challenging task for service discovery mechanisms. However, applications for peer-to-peer networks may be proposed to contribute to the design and creation of efficient user-transparent solutions for edge computing systems [100].

(4) Cooperation among disparate edge computing systems: the edge computing system comprises various heterogeneous technologies that serve to achieve the communication of information. The heterogeneous aspect of edge computing infrastructure enables this technology to access different edge devices using other wireless mechanisms. Synchronization, data confidentiality, load balancing, and interoperability are also part of challenges in the edge computing environment due to its heterogeneous nature [101].

(5) Low-cost fault tolerance deployment models: edge computing is built based on a mechanism that enables high availability, efficient disaster management, fault tolerance, and so forth. However, the issue with this technology is that building a low-cost fault tolerance mechanism is extremely difficult [49].

5.4. Challenges in Fog Computing. There are some open research problems in fog computing. However, many of the challenges in fog computing are similar to those faced by edge computing. Its relationship with edge computing is because fog computing is an implementation of edge computing [102]. Heterogeneity, QoS management, scalability, versatility, federation, and interoperability are the most pressing problems of fog computing [103].

Because of its location at the edge of the Internet, the fog network is heterogeneous. The fog network is responsible for linking each part of the fog. However, network management, maintaining connectivity, and delivering services, particularly in large-scale IoT scenarios, become more complicated [69, 70]. The challenges of fog computing are listed as follows:

(1) Mobility: in several domains such as healthcare, smart cities, and the Internet of Vehicles (IoV), the fog nodes are primarily mobile and make data management in terms of data storage, data resource provisioning, resource availability, and service migration a lot more challenging [68].

(2) Security: data privacy-preserving and data protection are two critical challenges for data management because of the mobile nature of nodes in fog computing. Therefore, data collection, data sharing, data replication, data offloading, and data aggregation become more complex. Also, authentication and data access control are complicated to manage in unsecured fog nodes [104].

(3) Distributed processing: efficient local processing on mobile or static nodes is a critical concern in distributed data processing. Since distinct behaviour and responses can be described for various situations, identifying data contexts in fog nodes in order to solve problems correctly under the right conditions is another problem [105].

(4) Storage and computational resources: complex data analysis or long-term data storage is difficult to achieve on fog devices due to storage and computing resource limitations [106].

5.5. Summary of the Gaps Identified in Each Technology. Table 4 gives an overview of the challenges encountered in cloud computing and its related technology.

5.6. Challenges of the Evolutionary Trend of Cloud Computing. Some quality attributes such as power consumption, latency, privacy, fault tolerance, and sharing of resources have been taken into account in assessing the performance of the evolutionary technologies of cloud computing [107]. Some other quality attributes such as the heterogeneous nature of the cloud paradigm might influence decision-making in identifying the critical quality attributes and corresponding metrics to quantify the importance of choosing a specific cloud paradigm [108]. The heterogeneous nature of the cloud paradigm adds complexity to decision-making regarding where to implement one of these technologies among all possible combinations. This requires a thorough analysis of various aspects that can influence the SLA [16]. Most literature only focus on quality attributes that are easily measurable; however, some other parameters to consider may appear to be relevant.

As has been mentioned in the literature, cloud computing paradigm is heterogeneous environment; moreover, compatibility, portability, and maintainability seem to be quality attributes that are not included in the evaluation of the performance of the different cloud paradigms. These new parameters are relevant because portability refers to "*the ease with which a device, product, or component can be moved from one hardware, software, or other operating system or user environment to another*." Compatibility refers to "*the ability of a device, system, or component to communicate with many other products, systems, or components*," and maintainability, which may be assessed by the modularity, refers to "*the degree to which a device, system or computer program is made up of discrete components, such that changing one does not affect the others*" [109, 110].

For overall communication in new cloud computing paradigms, sensing devices, computers, and other electronic equipment are incorporated. It involves a wide variety of geographical locations, leading to a broader risk of vulnerability. The process of authorizing and authenticating a large number of nodes is complex. Strategies that can dynamically assess the security of different nodes are needed [13].

The tremendous augmentation of data may cause disasters that cannot be unearthed at a small scale. This phenomenon

Table 4: The challenges and opportunities of cloud computing-related technologies.

