Authors: Ahmad AlTwaijiry[1]
Affiliations: Saudia Arabia[1]
Orcid ids: 0000-0001-7672-3158[1]
Contact e-mail: yikiroh535@gyn5.com

DOI: 10.14293/S2199-1006.1.SOR-.PPEYYII.v1
Preprint first posted online: 15 November 2021

Cloud Computing Present Limitations and Future Trends

Ahmad AlTwaijiry

2021

Abstract

Cloud computing is still in its early stage. There are several companies, both big and small, that provide a diverse range of cloud-based services. There are several types of apps, such as complete programs, support services, mail filtering services, and storage services. IT professionals have become used to using some of the many cloud-based services as business requirements required. Cloud computing aggregators and integrators, on the other hand, are already developing, providing bundles of goods and services as a single point of access to the cloud. This research attempts to explore the current limitations and future trends of cloud computing. More specifically, this research discusses current limitations such as limited control, Cloud outage, Vendor lock-in, Cloud security, Energy consumption and the future trends to combat these limitations such as Edge computing, Hybrid and Multi-Cloud solutions, green cloud computing, serverless computing.

1. Introduction

Historically, the word "cloud" has been used to refer to the Internet (Dikaiakos *et al.*, 2009). This use originated with its frequent representation in network diagrams as an outline of a cloud, which was used to show the transfer of data over carrier backbones (which controlled the cloud) to an endpoint location on the other side of the cloud. This notion stems all the way back to 1961, when Professor John McCarthy stated that time-sharing technology may pave the way for a future in which computing power and even individual programs could be marketed through a utility-style business model (Walden, 2011). This concept gained popularity in the late 1960s, but by the mid-1970s, it had waned in popularity as it became evident that the then-current IT-related technologies were incapable of supporting such a future

computer architecture. However, the notion has been reinvigorated since the turn of the century. Cloud computing became popular in technical circles during this period.

Due to the fact that consumers often do not own the infrastructure utilized in cloud computing environments, they may save capital investment and only pay for what they use. Numerous cloud computing products follow the utility computing and billing model, while others charge a membership fee (Rajan, 2013). By pooling computer resources across several users, usage rates are often increased significantly, since cloud computing servers are not idle due to inactivity. This element alone may dramatically cut infrastructure expenses and expedite application development. A benefit of this paradigm is that it significantly boosts computer capacity, since customers are no longer need to construct their applications for peak periods, when processing burdens are highest. Cloud computing use has also been facilitated by the growing availability of high-speed internet. However, with more enabling, there are additional considerations to address, most notably legal ones.

Clouds may quickly and dynamically provide IT resources to cloud consumers, on-demand or through the cloud consumer's direct configuration, by offering pools of IT resources and tools and technologies to use them collectively (Hashem *et al.*, 2015) (AlTwaijiry, 2020b). This enables cloud customers to automatically or manually scale their cloud-based IT resources to suit processing variations and peaks. Similarly, when processing needs drop, cloud-based IT resources may be released.

The primary obstacles these businesses confront are safe data storage, high-speed Internet connection, and standardization. Storing vast volumes of data relating to user privacy, identification, and application-specific preferences in centralized places presents several data security risks (Wei and Blake, 2010) (Dillon, Wu and Chang, 2010). These problems, in turn, raise concerns about the legal structure that should govern a cloud-based system. Cloud computing services cannot be broadly accessible without high-speed Internet connectivity (AlTwaijiry, 2020a). Finally, the technical standards governing the implementation of the many computer systems and applications required to make cloud computing function have not been fully established, evaluated publicly, and confirmed by an oversight organization (Popović and Hocenski, 2010). Even the newly formed consortiums must overcome this barrier at some point, and until they do, development on new goods is likely to be slow.

Apart from the issues described earlier, cloud computing's dependability has been a point of contention in current technological circles. Due to the public nature of a cloud environment, issues that arise there attract a great deal of public attention.

2. Current Limitations

2.1 Limited control

Cloud services adhere to the highest level of control since they serve as the base around which TOS providers construct their infrastructure and applications (Chauhan and Vermani, 2016). TOS providers retain control over the platform's frontend architecture; information, data, and applications; but have limited influence over the platform's backend infrastructure (Rong, Nguyen and Jaatun, 2013). Though this is not considered detrimental to any of the parties involved, but rather results in a beneficial relationship in which responsibility is divided according to each party's capabilities, with cloud providers facilitating data storage and the TOS provider offering terminals its cloud-based functionalities. Cloud computing generates a contradiction; its enhanced mobility necessarily equates to higher control over terminal data.

When obtaining a cloud-based TOS, the only actual hazard that demands immediate attention is when planning and administration are inadequate. Only firms who fail to match their IT strategy with their business goals will suffer cloud computing's disadvantages. Failure to accurately show the regions of inefficiency in a terminal makes it difficult to determine the optimal TOS for cloud computing (Kesan, Hayes and Bashir, 2013).

