The Next Generation Cloud technologies: A Review On Distributed Cloud, Fog And Edge Computing and Their Opportunities and Challenges

Ali T. Atieh

EGM- IT Infrastructure Operation,

Etihad Etisalat – MOBILY

ORCID

2021

Received: 2021/08/06 Available online: 2021/10/09

How to cite:
Atieh, A. T. (2021) 'The Next Generation Cloud technologies: A Review On Distributed Cloud, Fog And Edge Computing and Their Opportunities and Challenges', ResearchBerg Review of Science and Technology, 1(1), pp. 1–15. Available at: https://researchberg.com/.

Abstract

Cloud computing is a 21st-century wonder with applications in nearly every industry imaginable. As a new technology, it has certain shortcomings. There are always attempts for improvements to combat those shortcomings. The next generation cloud technologies is believed to overcome these shortcomings. This research seeks to examine the few next generation cloud technologies, namely, distributed cloud, fog computing, edge computing. The distributed cloud improves worldwide service communications while also allowing for more responsive communications in individual regions. The distributed approach is used by cloud providers to allow lower latency and greater efficiency for cloud services. We find that there are few opportunities in Distributed Cloud such as, Improved security, IoT implementations, Faster content delivery, and cost efficiency. However, it poses some challenges such as data exposure to hackers when transferred from public networks. Fog computing, according to the findings, reduces the amount of time it takes, lowers operational costs, increases the level of security. However, one of the most difficult aspects of fog computing is the substantial reliance on data transit. An edge computing system allows consumer data to be handled at the network's edge, as close to the source as feasible. Several opportunities of edge computing in various areas include Network optimization, Healthcare improvement, and Transportation. The popularity of some of the next generation cloud technologies has been strongly impacted by the growth of the internet of things and the unanticipated surge in data created by IoT-connected devices. It is possible to state that obstacles can be gradually overcome because the benefits of next generation cloud technologies enable solutions that meet a wide range of contemporary company requirements. The adoption of next generation cloud technologies might take some time as businesses consider the benefits and drawbacks, and the transition may be slow.

i) Introduction

Cloud computing is being hailed as the final solution to the problems of unpredictable traffic spikes, computing overloads, and potentially costly data processing and backup hardware investments. By altering the way hardware is developed and purchased, it has the potential to change the IT business, making both software and infrastructure even more appealing as services. In practice, cloud computing is a computing paradigm that provides dynamically scalable and frequently virtualized resources over the Internet to supplement the present consumption and delivery model for IT services based on the Internet.

Cloud computing's key benefits are ease and cost savings. Cloud providers are experts in the services they provide, which include renting hardware, operating systems, storage, and software. As a result, a corporation can focus on its principal objective rather than getting a range of IT personnel. A corporation, for example, does not need to employ backup personnel because it may acquire this service from a backup specialist. The backup cloud provider will almost certainly provide better service than ad hoc staff engaged to handle it. In addition to convenience, this computing outsourcing approach lowers both upfront and continuing costs for businesses. A corporation does not need to plan for resource usage fluctuations. Cloud computing services operate on a pay-as-you-go basis, shielding cloud users from tedious duties such as equipment and software updates and maintenance. The money saved on prospective equipment investments and administration can be spent on areas that are critical to the company's goal.

Cloud computing models

With application service provision to grid and utility computing, cloud computing encompasses a variety of solutions based on the services they provide. The most well-known models that underpin the cloud paradigm are discussed here.

Software services, data storage, operating systems, and hardware infrastructure are all instances of cloud computing resources. There are three main cloud delivery models depending on the type or granularity of the service: infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Cloud consumers will use cloud client programs to access cloud services, which can be deployed on a variety of premises (organizational buildings) and devices (desktops, laptops, tablets, and smartphones) (Mohammed and Zebaree, 2021).

1. Infrastructure-as-a-Service

The cloud users are provided with raw IT resources such as hardware, storage, IP addresses, and firewalls via the Internet in this paradigm. Hypervisors, such as Xen, Oracle VirtualBox, KVM, VMware ESX/ESXi, or Hyper-V, run a group of virtual machines on actual IT resources and provide cloud users with virtualized copies of these resources. Customers who use the cloud have the freedom to install whatever environment and software they want on these platforms, as well as a great deal of control over how these resources are managed and secured. Amazon Web Services (AWS), Windows Azure, Google Compute Engine, Rackspace Open Cloud, and IBM SmartCloud Enterprise are examples of cloud providers for IaaS (Mohammed and Zebaree, 2021).