SN	Related cloud technology	Challenges	Opportunity
1	Cloud computing	(i) For a single cloud, the storage and computing capability is finite. (ii) CSPs have issues in maintaining the overall structure, availability, and reliability 24/7. The probability of the SLA violation is not negligible. (iii) High computing processes require more bandwidth and hardware. Therefore, the cost of the overall structure increases considerably.	(i) Allows the scalability, flexibility, and elasticity of computational resources. (ii) Allows an on-demand delivery and pay-as-you-go service over the Internet. (iii) Resource pooling is also available.
2	Federated cloud	(i) Reliability and interoperability cause nonnegligible issues, since the heterogeneous aspect of the federated cloud affects its performance in terms of compatibility. The disaster management in the federation also becomes complicated. (ii) The federation's pricing and load balancing process are complex because several CSPs handle users' requests. The pricing mechanism is complicated.	(i) Advancement in cloud federation allows very high scalability, flexibility, and elasticity of computational resources and storage. CSPs leverage the resources available in the federation.
3	Edge computing	(i) Privacy and protection are aspects that capture the attention of users of this technology. Due to the innovation that this technology brings, it is difficult to have a confirmed assurance that users would put their trust in edge computing technology. Users need to protect their privacy. (ii) Finding a standard in terms of pricing is difficult in such technology. The implementation of an agile and dynamic pricing model is one of the significant challenges. (iii) Discovery, delivery, and mobility are also part of the battles that edge computing technology faces. The incredible number of devices used in the edge computing environment renders resource management more and more complex.	(i) The short response time that this technology offers is its principal asset. Privacy, resiliency against cloud/network failure, and extendibility are also the characteristics of this technology.
4	Fog computing	(i) As for edge computing technology, the heterogeneity aspect and its location close to the user render fog computing technology more complex. Thus, QoS management, scalability, versatility, and interoperability are challenging to handle. Also, the management of data is problematic because of the mobile nature of mobile nodes and the distributed aspect of fog computing technology. Therefore, mobility and security concerns can be raised. (ii) Efficient data processing is complex due to limited computational resources and distributed data processing.	(i) This technology is also distinguished by its significant improvement in cloud protection, efficiency, and accessibility by offering communication with a short delay (10 ms) and high throughput (10 Gbps).

renders fault diagnosis and tolerance more challenging in the management of resources in terms of resource monitoring. It can affect the integration or implementation of the cloud computing paradigm in diverse applications where a decision must be considered in advance [13].

The cost of each new paradigm impacts the approbation of the technology in the marketplace. Nevertheless, the deployment of the new paradigm of cloud computing considers the necessary price beforehand. However, the cost of installation and configuration tools are causes of significant concern when adopting a cloud computing paradigm in a specific application [93]. Meanwhile, other technologies such as cyber-physical systems are gaining ground over a considerable range of applications and businesses. A cyber-physical system provides a controllable, credible, and scalable physical system that profoundly embeds the capability of computation, communication, and control, which is based on data acquisition from IoT. The integration of cyber-physical systems with the cloud paradigm, though presenting an increased cost, results in the realization of safety-critical systems that are more robust [111, 112].

The security aspect in the emerging paradigms can be an entire area that needs more attention. A large number of sensitive transactions are carried out within the cloud environment and can impact user trust. Distributed Denial of Service (DDoS) is the most encountered attack in the cloud environment, and there is no effective solution that helps eradicate security issues [113]. Several techniques have been

proposed to solve the security matter. For instance, [114] suggested a Blockchain-Assisted Secure Fine-Grained Searchable Encryption (BASE) for a cloud-based healthcare cyber-physical system that provides an attractive level of security but requires considerable processing power. Meanwhile, many other techniques such as Software-Defined Networking (SDN) can, in certain circumstances, help to improve the DDoS attack detection and mitigation capabilities of the cloud [115]. Therefore, deploying additional policies for security involves extra effort such as cost, development of solid encryption algorithms, high demand of computational resources, and high level of monitoring.