A few established firms are concerned that adopting a cloud architecture may expose their data and information to security threats (Sabahi, 2011). This element continues to be the primary impediment to businesses working at their highest possible level of efficiency. Cloud computing is depicted as a liability when corporations make rash choices, resulting in a cascading effect that escalates into increasingly serious and dangerous concerns. For example, if a terminal adopts a TOS with forged cloud infrastructure and fails to scale resources appropriately, expenditures would skyrocket while profits will plummet. Investing in a multi-vendor approach is also a bad management choice since it results in needless expenditures associated with deviating from vendor lock-in (Silva, Costa and Oliveira, 2013).

Historically, a TOS was chosen based on the efficiency of the products that powered applications and data, as well as the number of discounts included in business agreements. However, maritime terminals have the challenge of identifying the ideal design system for the

functioning of their port. Diversifying computing workloads between suppliers is motivated by the threat of service interruption and data lock-in. Waze, the well-known GPS program, exemplifies this by running its apps concurrently on Google Cloud Platform and Amazon Web Services to ensure their survivability in the event of a DNS DDOS assault, regional failure, or even worldwide collapse of an entire cloud provider (Arthur, 2017). Though utilizing a multi-vendor approach is not financially feasible due to the high cost and resource requirements associated with devoting resources to several cloud platforms, which necessitates extra staff training. As a result, marine terminals must identify and review their business goals to ensure that they are tightly coupled to the cloud architecture they want to employ.

Being responsive to new and emerging trends in technology enables terminals to seek out more efficient ways to handle their resources, allowing them to continue succeeding financially and operationally. Recently, the wave of a TOS Cloud has prompted ports and marine terminals to reorganize their operations and migrate to cloud infrastructure. However, a terminal must undertake comprehensive research and take appropriate precautions to choose the optimum solution that will result in a rise in return on investment, reduced operating expenditures, and overall operational efficiency (Bauer, 2018).

2.2 Cloud outage

The term "Cloud Outage" refers to the period of time during which the cloud infrastructure service is unavailable for usage (Chen *et al.*, 2019). The term "unavailability" may also refer to the service's insufficiency in terms of performance as measured by the established SLA criteria (Baset, 2012). For example, an event during which a data center had just a partial outage may prompt the vendor to conduct appropriate repair and restoration actions. Until the service is completely restored in accordance with the negotiated SLA criteria, the end user may perceive it as downtime (Johnson, 2013) .

Numerous cloud services are possible to host in a cloud system, and each service is a large and complex system comprised of numerous components. Failures are inevitable in a sophisticated system owing to frequent component updates, changes in the operating environment, online fixes, and device mobility. Failures may significantly reduce system availability and result in a negative user experience (Jammal *et al.*, 2016). To manage failures, several system monitors and alerting systems are distributed across a cloud service system to determine whether or not a service is performing correctly.

Cloud outages may be caused by a variety of factors both within and without the control of the cloud provider. The following list summarizes the considerations that cloud suppliers do to guarantee that their services always meet their SLAs with adequate acceptability:

A power outage is one of the most frequent reasons of a cloud service going down. This is because the electric energy that supports the underlying datacenters is unavailable. Cloud suppliers operate on a vast scale by definition — a single datacenter may require tens to hundreds of megawatts of electricity, for which they often rely on the national grid or third-party power plants (Cérin *et al.*, 2013). This is a difficulty for datacenter firms in terms of ensuring constant access to appropriate energy, particularly when fast expansion and scalable market needs necessitate the use of scalable power sources, which are otherwise only accessible in limited quantities.

Cyber attacks: Cyberattacks such as Distributed Denial of Service (DDoS) overwhelm datacenters, preventing normal users from accessing the service through the same networking routes (Somani *et al.*, 2016). Despite robust security methods, hackers often exploit hidden flaws that cause protective mechanisms to isolate services from genuine users, leak data, or completely shut down the service.

Human Error: A single erroneous command may knock the whole IT infrastructure service down, despite the fact that strong processes and systems are in place to prevent such unanticipated failures (Bordnick *et al.*, 2009). This is possible even with the major cloud companies, as seen in 2017 when the worldwide Internet was down owing to a human mistake at an AWS data center location. While the systems detected the aberrant activity early enough, several of the afflicted datacenters' architecture needed a complete repair and restart.

Cloud infrastructure is a sophisticated combination of hardware and software technologies. Glitches and glitches are almost certain to occur in enterprise-grade datacenters that power businesses of all sizes and industries. These technological flaws may be missed or stay unnoticed until they manifest as a service outage affecting end customers. When a remedy to these difficulties is not immediately evident or relevant, the service may stay unavailable.