2. Platform-as-a-Service

Cloud companies also provide ready-to-use platforms as a service to cloud customers who desire a higher level of compute and administration outsourcing. A full virtualized environment with an operating system image loaded can be rented using this concept. Platforms for development, web servers, and databases are frequently included. After purchasing a platform, cloud users are free to install and manage apps that run in a virtualized environment. As the cloud provider installs, maintains, and patches the platform, the level of governance and control over the system falls. Security at the hardware and operating system level is entirely dependent on the policies and methods of the cloud provider (Rani and Ranjan, 2014).

3. Software-as-a-Service

When cloud customers use the Internet to access third-party applications, this is the most fine-grained delivery approach. Free access (e.g., Google Docs) or subscription options are available (e.g., DropBox for file synchronization). The consumer of cloud software has little control over how it operates or the security of the data it accesses. The administrative load is borne entirely by the cloud software supplier.

Cloud deployment models

Many businesses are progressively shifting a significant amount, if not all, of their IT operations to corporate cloud computing. When it comes to cloud ownership and administration, the company has a number of options. For cloud computing, there are four main deployment types.

a) Public cloud: A public cloud infrastructure is controlled by a company that sells cloud services and makes it available to the general public or a big industry group. The CP is in charge of the cloud infrastructure as well as data and operational control within the cloud. A commercial, academic, or government entity, or a combination of them, may own, manage, and operate a public cloud. It is located on the cloud service provider's premises.

In a public cloud architecture, all key components are placed in a multitenant infrastructure outside the company firewall. Applications and storage are made accessible via the Internet through a secure IP address and might be free or paid-per-use. This sort of cloud provides simple consumer-style services, such as on-demand online apps or capacity from Amazon and Google, Yahoo mail, and free photo storage from Facebook or LinkedIn. While public clouds are less expensive and can grow to meet demand, they usually lack service level agreements (SLAs) and might not provide the same level of protection against data loss or corruption as private or hybrid cloud services. Consumers and businesses who do not require the same standards of service as those anticipated behind the firewall should use the public cloud. Furthermore, public IaaS clouds may not always include limitations or compliance with privacy regulations, which are the subscriber's or corporate end user's obligation. Many public clouds cater to consumers and little and medium enterprises, with pay-per-use prices that can be as low as cents per gigabyte. Picture and music sharing, laptop backup, and file sharing are all examples of services.

The most significant benefit of the public cloud is its low cost. A subscriber charges only for the services and equipment it requires, and can make changes as needed. In addition, the subscriber's management overhead is significantly decreased. The main worry is security; nevertheless, a number of public cloud providers have proven excellent security measures, and such companies may have more resources and experience to dedicate to security than a private cloud provider (Jadeja and Modi, 2012).

2. Private Cloud

A private cloud is set up within an organization's own IT infrastructure. The company can either administer the cloud in-house or outsource the management to a third party. Furthermore, cloud servers and storage equipment may be located on or off premises.

Internally, over an intranet or the Internet through a VPN, private clouds can offer IaaS to employees or business units, as well as software (applications) or storage as a service to branch offices. In both situations, private clouds offer a means to use existing infrastructure to deliver and bill for bundled or full services while remaining within the organization's network's security perimeter. Database on demand, e-mail on demand, and storage on demand are examples of services offered through the private cloud (Goyal, 2014).

One of the most compelling reasons to use a private cloud is security. A private cloud architecture allows for more precise control over data storage location and other security features. Easy resource sharing and quick deployment to organizational entities are further advantages.

3. Community cloud

A community cloud combines the best features of both private and public clouds. A communal cloud, like a private cloud, has limited access. The cloud resources are shared across a number of independent companies, similar to a public cloud. The enterprises that utilize the community cloud have comparable needs and, in most cases, a necessity to share data. The healthcare business is one instance of an industry that is utilizing the community cloud idea (Shaheen, 2021c). To comply with government privacy and other requirements, a community cloud can be built. Participants in the community can trade data in a regulated manner (Singh and Jangwal, 2012).

The cloud infrastructure can be maintained by the participating businesses or by a third party, and it can be on-premises or off. Because the costs are shared across fewer users than in a public cloud (but more than in a private cloud), only a portion of the cost savings prospective of cloud computing is achieved in this deployment type.