6. Conclusion and Future Research

Cloud computing, cloud federation, edge computing, and fog computing are key technologies that have revolutionized the history of the IT domain. These paradigms have significantly changed how people process, store, and transmit data worldwide. These have also led to research in developing technology that changes drastically with time. Therefore, this paper has presented a detailed review of all these new paradigms by particularly illustrating their contributions to the healthcare ecosystem and presenting challenges that militate against the performance of each technology generally. Also, we provided some details about the architecture and improvements that they have been brought to cloud computing. A future research direction includes a systematic review of machine-learning algorithms that help to identify anomalies in a federated healthcare cloud environment to improve its QoS, which can be altered due to its heterogeneous aspect. A comparative study of fog-edge computing and the cyber-physical system will also be explored.

Data Availability

This is a review article and no underlying data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors acknowledge the Covenant Applied Informatics and Communication Africa Centre of Excellence (CApIC-ACE) domiciled at Covenant University for funding this work with the ACE Impact grant from World Bank through the National University Commission, Nigeria. The Covenant University Center for Research, Innovation and Discovery (CUCRID), Covenant University, is also acknowledged for providing fund towards the publication of this study.

References

[1] M. Gander, M. Felderer, B. Katt, A. Tolbaru, R. Breu, and A. Moschitti, "Anomaly detection in the cloud: detecting security incidents via machine learning," *Trustworthy Eternal Systems via Evolving Software, Data and Knowledge, Communications in Computer and Information Science*, Springer-Verlag, vol. 379, pp. 103–116, Heidelberg, Germany, 2013.

[2] R. R. Patil, "Cloud computing an overview," *International Journal of Engineering and Technology*, vol. 7, no. 4, p. 2743, 2018.

[3] M. Chopra, J. Mungi, and K. Chopra, "A survey on use of cloud computing in various fields," *International Journal of Science, Engineering and Technology Research*, vol. 2, no. 2, pp. 480–488, 2013.

[4] P. K. Senyo, J. Effah, and E. Addae, "Preliminary insight into cloud computing adoption in a developing country," *Journal of Enterprise Information Management*, vol. 29, no. 4, pp. 505–524, 2016.

[5] P.-F. Hsu, S. Ray, and Y.-Y. Li-Hsieh, "Examining cloud computing adoption intention, pricing mechanism, and deployment model," *International Journal of Information Management*, vol. 34, no. 4, pp. 474–488, 2014.

[6] A. Hammoud, A. Mourad, H. Otrok, O. A. Wahab, and H. Harmanani, "Cloud federation formation using genetic and evolutionary game theoretical models," *Future Generation Computer Systems*, vol. 104, pp. 92–104, 2020.

[7] G. Li, X. Ren, J. Wu et al., "Blockchain-based mobile edge computing system," *Information Sciences*, vol. 561, pp. 70–80, 2021.

[8] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, "Fog computing for the internet of things," *ACM Transactions on Internet Technology*, vol. 19, no. 2, pp. 1–41, 2019.

[9] Y. Mansouri and M. A. Babar, "A review of edge computing: features and resource virtualization," *Journal of Parallel and Distributed Computing*, vol. 150, pp. 155–183, 2021.

[10] R. Bloomfield and J. Lala, "Safety-critical systems: the next generation," *IEEE Security & Privacy*, vol. 11, no. 4, pp. 11–13, 2013.

[11] S. Ahamad and Ratneshwer, "Some studies on performability analysis of safety critical systems," *Computer Science Review*, vol. 39, Article ID 100319, 2021.

[12] H. Sabireen and V. Neelanarayanan, "A review on fog computing: architecture, fog with IoT, algorithms and research challenges," *ICT Express*, vol. 7, no. 2, pp. 162–176, 2021.

[13] V. Dahiya and S. Dalal, "Fog computing: a review on integration of cloud computing and internet of things," in *Proceedings of the 2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, pp. 1–6, Bhopal, India, 2018.

[14] M. Y. uddin and S. Ahmad, "A review on edge to cloud: paradigm shift from large data centers to small centers of data everywhere," in *Proceedings of the 2020 International Conference on Inventive Computation Technologies (ICICT)*, pp. 318–322, Coimbatore, India, February 2020.