Networking Issues: Cloud suppliers may collaborate with telecommunications service providers and government agencies that operate long-distance communication networks. Issues relating to networks outside the organization, particularly across borders, may be beyond the service provider's control, particularly in terms of addressing a connection issue. Cloud suppliers and users alike depend on their telecommunications partners to guarantee service is

restored in this event (Potharaju and Jain, 2013). To overcome this constraint, the majority of large-scale cloud suppliers operate internationally in various countries and are capable of dynamically balancing workloads across geographically dispersed datacenters. This enables the business to continue providing the service to end customers even if repairing the networking difficulties is beyond their internal controls.

Cloud suppliers are accountable for the operation, maintenance, and administration of their information technology infrastructure. End customers only pay for the services they utilize, while suppliers continuously invest in service enhancement. This cover planned and unplanned maintenance and improvements. Maintenance procedures may entail service interruptions, workload transfers across datacenters, or general repairs that need a complete system restart (Chen *et al.*, 2019). The service may stay inaccessible to end customers throughout this time period.

Without a doubt, the cloud underlies technologies that enable efficient company operations. However, extended cloud disruptions impair internet services and have a significant negative effect on customer service and corporate income. Businesses must be prepared for unexpected interruptions with a robust recovery strategy and increase their reliance on a hybrid cloud approach.

2.3 Vendor lock-in

Vendor lock-in occurs when a consumer who is utilizing a product or service is unable to readily switch to a competitor's product or service (De Oliveira, Martins and Simao, 2017). Vendor lock-in is often the outcome of incompatible proprietary technology with those of rivals. However, it may also be a result of inefficient procedures or contractual restraints. In other context, vendor lock-in occurs when the cost of switching vendors is so high that the client is effectively trapped with the original vendor. Due to budgetary constraints, an inadequate staff, or the desire to minimize business disruptions, the client becomes "locked in" to an inferior product or service (Silva, Rose and Calinescu, 2013).

Numerous events might have a detrimental influence on a corporation that is tied into a certain cloud vendor: If a vendor's quality of service deteriorates or never reaches a desirable level, the customer is stuck with it. Additionally, the vendor may radically alter their product offerings to the point where they no longer fit the demands of a firm. A vendor may cease operations entirely. Finally, a vendor may unilaterally raise the price of a service, knowing that its customers are locked in (Kratzke, 2014).

In general, outsourcing core, business-critical technology to an external vendor is difficult for any firm and demands a high level of confidence in the vendor.

Fear of vendor lock-in is often highlighted as a significant barrier to cloud service adoption. Due to the complexity of cloud service migration, many clients continue to use a provider that does not fulfill their demands in order to avoid the lengthy process (Opara-Martins, Sahandi and Tian, 2014). To migrate data from one cloud provider to another, for example, it is often required to first transfer the data back to the customer's site and then to the new provider's environment. Additionally, the data may have been changed to ensure compliance with the original provider's system, requiring that what is returned to the client be restored to its original condition before being transferred again.

2.4 Cloud security

Cloud security, sometimes referred to as cloud computing security, is a collection of rules, controls, procedures, and technologies that work together to safeguard cloud-based systems, data, and infrastructure (Onwubiko, 2010). These security measures are designed to safeguard cloud data, ensure regulatory compliance, and safeguard the privacy of consumers, as well as to establish authentication criteria for particular users and devices. From access authentication to traffic filtering, cloud security may be adjusted to meet the specific demands of the organization. Additionally, since these rules can be established and maintained centrally, administrative costs are decreased, freeing up IT staff to concentrate on other aspects of the company.

As corporate cloud usage expands, business-critical apps and data transfer to trusted third-party cloud service providers (CSPs). While the majority of large CSPs provide basic cybersecurity tools with monitoring and alerting capabilities as part of their service offerings, in-house information technology (IT) security employees may discover that these tools do not provide sufficient coverage, implying that cybersecurity gaps exist between what the CSP offers and what the company needs (Allen, Puchaty and Zoghi, 2021). This raises the danger of data theft and loss.

While various users may use a cloud-based data center, it may be just as secure as a corporate data center. As a result of the previously described lack of control, there is a notion that Public Cloud is less secure. This, in the author's view, is a red herring, since extra precautions such as encrypting one's data in the Cloud and also every virtual machine operating on a multi-tenanted server, with keys kept separately, may be taken.

Because no company or CSP can eradicate all security risks and vulnerabilities, business executives must weigh the advantages of embracing cloud services with the degree of data security risk their enterprises are prepared to incur.

Organizations are increasingly recognizing the many commercial advantages of migrating their systems to the cloud. Cloud computing enables businesses to operate at scale, decrease technological expenses, and use flexible systems to gain a competitive advantage (Choo, 2010). However, enterprises must have total trust in their cloud computing security and in the protection of all data, systems, and applications against theft, leakage, corruption, and deletion.