4. Hybrid Cloud

The hybrid cloud architecture is made up of two or more clouds (private, communal, or public) that are separate yet linked by standardized or proprietary technology that allows data and application mobility. With a hybrid cloud system, critical data may be stored in a secure part of the cloud while less sensitive data can benefit from the public cloud's features (Ghazizadeh, 2012).

Smaller organizations may find a hybrid public/private cloud solution particularly appealing. Without committing the company to shifting more sensitive data and apps to the public cloud, many applications for which security issues are less of a problem can be offloaded at significant cost savings.

ii) Distributed Cloud (DC): opportunities and challanges

The implementation of cloud computing technology to interconnect data and applications served from many geographic sites is known as distributed cloud. In the context of information technology (IT), the term "distributed" refers to something that is shared among numerous systems that may be located in different locations. The distributed cloud improves worldwide service communications while also allowing for more responsive communications in individual regions (Oza *et al.*, 2013). The distributed approach is used by cloud providers to allow lower latency and greater efficiency for cloud services. Public resource computing and the volunteer cloud are two further instances of distributed cloud outside of the cloud provider setting.

Types of distributed cloud:

• Public-resource computing: This sort of distributed cloud is the outcome of a broad definition of cloud computing, as it is more closely associated with distributed computing than cloud computing. This can also be thought of as a sub-category of cloud computing (Coady *et al.*, 2015).

• Volunteer cloud: This computing type is defined as the meeting of cloud technology and public-resource computing. A cloud computing architecture is constructed using volunteer resources in this scenario. However, because of the variability of the resources required to construct it and the dynamic setting in which it functions, this form of infrastructure faces numerous issues. It's also known as ad-hoc clouds or peer-to-peer clouds (Endo *et al.*, 2011).

DC offers some opportunities over centralized cloud, including:

a) Internet of Things (IoT), artificial intelligence (AI), and machine learning implementations: Real-time data processing is required for video surveillance, industrial robotics, self-driving vehicles, healthcare applications, smart buildings, and other applications that cannot wait for data to go to a central cloud data center and back. These applications require minimal latency, which is provided via distributed cloud and edge computing.

b) Faster content delivery: By storing and distributing video material from locations closer to end-users, a content delivery network (CDN) installed on a distributed cloud can enhance streaming video content quality - and the user experience.

c) Greater visibility and manageability of hybrid cloud/multicloud architecture: Distributed cloud may assist any organization achieve better control over its hybrid multicloud infrastructure by enabling visibility and management from a single console, using a single set of tools.

d) Improved, cost-effective scalability and quickness: Expansion of a dedicated data center, or the construction of new data center sites in multiple regions, is costly and time-consuming. With distributed cloud, a company can swiftly create and execute anywhere in the environment, using the same tools and staff, without having to build out new infrastructure or edge locations (Oza *et al.*, 2013).

e) Easier industry or regional regulatory compliance: Many data privacy laws stipulate that a customer's personal information (PI) cannot be transferred outside of the user's jurisdiction. An organization's ability to process PI in each user's region of residency is greatly facilitated by distributed cloud infrastructure. In the healthcare, telecommunications, and other industries, processing data at the source can make it easier to comply with data privacy requirements (Nguyen *et al.*, 2018).

Although the current cloud model is quite successful, a new generation of platforms is working on decentralizing cloud infrastructure using AI and blockchain in order to tackle some issues faced by enterprises in traditional cloud (Rashid *et al.*, 2018). This new cloud model can accommodate scalable applications while maintaining the benefits of a decentralized, trust-free ecosystem.

As opposed to centralized cloud storage, which necessitates transferring and storing duplicate entries files on the internet to a core datacenter located thousands of miles away, a decentralized cloud or edge computing architecture tries to solve the inefficiency issues of uploading, downloading, to the constrained storing capabilities of cloud servers.

A decentralized architecture may increase the security of cloud services. To safeguard privacy and covert theft of information from third parties, law enforcement, and foreign powers, files can be maintained locally behind a firewall in specific geographic areas with access regulated. The attack surface is reduced since data is not replicated to third-party systems or other locations. Because files and storage are under an organization's control, adherence with other regulations is also accelerated.