[15] M. E. Idrissi, O. Elbeqqali, and J. Riffi, "From cloud computing to fog computing: two technologies to serve iot-a review," in *Proceedings of the 2019 IEEE International Smart Cities Conference (ISC2)*, pp. 272–279, Casablanca, Morocco, October 2019.

[16] 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 of Things*, vol. 12, Article ID 100273, 2020.

[17] M. Armbrust, A. Fox, R. Griffith et al., "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[18] B. Hayes, "Cloud computing," *Communications of the ACM*, vol. 51, no. 7, pp. 9–11, 2008.

[19] P. Sun, "Security and privacy protection in cloud computing: discussions and challenges," *Journal of Network and Computer Applications*, vol. 160, Article ID 102642, 2020.

[20] A. Kamali, S. Mohammadi, and A. A. Barforoush, "UCC: UML profile to cloud computing modeling: using stereotypes and tag values," in *Proceedings of the 7'th International Symposium on Telecommunications (IST'2014)*, Tehran, Iran, 2014.

[21] S. Joshi and U. Kumari, "Cloud computing: architecture & challenges," *Mody University International Journal of Computing and Engineering Research*, vol. 1, no. 1, p. 6, 2019.

[22] A. Heydari, M. Ali Tavakoli, and M. Riazi, "An overview of public cloud security issues," *International Journal of Management Excellence*, vol. 3, no. 2, pp. 440–445, 2014.

[23] G. Aryotejo, D. Y. Kristiyanto, and Mufadhol, "Hybrid cloud: bridging of private and public cloud computing," *Journal of Physics: Conference Series*, vol. 1025, no. 1, Article ID 012091, 2018.

[24] F. Shirazi and A. Iqbal, "Community clouds within M-commerce: a privacy by design perspective," *Journal of Cloud Computing*, vol. 6, no. 1, p. 22, 2017.

[25] E. Loukis, M. Janssen, and I. Mintchev, "Determinants of software-as-a-service benefits and impact on firm performance," *Decision Support Systems*, vol. 117, pp. 38–47, 2019.

[26] N. Khanghahi and R. Ravanmehr, "Cloud computing performance evaluation: issues and challenges," *International Journal of Cloud Computing: Services and Architecture*, vol. 3, no. 5, pp. 29–41, 2013.

[27] S. Shahzadi, M. Iqbal, Z. U. Qayyum, and T. Dagiuklas, "Infrastructure as a service (IaaS): a comparative performance analysis of open-source cloud platforms," in *Proceedings of the 2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, vol. 2017, pp. 1–6, Lund, Sweden, June 2017.

[28] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services and Applications*, vol. 1, no. 1, pp. 7–18, 2010.

[29] V. Goyal, "Review: layers arhitecture of cloud computing," *International Journal of Computing & Business Research*, vol. 8, 2012.

[30] J. Jeya Singh, "Layers based security issues in cloud computing," 2015, http://www.ijarse.com.

[31] O. Malomo, D. B. Rawat, and M. Garuba, "A federated cloud computing framework for adaptive cyber defense and distributed computing," in *Proceedings of the 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1–6, Atlanta, GA, USA, May 2017.

[32] L. Schaefer and A. Atreya, "Intelligent applications of cloud computing in enhancing health care services," *International Journal of Intelligent Networks*, vol. 1, pp. 128–134, 2020.

[33] P. D. Kaur and I. Chana, "Cloud based intelligent system for delivering health care as a service," *Computer Methods and Programs in Biomedicine*, vol. 113, no. 1, pp. 346–359, 2014.

[34] C. Zhang, L. Zhu, C. Xu, and R. Lu, "PPDP: an efficient and privacy-preserving disease prediction scheme in cloud-based e-healthcare system," *Future Generation Computer Systems*, vol. 79, pp. 16–25, 2018.

[35] N. Gupta, N. Ahuja, S. Malhotra, A. Bala, and G. Kaur, "Intelligent heart disease prediction in cloud environment through ensembling," *Expert Systems*, vol. 34, no. 3, Article ID e12207, 2017.

[36] J. Yang, "Cloud computing for storing and analyzing petabytes of genomic data," *Journal of Industrial Information Integration*, vol. 15, pp. 50–57, 2019.