2.5 Energy consumption

Modern data centers, which operate on the Cloud computing paradigm, serve a diverse range of applications, from those that run for a few seconds (e.g. providing requests for online applications such as ecommerce and social networking portals) to those that run for an extended amount of time (e.g. simulations or large dataset processing) (Buyya, Beloglazov and Abawajy, 2010) (Chen, Xie and Li, 2018). Cloud Data Centers are energy inefficient. It is responsible for the worldwide growth in energy use and, therefore, energy costs.

Nowadays, the incipient software that is being utilized consumes an increasing amount of electricity each year (Chen *et al.*, 2012). Several of them demand near-constant access to the hard disk, which consumes more power than previous software did.

The data centers that host cloud applications often use a large amount of electrical energy, resulting in an increase in operating costs and increased CO2 emissions. Cloud service providers must take steps to guarantee that their profit margins do not suffer significantly as a result of increased energy expenses (Chen *et al.*, 2011) (Chen *et al.*, 2011). Reduce data center energy consumption is a difficult and complicated problem because computer applications and data are expanding at such a rapid rate that bigger servers and disks are required to process them rapidly enough within the necessary time period.

3. Future trends

3.1 Edge computing

Edge Computing provides data analysis, processing, and transmission at the network's edge. That is, the data is analyzed locally, closer to its storage location, in real time and with no delay

(Shi and Dustdar, 2016). Edge computing enables the analysis of data from Internet of Things devices at the network's edge before it is sent to a data center or cloud.

Due to the allure of edge computing, cloud architects may want to shift as many workloads as possible to the edge. However, they should evaluate the structure, performance needs, and security implications of each application, among other aspects (Satyanarayanan, 2017) (Bilal *et al.*, 2018).

There are two distinct architectures for edge computing. When determining if an edge computing model is a good match, the first thing to consider is the available architecture. There are two primary categories: The first is edge computing, which processes data directly on client devices (Khan *et al.*, 2019) (Atieh, 2021). The second form is cloud-edge computing, which processes data on edge hardware located nearer to client devices than centralized cloud data centers.

The device-edge approach is effective if the client devices are competent of uniformly managing the processing load (Wen, Ren and Sangaiah, 2018). While standard PCs and laptops are capable of this, low-power Internet of Things sensors may lack the computation and storage capacity required to analyze data effectively.

Additionally, implementing a device-edge model might be challenging if the users are dependent on a variety of various kinds of edge devices and operating systems, each of which may have a unique set of capabilities and settings (Li, Zhou and Chen, 2018).

With the cloud-edge approach, end-user devices play a minor role in the architecture's design. The sort of device end users utilize is irrelevant if a cloud edge computing architecture is adopted. Typically, these servers are housed in a data center closer to end customers than the central cloud.

3.2 Hybrid and Multi-Cloud Solutions

The term "hybrid" refers to anything that is of mixed origin or composition. In other words, it is anything that is constructed from a variety of different elements. Multi-cloud is a rather straightforward term that refers to the use of many cloud computing services (Hong *et al.*, 2019).

What organizations want today more than ever is the ability to safely install, operate, and manage their data and applications on the cloud of their choice—without fear of being locked in (Yasrab and Gu, 2016).

This is precisely the value proposition that a hybrid multi-cloud strategy provides to major enterprises. It provides businesses with the freedom and flexibility to host their own software one day, migrate to a cloud provider the next, and maintain the ability to switch cloud providers in the future.

Cloud computing evolved from the utility computing notion. It started with the distinction between dedicated resources and shared resource platforms. Businesses have embraced cloud computing platforms of various types, including private, public, hybrid, and hybrid multicloud.

A hybrid multicloud, in the simplest terms, is the combination of hybrid cloud and multicloud architectures, as shown in figure 1.

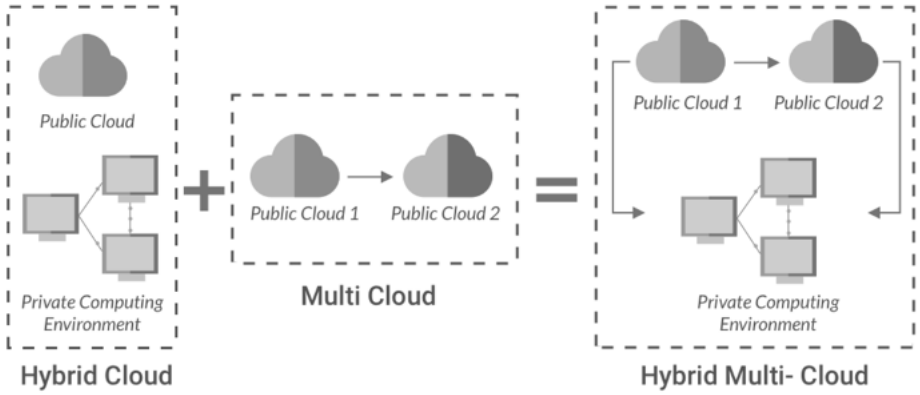


Figure 1. Hybrid cloud and multicloud architecture

Additionally, a hybrid multicloud model enables businesses to adopt standard management and software development capabilities that span all of their locations—whether public cloud, private cloud, or on-premises (Benmerzoug, 2013). This is particularly critical in light of the fact that computing is now conducted in a variety of locations.