Because it enables security through compartmentalization, a decentralized cloud system operates on blockchain, making network security significantly stronger than current infrastructure. Even if attackers gain access to a section of data, they will not be able to permeate it because it is only a partial file. In addition, the design divides files into small chunks and duplicates data over distributed file systems, enabling redundancy through numerous nodes. Other nodes stay operating if one is attacked or brought down, providing a failsafe that improves cloud stability.

This shift in storage models will not occur over night. However, given the increasing volume of data and the rapid addition of new devices (particularly IoT) to networks, cloud security strategies will undergo a paradigm shift. Because the storage industry is so huge, it's possible that we'll see more businesses adopt a distributed cloud computing strategy.

Its distributed cloud or edge computing design distinguishes it from file sync and share systems, which use a centralized paradigm. It improves the organization's security posture, gives access to all storage, guarantees privacy, keeps file management under organization 's control, and makes use of the organization's current storage infrastructure.

Challenges in distributed cloud

• Distributed cloud computing might pose security issues, such as data being exposed to hackers when transferred from public networks, just like any other technology.

• Troubleshooting will also be challenging due to the infrastructure's complexity.

• Infrastructure with dispersed cloud has additional interfaces, resulting in hardware and software problem spots.

Finally, it is possible to state that these obstacles can be gradually overcome because the benefits of distributed cloud enable solutions that meet a wide range of contemporary company requirements. The adoption of distributed cloud might take some time as businesses consider the benefits and drawbacks, and the transition will be slow, but distributed cloud is unquestionably the future of distributed computation (Ludwig and Schmid, 2015).

Volunteer computing (VC) is a type of distributed computing that allows members of the public to volunteer their unused computing capabilities and assist in the execution of computationally intensive tasks (Anderson, Korpela and Walton, 2005). VC offers a large number of low-cost resources that can deliver more computer power to science than any other sort of computing. It increases public engagement in scientific research and gives scientists a role in selecting the direction of research that would otherwise be impossible to accomplish. A scientific endeavor with low resources but broad public appeal can benefit from VC's huge processing capacity (Durrani and Shamsi, 2014). Some existing VC platforms have millions of users and offer massive amounts of memory and processing power. VC provides its users with a scalable, low-cost, dependable, and efficient computing platform in which time-consuming activities are broken down into manageable chunks for parallel processing. Volunteers (also referred as workers, hosts, or nodes) contribute a part of their storage or computing power to construct a resource-cloud. A middleware is required to execute computationally intensive projects, since it receives pieces from servers and sends them to volunteers for storage or processing (Sarmenta, 2001).

iii) Fog computing

Cisco coined the phrase fog computing to describe a cloud computing alternative (Khanagha *et al.*, 2020). By placing some resources and transactions at the network's edge, this method capitalizes on the simultaneous dilemma of the proliferation of computer devices and the opportunity afforded by the data those devices generate. Rather than constructing in-cloud channels for usage and storage, users collect bandwidth at access points including such as routers by placing them closer to devices. As a result, less data can be transported away from data centers, through cloud channels, and over long distances, lowering overall bandwidth requirements (Uriarte and DeNicola, 2018).

Another significant distinction between cloud computing and fog computing is data storage. Because less data requires immediate cloud storage in fog computing, clients could rather subject data to strategic assembly and distribution procedures that increase efficiency and lower costs. It is simpler to leverage on the available computing capacity in devices by putting real-time analytics into a cloud computing fog placed closer to them. This improves the user experience while also lowering the cloud's overall strain. Devices linked to the internet of things benefit from fog computing the most (IoT) (Dastjerdi and Buyya, 2016).

Fog computing and cloud computing differ mostly in terms of decentralization and flexibility. Fog computing, also known as fog networking or fogging, is a decentralized computer architecture that sits between the cloud and data-generating devices. This adaptable framework lets users to optimize performance by placing resources, such as apps and the data users generate, in logical areas (Mahmud, Kotagiri and Buyya, 2018). The structure's purpose is to put fundamental analytic services closer to where they're needed, at the network's edge. This decreases the distance over which users must transfer data over the network, resulting in improved speed and overall network performance. Users gain from fog computing security concerns as well. The fog computing model can segregate bandwidth traffic, allowing users to increase network security by adding extra firewalls.

Fog computing retains some of the characteristics of cloud computing, from which it evolved. While employing a fog computing architecture, users can still store apps and data elsewhere and pay for not only offshore storage, but also cloud improvements and management for their data. For example, their workers will still be capable to obtain data remotely.