[37] M. Ambigavathi and D. Sridharan, "Big data analytics in healthcare," in *Proceedings of the 2018 Tenth International Conference on Advanced Computing (ICoAC)*, pp. 269–276, Chennai, India, December 2018.

[38] J. Archenaa and E. A. M. Anita, "A survey of big data analytics in healthcare and government," *Procedia Computer Science*, vol. 50, pp. 408–413, 2015.

[39] B. M. Balachandran and S. Prasad, "Challenges and benefits of deploying big data analytics in the cloud for business intelligence," *Procedia Computer Science*, vol. 112, pp. 1112–1122, 2017.

[40] N. Khorasani, S. Abrishami, M. Feizi, M. A. Esfahani, and F. Ramezani, "Resource management in the federated cloud environment using Cournot and Bertrand competitions," *Future Generation Computer Systems*, vol. 113, pp. 391–406, 2020.

[41] S. Alansari, F. Paci, A. Margheri, and V. Sassone, "Privacy-preserving access control in cloud federations," in *Proceedings of the 2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, vol. 2017, pp. 757–760, Copenhagen, Denmark, June 2017.

[42] A. N. Toosi, R. N. Calheiros, and R. Buyya, "Interconnected cloud computing environments," *ACM Computing Surveys*, vol. 47, no. 1, pp. 1–47, 2014.

[43] G. Zangara, D. Terrana, P. P. Corso, M. Ughetti, and G. Montalbano, "A cloud federation architecture," in *Proceedings of the 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, pp. 498–503, Krakow, Poland, November 2015.

[44] S. S. Chauhan, E. S. Pilli, R. C. Joshi, G. Singh, and M. C. Govil, "Brokering in interconnected cloud computing environments: a survey," *Journal of Parallel and Distributed Computing*, vol. 133, pp. 193–209, 2019.

[45] S. Seo, M. Kim, Y. Cui, S. Seo, and H. Lee, "SFA-based cloud federation monitoring system for integrating physical resources," in *Proceedings of the 2015 International Conference on Big Data and Smart Computing, BIGCOMP 2015*, pp. 55–58, Jeju, South Korea, 2015.

[46] O. O. Ajayi, A. B. Bagula, and K. Ma, "Fourth industrial revolution for development: the relevance of cloud federation in healthcare support," *IEEE Access*, vol. 7, pp. 185322–185337, 2019.

[47] A. Ruggeri, M. Fazio, A. Celesti, and M. Villari, "Blockchain-based healthcare workflows in federated hospital clouds, service-oriented and cloud computing," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12054, pp. 113–121, Springer, Berlin, Germany, 2020.

[48] S. Shenai and M. Aramudhan, "Cloud computing framework to securely share health & medical records among federations of healthcare information systems," *Biomedical Research*, vol. 2018, pp. S133–S136, 2018.

[49] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: a survey," *Future Generation Computer Systems*, vol. 97, pp. 219–235, 2019.

[50] H. Ning, Y. Li, F. Shi, and L. T. Yang, "Heterogeneous edge computing open platforms and tools for internet of things," *Future Generation Computer Systems*, vol. 106, pp. 67–76, 2020.

[51] I. Sittón-Candanedo, R. S. Alonso, J. M. Corchado, S. Rodríguez-González, and R. Casado-Vara, "A review of edge computing reference architectures and a new global edge proposal," *Future Generation Computer Systems*, vol. 99, pp. 278–294, 2019.

[52] P. Garcia Lopez, A. Montresor, D. Epema et al., "Edge-centric computing," *ACM SIGCOMM-Computer Communication Review*, vol. 45, no. 5, pp. 37–42, 2015.

[53] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[54] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

[55] R. Sanchez-Iborra, J. Sanchez-Gomez, and A. Skarmeta, "Evolving IoT networks by the confluence of MEC and LP-WAN paradigms," *Future Generation Computer Systems*, vol. 88, pp. 199–208, 2018.

[56] H. Li, K. Ota, and M. Dong, "Learning IoT in edge: deep learning for the internet of things with edge computing," *IEEE Network*, vol. 32, no. 1, pp. 96–101, 2018.

[57] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018.

[58] W. Yu, F. Liang, X. He et al., "A survey on the edge computing for the internet of things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018.