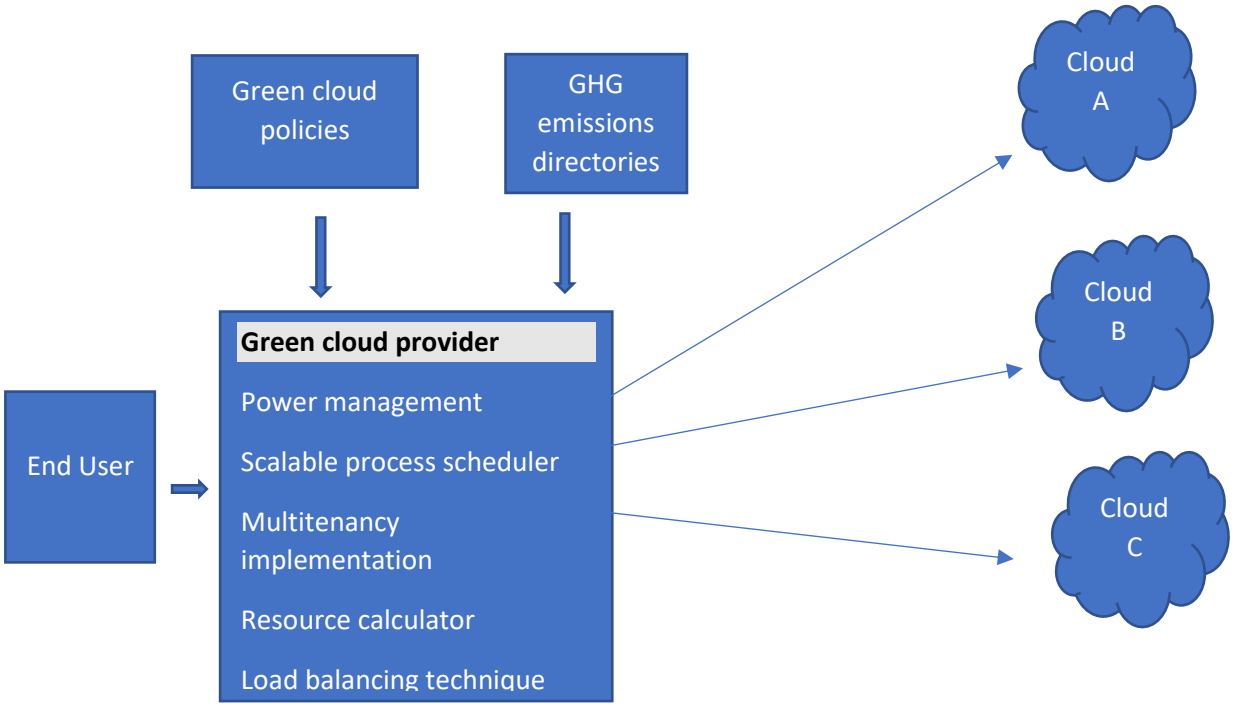
Hybrid multicloud is a significant potential with far-reaching implications for the industry as a whole. The stakes are quite high for corporations. Every business is, in effect, becoming into a technology business. Information technology has advanced to the point where it is almost hard to discern between a successful organization's business and IT strategies (Hong *et al.*, 2019).

Having said that, the rising relevance of hybrid multicloud represents a once-in-a-generation opportunity for businesses to break free from vendor lock-in and, more significantly, to unleash the maximum potential of the cloud (Raj and Raman, 2018).

Additionally, a hybrid multicloud solution extends the advantages of a public cloud to other components of an organization's IT ecosystem. It enables businesses to have insight and control over their whole infrastructure, enabling them to conduct business and introduce new technologies in a far more secure and efficient way.

3.3 Green cloud computing

Data centers are costly to operate and have a negative impact on the environment. Energy expenses and carbon emissions are high because large quantities of electricity are required to operate and cool the many servers housed in these data centers (Baliga *et al.*, 2010) (Patel, Mehrotra and Soner, 2015). Cloud service providers must take steps to guarantee that their profit margins do not suffer significantly as a result of increased energy expenses. For example, Google, Microsoft, and Yahoo are constructing massive data centers in the desolate desert terrain bordering the Columbia River in the United States of America in order to take use of cheap and dependable hydroelectric power (Xiong, Han and Vandenberg, 2012) (Atrey, Jain and Iyengar, 2013). Additionally, governments worldwide are under growing pressure to minimize their carbon footprints, which have a huge influence on climate change. For instance, the Japanese government formed the Japan Data Center Council to address the data center industry's growing energy usage (Buyya, Beloglazov and Abawajy, 2010) (Xiong, Han and Vandenberg, 2012).