Fog Computing's opportunities and challenges.

The following are some of the opportunities from fog computing:

a) Reduce the amount of time it takes for something to happen. Keep analysis near to the data source to avoid cascade system problems, production line blackouts, and other severe issues, particularly in verticals where each second matters. The capacity to undertake real-time data analysis implies faster alerts, less risk for consumers, and less wasted time (Krishnaraj *et al.*, 2022).

b) Make the most of network bandwidth. Many data analytics jobs, including essential studies, may not necessitate the scalability provided by cloud-based storage and processing. Meanwhile, linked gadgets generate an increasing amount of data that can be analyzed. Fog computing reduces the need for most of this massive data to be transported, freeing up bandwidth for other mission-critical operations.

c) Lower operational costs. Lower operating costs are achieved by processing as much data domestically as feasible and preserving network bandwidth.

d) Increase the level of security. It is critical to safeguard IoT data while it is being transmitted or stored. To provide increased cybersecurity, clients can watch and safeguard fog nodes employing the similar controls, guidelines, and processes applied across the whole IT system and attack continuum (Iorga *et al.*, 2018).

e) Boost trustworthiness. Because IoT devices are frequently deployed in tough environments and during emergencies, circumstances can be harsh. Under these conditions, fog computing can enhance the accuracy while lowering the data transfer load.

f) Deepen your understanding without jeopardizing your privacy. Instead of transferring confidential data to the cloud for analytics and risking a data breach, your team may analyze it locally on the devices that gather, evaluate, and store that data. As a result, the nature of fog computing's data security and privacy provides wiser solutions for more sensitive data.

g) Boost company's flexibility. Businesses can only respond to client demand swiftly if they know what resources they require, where they require them, and when they need them. Developers can create fog applications quickly and execute them as needed thanks to fog computing. Fog computing technology also enables users to provide more tailored services and products to their clients, as well as position data and data tools where they can be processed most effectively, all while leveraging current computer capabilities and infrastructure (Krishnaraj *et al.*, 2022).

But the fog computing poses also certain challenges. One of the most difficult aspects of fog computing is the substantial reliance on data transit. The introduction of the 5G network has helped to alleviate this problem, although there are still concerns such as limited availability, slower speeds, and peak congestion. Other potential challenges that need to be addressed at fog nodes are speed and security.

iv) Edge computing

An edge computing system allows consumer data to be handled at the network's edge, as close to the source as feasible. The significance of data in today's enterprises cannot be overstated. It is the foundation for modern-day industry. It offers critical information and allows for critical business activities and procedures to take place. (Khan *et al.*, 2019)

There is currently an abundance of data, and organizations are overwhelmed by the vast amount of data available. This surplus data, on the other hand, may be acquired and classified utilizing Internet of Things (IoT) devices and sensors that function in computer time from remote places and in hostile computing environments everywhere on the planet, including space.

For task computing, a proper framework is always required. The framework and structure that are appropriate for one job may not be appropriate for all types of computer tasks. Edge computing is a technological breakthrough that has resulted in a necessary and feasible system that allows distributed computing to use storage resources and compute closer to the data source (objectively, without altering the physical location). In general, distributed computing models are not new. The computational performance of remote and regional workplaces, cloud computing, and data center colocation ideas is well documented. Data decentralization necessitates a high degree of control and monitoring, which might be problematic. During transmission from the common centralized system, the number of requests might easily be missed.

Edge computing's relevance has grown in recent years, and it now offers a suitable solution to the resulting network difficulties associated with the movement of large amounts of data that organizations and industries generate and utilize. Aside from the volume of data sent, there is also the problem of time. Computing operations rely heavily on data input and output that has grown increasingly time-sensitive, as seen by the rise of self-driving automobiles. A traffic management system will be crucial for self-driving automobiles. Data will be generated, analyzed, and shared in real time by traffic controllers and automobiles. When this requirement is compounded by a large number of self-driving or autonomous devices, the scope of the potential difficulties becomes clear. This situation needs a rapid reaction network. Fog and edge computing are used to address three major network issues: latency, bandwidth, and congestion.