[59] C. Jiang, T. Fan, H. Gao et al., "Energy aware edge computing: a survey," *Computer Communications*, vol. 151, pp. 556–580, 2020.

[60] F. A. Khan, A. A. Ibrahim, and A. M Zeki, "Environmental monitoring and disease detection of plants in smart greenhouse using internet of things," *Journal of Physics Communications*, vol. 4, no. 5, Article ID 055008, 2020.

[61] M. Chen, W. Li, Y. Hao, Y. Qian, and I. Humar, "Edge cognitive computing based smart healthcare system," *Future Generation Computer Systems*, vol. 86, pp. 403–411, 2018.

[62] A. Sacco, F. Esposito, G. Marchetto, G. Kolar, and K. Schwetye, "On edge computing for remote pathology consultations and computations," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 9, pp. 2523–2534, 2020.

[63] C. Dilibal, "Development of edge-IoMT computing architecture for smart healthcare monitoring platform," in *Proceedings of the 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, Istanbul, Turkey, 2020.

[64] S. Ningning, G. Chao, A. Xingshuo, and Z. Qiang, "Fog computing dynamic load balancing mechanism based on graph repartitioning," *China Communications*, vol. 13, no. 3, pp. 156–164, 2016.

[65] M. Luqman and A. R. Faridi, "An overview of security issues in fog computing," in *Proceedings of the 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 1157–1162, New Delhi, India, 2019.

[66] H. S. Pannu, J. Liu, and S. Fu, "AAD: adaptive anomaly detection system for cloud computing infrastructures," in *Proceedings of the 2012 IEEE 31st Symposium on Reliable Distributed Systems*, pp. 396-397, Irvine, CA, USA, 2012.

[67] G. Li, Y. Yao, J. Wu, X. Liu, X. Sheng, and Q. Lin, "A new load balancing strategy by task allocation in edge computing based on intermediary nodes," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, p. 3, 2020.

[68] A. Yousefpour, C. Fung, T. Nguyen et al., "All one needs to know about fog computing and related edge computing paradigms: a complete survey," *Journal of Systems Architecture*, vol. 98, pp. 289–330, 2019.

[69] E. C. Pinto Neto, G. Callou, and F. Aires, "An algorithm to optimise the load distribution of fog environments," in *Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 1292–1297, Banff, Canada, October 2017.

[70] S. Yi, C. Li, and Q. Li, "A survey of fog computing," in *Proceedings of the 2015 Workshop on Mobile Big Data*, pp. 37–42, Hangzhou, China, June 2015.

[71] A. Al-Qerem, M. Alauthman, A. Almomani, and B. B. Gupta, "IoT transaction processing through cooperative concurrency control on fog-cloud computing environment," *Soft Computing*, vol. 24, no. 8, pp. 5695–5711, 2020.

[72] X. An, J. Su, X. Lü, and F. Lin, "Hypergraph clustering model-based association analysis of DDOS attacks in fog computing intrusion detection system," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 249, 2018.

[73] M. Engineer, R. Tusha, A. Shah, and D. K. Adhvaryu, "Insight into the importance of fog computing in internet of medical things (IoMT)," in *Proceedings of the 2019 International Conference on Recent Advances in Energy-Efficient Computing And Communication (ICRAECC)*, pp. 1–7, Piscataway, NJ, USA, 2019.

[74] Y. Huo, C. Yong, and Y. Lu, "Re-ADP: real-time data aggregation with adaptive ω-event differential privacy for fog computing," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 6285719, 13 pages, 2018.

[75] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "IoT-based big data secure management in the fog over a 6G wireless network," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5164–5171, 2021.

[76] Y. Jebbar, F. Belqasmi, R. Glitho, and O. Alfandi, "A fog-based architecture for remote phobia treatment," in *Proceedings of the International Conference on Cloud Computing Technology and Science, CloudCom*, vol. 2019, pp. 271–278, Sydney, Australia, December 2019.

[77] K. Tiwari, S. Kumar, and R. K. Tiwari, "Fog assisted healthcare architecture for pre-operative support to reduce latency," *Procedia Computer Science*, vol. 167, pp. 1312–1324, 2020.