It has been acknowledged that massive amounts of natural resources are used in the manufacture of desktop computers. They get an enormous quantity of energy, but half of it is squandered, with the other half being consumed by the computers. Power management measures should be applied to ensure that they make the best possible use of the energy provided (Patel, Mehrotra and Soner, 2015). The primary constraint is the high cost of the components necessary to improve the efficiency of cloud computing. The simulator's efficiency is difficult to replicate in practice. Additionally, the data center's upkeep of the equipment is a constraint. The infrastructure of data centers is one of the most challenging difficulties facing the information technology ecosystem. With the progress of technology, it is vital to prioritize resource management and equipment cooling. Another significant concern is carbon footprints, which are exacerbated by the massive quantity of electricity and power required, as well as the cooling mechanisms necessary to keep the servers cool (Xiong, Han and Vandenberg, 2012). There are several methods to become green in cloud computing. However, getting service providers to adopt and invest in such approaches is a challenge. This is because service providers anticipate rapid results, which are often not achievable immediately after using green cloud computing solutions. It takes time for the outcomes and advantages of it to become apparent (Atrey, Jain and Iyengar, 2013) (Radu, 2017).

3.4 Serverless computing

Serverless computing is an approach where code processing is totally controlled by a cloud provider, instead of the conventional way of designing programs and installing them on servers (Baldini *et al.*, 2017).

It implies developers don't have to concern about managing, procuring and maintaining servers when delivering code. Previously a developer would have to determine how much storage and database capacity would be required pre-deployment, slowing the entire process down (Adzic and Chatley, 2017).

Serverless computing enables developers to acquire backend services on a flexible 'pay-as-you-go' basis, requiring them to pay for only the services they utilize. This is analogous to moving from a monthly fixed-limit mobile phone data plan to one that costs only for the data that is actually consumed (Hellerstein *et al.*, 2018).

The term 'serverless' is rather deceptive, since these backend services are still provided by servers, but the vendor handles all server space and infrastructure problems. Serverless implies that developers can work without worrying about server (Taibi, Spillner and Wawruch, 2020)s.

The benefits that serverless computing offer are:

Reduced expenses - Serverless computing is often very cost efficient, since conventional cloud providers' backend services (server allocation) sometimes charge the customer for excess space or CPU time (Lee, Satyam and Fox, 2018).

Scalability is simplified - Developers that use serverless architecture do not have to worry about scaling up their code. The serverless vendor is responsible for all on-demand scalability .

Simplified backend code - With FaaS, developers may construct simple functions that execute a single task independently, such as calling an API (Sewak and Singh, 2018).

5. Conclusion

Each new technology is introduced with the promise of resolving the faults of previous ones. Over the last several decades, traditional computing has played a critical role in the fields of computing and communication. Given that cloud computing is being positioned as the replacement to conventional computing systems, it would be prudent to first acknowledge the shortcomings of traditional computing ways before delving into the cloud computing topic.

In the past several decades, computing and information technology (IT) have altered the character and extent of human civilization. There was a time, almost half a decade ago, when companies operated only via the use of the pen, paper, telephone, and fax machine. Computer systems gradually encroached on human procedures and began automating them. Pen and paper were phased out in favor of digital communication, and even phone and fax services were taken over by computers.

At the moment, companies of all sizes, from little to large, rely on computer systems for practically everything they do. Individuals, too, rely extensively on computer systems to carry out their daily duties. IT and computing are crucial aspects in today's world, and life is unimaginable without constant, simple access to computer systems.

Access to computer facilities that are both convenient and affordable has become a need for everyone. However, a cursory examination of the usual applications of computer technology presents various difficulties.

Since its beginning in 1999, cloud computing has grown at a breakneck pace and adapted to current trends. Cloud computing is also projected to accelerate in the future, eventually becoming one of the most trustworthy and modern technologies for data storage. Cloud computing is appealing because of its portability, security, and ease of use.

Over the years, computing technology has progressed. Over the previous decade, there has been consistent progress in the fields of computer hardware, software architecture, web technology, and network communications. The speed of internet connections has grown daily, and they have also gotten more affordable. All of these breakthroughs paved the way for the groundbreaking notion of 'cloud computing' to be introduced.

One of the primary benefits of edge computing is that data processing occurs at a more local level, taking less time and resulting in a shorter latency time for the device, and hence the user. Edge computing is particularly advantageous for IoT devices, such as smart house hubs, since it enables faster response times to user queries by eliminating the need for data to travel to and from a remote cloud data center.

Cloud computing is likely to make a significant leap forward in the near future, assisting firms in flourishing and expanding. Integral Choice is the market leader in cloud computing solutions for organizations of all sizes.

References

Adzic, G. and Chatley, R. (2017) ‘Serverless computing: economic and architectural impact’, in *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering*, pp. 884–889.