Opportunities and challenges of edge computing

Several opportunities of edge computing in various disciplines and businesses are listed below. Here are a few instances:

Network optimization is assisted by edge computing. edge computing guarantees that network performance is improved and optimized by evaluating users' performance throughout the Internet. Edge computing also employs an analytics method to choose the most reliable and low-latency network stream for a given user's traffic. In conclusion, edge computing is used to manage traffic across networks in order to get the greatest time-sensitive traffic performance (Satyanarayanan, 2017).

Edge computing may assist organizations monitor workplace circumstances and allow improved conditions to promote employee safety by combining data processing from onsite monitoring with data from sensor devices such as worker protection devices and other sensors. It may also be used to guarantee that personnel follow safety regulations, particularly in distant locations or risky environments such as oil rigs and construction sites (Shi and Dustdar, 2016).

Healthcare improvement occurs through edge computing. As patient data is acquired from various sensors, gadgets, and health appliances, the quantity of data collected in the healthcare industry has considerably risen (Shaheen, 2021b) (Shaheen, 2021a). The massive data volume necessitates the adoption of edge computing, which employs machine learning and automation to analyze data and detect issues, allowing doctors to respond quickly to treat patients. Transportation: According to research, autonomous cars create between 5 and 20 gigabytes of data each day. Autonomous cars acquire information about other vehicles, their position, vehicle condition, and road and traffic conditions. While the car is still driving, this data may be collected and evaluated in real time. Autonomous vehicles require significant onboard computer processing, which turns them into edges. (Shi *et al.*, 2016)

The popularity of edge computing has been strongly impacted by the growth of the internet of things and the unanticipated surge in data created by IoT-connected devices. However, the Internet of Things is still in its infancy, and its growth and development will have a significant impact on edge computing. The construction of micro modular data centers (MMDCs) is one of the future options. MMDCs are essentially data hubs in boxes, where an entire data center is packed into a small device that can be moved closer to data (Bilal *et al.*, 2018) (Shi and Dustdar, 2016). It brings computers as near to data as feasible while avoiding completely defining the data's edge.

V) Conclusion

Cloud computing is the most spectacular technical development of the last decades. This is due to the fact that it has been adopted into the mainstream at a faster rate than any other technology in the area. Cloud computing isn't just for corporations and organizations; it's also beneficial to the common consumer. It allows us to execute software applications without having to install them on our computers. This decade will see a lot of technical advancements. AI and IoT are revolutionizing the IT infrastructure, resulting in a rise in data creation that necessitates efficient datacenters and new solutions for real-time access to massive amounts of data.

Given the various advantages that cloud computing provides to businesses, it is reasonable to conclude that cloud computing is rapidly becoming the new normal. Cloud computing is assisting society in dealing with future issues such as large data management, cyber-security, and quality control (Atieh, 2021). Furthermore, cloud computing is making new technologies such as artificial intelligence, decentralized ledger technology, and many other features available as services.

The general tendency appears to be toward combining infrastructure from many suppliers and decentralizing computation away from the data centers' present concentration of resources. This is in contrast to typical single-provider cloud services. As a result, new computer models are emerging to meet market demands.

A variety of sectors will be impacted by the evolving cloud infrastructure and developing computer architecture. They will be critical in facilitating the Internet-of-Things paradigm by increasing connection between humans and things. In the field of data intensive computing, innovative approaches will be developed to solve the problems of dealing with large amounts of data. Containers, acceleration, and function are examples of new services that are expected to become popular. To offer self-learning systems, a variety of research fields will merge with next-generation cloud systems.

Many CEOs in companies that have already adopted cloud computing take safety for granted. When it comes to security, the destiny of cloud computing is obvious. As more businesses resort to cloud computing, the issue of unquestionable security has become unavoidable. Wherever there is a big quantity of data kept, cybercriminals are always there. Nothing can change that, but dependability and security may be adjusted.

References

Anderson, D. P., Korpela, E. and Walton, R. (2005) 'High-performance task distribution for volunteer computing', in *First International Conference on e-Science and Grid Computing (e-Science'05)*. IEEE, pp. 8-pp.

Atieh, A. T. (2021) 'Establishing Efficient IT Operations Management through Efficient Monitoring, Process Optimization, and Effective IT Policies', *Empirical Quests for Management Essences*, 1(1), pp. 1–13. Available at: https://researchberg.com/.

Bilal, K. *et al.* (2018) 'Potentials, trends, and prospects in edge technologies: Fog, cloudlet, mobile edge, and micro data centers', *Computer Networks*, 130, pp. 94–120.