[78] O. Akrivopoulos, I. Chatzigiannakis, C. Tselios, and A. Antoniou, "On the deployment of healthcare applications over fog computing infrastructure," in *Proceedings of the 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, pp. 288–293, Torino, Italy, July 2017.

[79] M. Attaran and J. Woods, "Cloud computing technology: improving small business performance using the Internet," *Journal of Small Business and Entrepreneurship*, vol. 31, no. 6, pp. 495–519, 2019.

[80] O. Al-Hujran, E. M. Al-Lozi, M. M. Al-Debei, and M. Maqableh, "Challenges of cloud computing adoption from the TOE framework perspective," *International Journal of E-Business Research*, vol. 14, no. 3, pp. 77–94, 2018.

[81] D. T. Issa, V. Chang, and D. T. Issa, "The impact of cloud computing and organizational sustainability," in *Proceedings of the International Conference on Cloud Computing & Virtualization 2010 CCV 2010*, pp. 163–169, Lisbon, Portugal, April 2010.

[82] G. Brataas, N. Herbst, S. Ivansek, and J. Polutnik, "Scalability analysis of cloud software services," in *Proceedings of the 2017 IEEE International Conference on Autonomic Computing (ICAC)*, pp. 285–292, Columbus, OH, USA, 2017.

[83] M. R. Mesbahi, A. M. Rahmani, and M. Hosseinzadeh, "Reliability and high availability in cloud computing environments: a reference roadmap," *Human-centric Computing and Information Sciences*, vol. 8, no. 1, 2018.

[84] M. Mircea and A. Andreescu, "Using cloud computing in higher education: a strategy to improve agility in the current financial crisis," *Communications of the IBIMA*, vol. 2011, Article ID 875547, 15 pages, 2011.

[85] P. Modisane and O. Jokonya, "Evaluating the benefits of cloud computing in small, medium and micro-sized enterprises (SMMEs)," *Procedia Computer Science*, vol. 181, pp. 784–792, 2021.

[86] F. Fatemi Moghaddam, M. Ahmadi, S. Sarvari, M. Eslami, and A. Golkar, "Cloud computing challenges and opportunities: a survey," in *Proceedings of the 2015 1st International Conference on Telematics And Future Generation Networks (TAFGEN)*, pp. 34–38, Kuala Lumpur, Malaysia, May 2015.

[87] A. Singh and K. Chatterjee, "Cloud security issues and challenges: a survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, 2017.

[88] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174–184, 2018.

[89] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "Key issues for embracing the cloud computing to adopt a digital transformation: a study of Saudi public sector," *Procedia Computer Science*, vol. 130, pp. 1037–1043, 2018.

[90] D. Yimam and E. B. Fernandez, "A survey of compliance issues in cloud computing," *Journal of Internet Services and Applications*, vol. 7, no. 1, p. 5, 2016.

[91] T. J. Li and M. M. Singh, "Hybrid trust framework for loss of control in cloud computing," *Lecture Notes in Electrical Engineering*, Springer-Verlag, vol. 279, pp. 669–675, Berlin, Germany, 2014.

[92] O. Kocabas, "Towards privacy-preserving medical cloud computing using homomorphic encryption," in *Enabling Real-Time Mobile Cloud Computing through Emerging Technologies*, T. Soyata, Ed., IGI Global, Hershey, PA, USA, , pp. 213–216.

[93] P. Varshney and Y. Simmhan, "Demystifying fog computing: characterizing architectures, applications and abstractions," in *Proceedings of the 2017 IEEE 1st International Conference on Fog And Edge Computing, ICFEC 2017*, pp. 115–124, Madrid, Spain, February 2017.

[94] F. Ebadifard and S. M. Babamir, "Federated geo-distributed clouds: optimizing resource allocation based on request type using autonomous and multi-objective resource sharing model," *Big Data Research*, vol. 24, Article ID 100188, 2021.

[95] M. Habibi, M. Fazli, and A. Movaghar, "Efficient distribution of requests in federated cloud computing environments utilizing statistical multiplexing," *Future Generation Computer Systems*, vol. 90, pp. 451–460, 2019.

[96] M. Liaqat, V. Chang, A. Gani et al., "Federated cloud resource management: review and discussion," *Journal of Network and Computer Applications*, vol. 77, pp. 87–105, 2017.