Allen, A., Puchaty, E. and Zoghi, B. (2021) ‘Challenges Cybersecurity Architects Are Facing In A Cloud Computing Environment’, *International Journal of Computer Science and Information Security (IJCSIS)*, 19(6).

AlTwaijiry, A. (2020a) ‘Impact of cloud deployment on operational expenses of healthcare centers’, *Empirical Quests for Management Essences*, 1(1), pp. 1–9.

AlTwaijiry, A. (2020b) ‘The Determinants of Cloud Computing Adoption in Healthcare’, *ResearchBerg Review of Science and Technology*, 1(1), pp. 9–20.

Arthur, E. (2017) ‘Strategic Decision Making: Google’s Acquisitions, Partnerships and the “Toothbrush Test”’, in *The 15th Annual Conference on Telecommunications and Information*

Technology, pp. 1–11.

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/.

Atrey, A., Jain, N. and Iyengar, N. (2013) 'A study on green cloud computing', *International Journal of Grid and Distributed Computing*, 6(6), pp. 93–102.

Baldini, I. *et al.* (2017) 'Serverless computing: Current trends and open problems', in *Research advances in cloud computing*. Springer, pp. 1–20.

Baliga, J. *et al.* (2010) 'Green cloud computing: Balancing energy in processing, storage, and transport', *Proceedings of the IEEE*, 99(1), pp. 149–167.

Baset, S. A. (2012) 'Cloud SLAs: present and future', *ACM SIGOPS Operating Systems Review*, 46(2), pp. 57–66.

Bauer, E. (2018) 'Improving operational efficiency of applications via cloud computing', *IEEE Cloud Computing*, 5(1), pp. 12–19.

Benmerzoug, D. (2013) 'An agent-based approach for hybrid multi-cloud applications', *Scalable Computing: Practice and Experience*, 14(2), pp. 95–110.

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.

Bordnick, P. S. *et al.* (2009) 'Reactivity to cannabis cues in virtual reality environments', *Journal of psychoactive drugs*, 41(2), pp. 105–112.

Buyya, R., Beloglazov, A. and Abawajy, J. (2010) 'Energy-efficient management of data center resources for cloud computing: a vision, architectural elements, and open challenges', *arXiv preprint arXiv:1006.0308*.

Cérin, C. *et al.* (2013) 'Downtime statistics of current cloud solutions', *International Working Group on Cloud Computing Resiliency, Tech. Rep*, 1, p. 2.

Chauhan, S. and Vermani, S. (2016) 'Cloud Computing to Fog Computing: A Paradigm Shift', *Journal of Applied Computing*, 1(1), pp. 25–29.

Chen, F. *et al.* (2012) 'An energy consumption model and analysis tool for cloud computing environments', in *2012 First International Workshop on Green and Sustainable Software*

(GREENS). IEEE, pp. 45–50.

Chen, Q. *et al.* (2011) 'Profiling energy consumption of VMs for green cloud computing', in *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing*. IEEE, pp. 768–775.

Chen, Y. *et al.* (2019) 'Outage prediction and diagnosis for cloud service systems', in *The World Wide Web Conference*, pp. 2659–2665.

Chen, Y., Xie, G. and Li, R. (2018) 'Reducing energy consumption with cost budget using available budget preassignment in heterogeneous cloud computing systems', *IEEE Access*, 6, pp. 20572–20583.

Choo, K.-K. R. (2010) 'Cloud computing: Challenges and future directions', *Trends and Issues in Crime and Criminal justice*, (400), pp. 1–6.

Dikaiakos, M. D. *et al.* (2009) 'Cloud computing: Distributed internet computing for IT and scientific research', *IEEE Internet computing*, 13(5), pp. 10–13.

Dillon, T., Wu, C. and Chang, E. (2010) 'Cloud computing: issues and challenges', in *2010 24th IEEE international conference on advanced information networking and applications*. Ieee, pp. 27–33.

Hashem, I. A. T. *et al.* (2015) 'The rise of "big data" on cloud computing: Review and open research issues', *Information systems*, 47, pp. 98–115.

Hellerstein, J. M. *et al.* (2018) 'Serverless computing: One step forward, two steps back', *arXiv preprint arXiv:1812.03651*.

Hong, J. *et al.* (2019) 'An overview of multi-cloud computing', in *Workshops of the International Conference on Advanced Information Networking and Applications*. Springer, pp. 1055–1068.

Jammal, M. *et al.* (2016) 'Mitigating the risk of cloud services downtime using live migration and high availability-aware placement', in *2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE, pp. 578–583.

Johnson, J. A. (2013) 'Optimization of migration downtime of virtual machines in cloud', in *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*. IEEE, pp. 1–5.

Kesan, J. P., Hayes, C. M. and Bashir, M. N. (2013) ‘Information privacy and data control in cloud computing: Consumers, privacy preferences, and market efficiency’, *Wash. & Lee L. Rev.*, 70, p. 341.