Coady, Y. *et al.* (2015) 'Distributed cloud computing: Applications, status quo, and challenges', *ACM SIGCOMM Computer Communication Review*, 45(2), pp. 38–43.

Dastjerdi, A. V. and Buyya, R. (2016) 'Fog computing: Helping the Internet of Things realize its potential', *Computer*, 49(8), pp. 112–116.

Durrani, M. N. and Shamsi, J. A. (2014) 'Volunteer computing: requirements, challenges, and solutions', *Journal of Network and Computer Applications*, 39, pp. 369–380.

Endo, P. T. *et al.* (2011) 'Resource allocation for distributed cloud: concepts and research challenges', *IEEE network*, 25(4), pp. 42–46.

Ghazizadeh, A. (2012) 'Cloud computing benefits and architecture in e-learning', in *2012 IEEE seventh international conference on wireless, mobile and ubiquitous technology in education*. IEEE, pp. 199–201.

Goyal, S. (2014) 'Public vs private vs hybrid vs community-cloud computing: a critical review', *International Journal of Computer Network and Information Security*, 6(3), p. 20.

Iorga, M. *et al.* (2018) 'Fog computing conceptual model'.

Jadeja, Y. and Modi, K. (2012) 'Cloud computing-concepts, architecture and challenges', in *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*. IEEE, pp. 877–880.

Khan, W. Z. *et al.* (2019) 'Edge computing: A survey', *Future Generation Computer Systems*, 97, pp. 219–235.

Khanagha, S. *et al.* (2020) 'Mutualism and the dynamics of new platform creation: A study of Cisco and fog computing', *Strategic Management Journal*.

Krishnaraj, N. *et al.* (2022) 'The Future of Cloud Computing: Blockchain-Based Decentralized Cloud/Fog Solutions–Challenges, Opportunities, and Standards', in *Blockchain Security in Cloud Computing*. Springer, pp. 207–226.

Ludwig, A. and Schmid, S. (2015) 'Distributed cloud market: Who benefits from specification flexibilities?', *ACM SIGMETRICS Performance Evaluation Review*, 43(3), pp. 38–41.

Mahmud, R., Kotagiri, R. and Buyya, R. (2018) 'Fog computing: A taxonomy, survey and future directions', in *Internet of everything*. Springer, pp. 103–130.

Mohammed, C. M. and Zebaree, S. R. M. (2021) 'Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review', *International Journal of Science and Business*, 5(2), pp. 17–30.

Nguyen, T.-D. *et al.* (2018) 'Mobile Services Meet Distributed Cloud: Benefits, Applications, and Challenges', *Mobile Computing: Technology and Applications*, p. 39.

Oza, N. *et al.* (2013) 'Identifying potential risks and benefits of using cloud in distributed software development', in *International Conference on Product Focused Software Process Improvement*. Springer, pp. 229–239.

Rani, D. and Ranjan, R. K. (2014) 'A comparative study of SaaS, PaaS and IaaS in cloud computing', *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(6).

Rashid, Z. N. *et al.* (2018) 'Distributed cloud computing and distributed parallel computing: A review', in *2018 International Conference on Advanced Science and Engineering (ICOASE)*. IEEE, pp. 167–172.

Sarmenta, L. F. G. (2001) 'Volunteer computing'. Massachusetts Institute of Technology.

Satyanarayanan, M. (2017) 'The emergence of edge computing', *Computer*, 50(1), pp. 30–39.

Shaheen, M. Y. (2021a) 'Adoption of machine learning for medical diagnosis'.

Shaheen, M. Y. (2021b) 'AI in Healthcare: medical and socio-economic benefits and challenges'.

Shaheen, M. Y. (2021c) 'Applications of Artificial Intelligence (AI) in healthcare: A review'.

Shi, W. *et al.* (2016) 'Edge computing: Vision and challenges', *IEEE internet of things journal*, 3(5), pp. 637–646.

Shi, W. and Dustdar, S. (2016) 'The promise of edge computing', *Computer*, 49(5), pp. 78–81.

Singh, S. and Jangwal, T. (2012) 'Cost breakdown of public cloud computing and private cloud computing and security issues', *International Journal of Computer Science & Information Technology*, 4(2), p. 17.

Uriarte, R. B. and DeNicola, R. (2018) 'Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards', *IEEE Communications Standards Magazine*, 2(3), pp. 22–28.