[97] A. Anas, M. Sharma, R. Abozariba, M. Asaduzzaman, E. Benkhelifa, and M. N. Patwary, "Autonomous workload balancing in cloud federation environments with different access restrictions," in *Proceedings of the 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pp. 636–641, Orlando, FL, USA, October 2017.

[98] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, and Q. Arshad, "Data and privacy: getting consumers to trust products enabled by the internet of things," *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 35–38, 2019.

[99] M. Al-Roomi, S. Al-Ebrahim, S. Buqrais, and I. Ahmad, "Cloud computing pricing models: a survey," *International Journal of Grid and Distributed Computing*, vol. 6, no. 5, pp. 93–106, 2013.

[100] E. Ahmed, A. Gani, M. Khurram Khan, R. Buyya, and S. U. Khan, "Seamless application execution in mobile cloud computing: motivation, taxonomy, and open challenges," *Journal of Network and Computer Applications*, vol. 52, pp. 154–172, 2015.

[101] E. Ahmed, A. Gani, M. Sookhak, S. H. A. Hamid, and F. Xia, "Application optimization in mobile cloud computing: motivation, taxonomies, and open challenges," *Journal of Network and Computer Applications*, vol. 52, pp. 52–68, 2015.

[102] M. De Donno, K. Tange, and N. Dragoni, "Foundations and evolution of modern computing paradigms: cloud, IoT, edge, and fog," *IEEE Access*, vol. 7, pp. 150936–150948, 2019.

[103] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: state-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 416–464, 2018.

[104] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, "Fog computing security challenges and future directions [energy and security]," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 92–96, 2019.

[105] P. Bellavista, J. Berrocal, A. Corradi, S. K. Das, L. Foschini, and A. Zanni, "A survey on fog computing for the Internet of Things," *Pervasive and Mobile Computing*, vol. 52, pp. 71–99, 2019.

[106] A. A. Sadri, A. M. Rahmani, M. Saberikamarposhti, and M. Hosseinzadeh, "Fog data management: a vision, challenges, and future directions," *Journal of Network and Computer Applications*, vol. 174, Article ID 102882, 2021.

[107] J. Du, L. Zhao, J. Feng, and X. Chu, "Computation offloading and resource allocation in mixed fog/cloud computing systems with min-max fairness guarantee," *IEEE Transactions on Communications*, vol. 66, no. 4, pp. 1594–1608, 2018.

[108] M. Ashouri, P. Davidsson, and R. Spalazzese, "Cloud, edge, or both? Towards decision support for designing IoT applications," in *Proceedings of the 2018 Fifth International Conference on Internet of Things: Systems, Management And Security*, pp. 155–162, Valencia, Spain, October 2018.

[109] M. Ghobaei-Arani, A. Souri, and A. A. Rahmanian, "Resource management approaches in fog computing: a comprehensive review," *Journal of Grid Computing*, vol. 18, no. 1, pp. 1–42, 2020.

[110] W. d. E. Santo, R. d. S. Matos Junior, A. d. R. L. Ribeiro, D. S. Silva, and R. Santos, "Systematic mapping on orchestration of container-based applications in fog computing," in *Proceedings of the 2019 15th International Conference on Network and Service Management (CNSM)*, Halifax, Canada, 2019.

[111] D. G. S. Pivoto, L. F. F. de Almeida, R. da Rosa Righi, J. J. P. C. Rodrigues, A. B. Lugli, and A. M. Alberti, "Cyber-physical systems architectures for industrial internet of

things applications in Industry 4.0: a literature review," *Journal of Manufacturing Systems*, vol. 58, pp. 176–192, 2021.

[112] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 27–40, 2017.

[113] A. Mishra, N. Gupta, and B. B. Gupta, "Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller," *Telecommunication Systems*, vol. 77, no. 1, pp. 47–62, 2021.

[114] B. B. Mamta, B. B. Gupta, K.-C. Li, V. C. M. Leung, K. E. Psannis, and S. Yamaguchi, "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 12, pp. 1–14, 2021.

[115] K. Bhushan and B. B. Gupta, "Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 5, pp. 1985–1997, 2019.