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

Kratzke, N. (2014) ‘Lightweight virtualization cluster how to overcome cloud vendor lock-in’, *Journal of Computer and Communications*, 2(12), p. 1.

Lee, H., Satyam, K. and Fox, G. (2018) ‘Evaluation of production serverless computing environments’, in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE, pp. 442–450.

Li, E., Zhou, Z. and Chen, X. (2018) ‘Edge intelligence: On-demand deep learning model co-inference with device-edge synergy’, in *Proceedings of the 2018 Workshop on Mobile Edge Communications*, pp. 31–36.

De Oliveira, R. R., Martins, R. M. and Simao, A. D. S. (2017) ‘Impact of the vendor lock-in problem on testing as a service (TaaS)’, in *2017 IEEE International Conference on Cloud Engineering (IC2E)*. IEEE, pp. 190–196.

Onwubiko, C. (2010) ‘Security issues to cloud computing’, in *Cloud Computing*. Springer, pp. 271–288.

Opara-Martins, J., Sahandi, R. and Tian, F. (2014) ‘Critical review of vendor lock-in and its impact on adoption of cloud computing’, in *International Conference on Information Society (i-Society 2014)*. IEEE, pp. 92–97.

Patel, Y. S., Mehrotra, N. and Soner, S. (2015) ‘Green cloud computing: A review on Green IT areas for cloud computing environment’, in *2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE)*. IEEE, pp. 327–332.

Popović, K. and Hocenski, Ž. (2010) ‘Cloud computing security issues and challenges’, in *The 33rd international convention mipro*. IEEE, pp. 344–349.

Potharaju, R. and Jain, N. (2013) ‘When the network crumbles: An empirical study of cloud network failures and their impact on services’, in *Proceedings of the 4th annual Symposium on Cloud Computing*, pp. 1–17.

Radu, L.-D. (2017) ‘Green cloud computing: A literature survey’, *Symmetry*, 9(12), p. 295.

Raj, P. and Raman, A. (2018) ‘Multi-cloud management: Technologies, tools, and techniques’, in *Software-Defined Cloud Centers*. Springer, pp. 219–240.

Rajan, A. P. (2013) ‘Evolution of cloud storage as cloud computing infrastructure service’, *arXiv preprint arXiv:1308.1303*.

Rong, C., Nguyen, S. T. and Jaatun, M. G. (2013) ‘Beyond lightning: A survey on security challenges in cloud computing’, *Computers & Electrical Engineering*, 39(1), pp. 47–54.

Sabahi, F. (2011) ‘Cloud computing security threats and responses’, in *2011 IEEE 3rd International Conference on Communication Software and Networks*. IEEE, pp. 245–249.

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

Sewak, M. and Singh, S. (2018) ‘Winning in the era of serverless computing and function as a service’, in *2018 3rd International Conference for Convergence in Technology (I2CT)*. IEEE, pp. 1–5.

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

Silva, G. C., Rose, L. M. and Calinescu, R. (2013) ‘Towards a model-driven solution to the vendor lock-in problem in cloud computing’, in *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*. IEEE, pp. 711–716.

Silva, L. A. B., Costa, C. and Oliveira, J. L. (2013) ‘A common API for delivering services over multi-vendor cloud resources’, *Journal of Systems and Software*, 86(9), pp. 2309–2317.

Somani, G. *et al.* (2016) ‘DDoS attacks in cloud computing: Collateral damage to non-targets’, *Computer Networks*, 109, pp. 157–171.

Taibi, D., Spillner, J. and Wawruch, K. (2020) ‘Serverless computing-where are we now, and where are we heading?’, *IEEE Software*, 38(1), pp. 25–31.

Tong, A. (2021a) ‘Comparison of the fin-tech evergreen fund in China and USA’, *Available at SSRN 3904647*.

Tong, A. (2021b) ‘The possibility of a decentralized economy in China and the USA’.

Walden, D. (2011) ‘50th Anniversary of MIT’s Compatible Time-Sharing System’, *IEEE*

Annals of the History of Computing, 33(4), pp. 84–85.

Wei, Y. and Blake, M. B. (2010) 'Service-oriented computing and cloud computing: Challenges and opportunities', *IEEE Internet Computing*, 14(6), pp. 72–75.

Wen, J., Ren, C. and Sangaiah, A. K. (2018) 'Energy-efficient device-to-device edge computing network: An approach offloading both traffic and computation', *IEEE Communications Magazine*, 56(9), pp. 96–102.

Xiong, N., Han, W. and Vandenberg, A. (2012) 'Green cloud computing schemes based on networks: a survey', *Iet Communications*, 6(18), pp. 3294–3300.

Yasrab, R. and Gu, N. (2016) 'Multi-cloud PaaS architecture (MCPA): a solution to cloud lock-in', in *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*. IEEE, pp. 473–477.