

Review of cloud computing in science, technology, and real life

Ola Hussein Abd Ali Alzuabidi ^{1*}, Ban M. Alameri ²

¹ Dijlah University College, Computer Engineering Techniques, Iraq

² Department of Electrical Engineering, Faculty of Engineering, Mustansiriyah University, Iraq

*Corresponding author: ola.hussein@duc.edu.iq

© The Author

2021.

Published by

ARDA.

Abstract

This paper presents an overview of the general idea and history of cloud computing in theory. The objective of this review is to draw attention to preceding studies about cloud computing that have common characteristics with the theme of this paper. There were some points discussed in general, including the advantages of this technology, its subjects, security, and the effects of adopting cloud computing in an organization.

Keywords: Cloud computing, Technology, Security, Privacy, Real life

1. Introduction

There are various different definitions of the "cloud computing." The majority of them are solely concerned with technology difficulties. Cloud computing is a term that refers to a vast collection of varied software, hardware and other services that may be handled via "cloud" environment. Their whole resource base is available to them at any time and from any location. Normally, the cloud provider's service is sold on a pay-per-use basis. That is, it demonstrates a high degree of adaptability in the use of these services as new resources that are always available.

This methodology is the most overvalued and effective strategy for dynamically increasing capabilities or capacity without requiring new infrastructure in all disciplines of engineering, business, and other sciences [1].

U.S. National Institute of Standards and Technology defines cloud computing as a way to provide users with instantaneous on-demand access to a shared pool of reconfigurable computing resources (such as servers and storage), which can arrive on-time with no disturbance or scalability.

Cloud computing as a concept emerged between 2004 and 2005. Prior to 1994, the cloud icon symbolized the Internet concept. When Amazon Web service (AWS) was founded in 2006 with the primary objective of providing utility computing, it developed the industry's fundamental concept of cloud computing. J.C.R. Licklider proposed the concept of an "intergalactic computer network" in the 1960s, while he was accountable with ARPANET (Advanced Research Projects Agency Network) promotion in 1969 [2].

Cloud services' virtualization, quick elasticity, widespread network connectivity, and better performance are the primary drivers of this technology's exponential growth. Typically, with ordinary "off-the-shelf" software packages, an application is installed on the organization's primary server and subsequently on each office computer [3].

1.1. Cloud architecture

When it comes to architecture, it's hard to tell how cloud computing is equivalent to or different from traditional accessible computing models, or how these equivalences or differences influence the management, functioning, and practical aspects of network and information security procedures. Fig. 1

This work is licensed under a [Creative Commons Attribution License](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>) that allows others to share and adapt the material for any purpose (even commercially), in any medium with an acknowledgement of the work's authorship and initial publication in this journal.



depicts the many types of cloud employment models. These are: public cloud, private cloud, and hybrid cloud models. Despite this, some cloud-based services, such as Community cloud and mobile cloud, are commercially viable [3, 4].

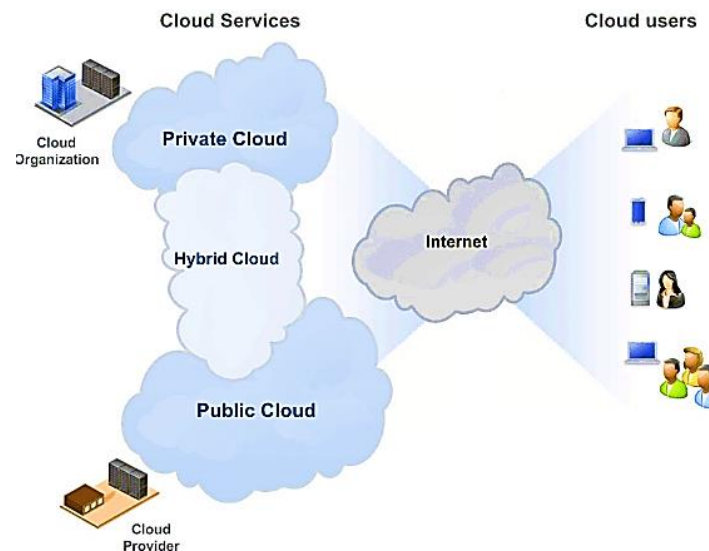


Figure 1. Important structural design of cloud

For example, a service provider may offer storage and other resources to the entire community for free or at a cost-per-use rate.

An internal or externally managed, domestically or externally hosted private cloud infrastructure is dedicated to one organization.

There are fewer security concerns when hosting mission-critical programs on private clouds for some enterprises. Private and public clouds can coexist in a hybrid cloud environment. When multiple clouds (private, communal, or public) are combined, they remain separate but are linked together, allowing for a wide range of deployment patterns to be used.

There are many enterprises that have common concerns (security, compliance, jurisdiction, etc.) and want to pool their computing resources to create a community cloud. This cloud can be managed internally or by a third-party, and it can be hosted on-site or in the cloud. However, because the costs are spread out over a larger number of users in a private cloud, only a part of the savings potential of cloud computing is realized. Using community cloud, multiple service providers work together to create an online community around a particular service.

The phrase "mobile cloud computing" refers to utilizing cloud computing services on mobile devices. Because of the availability of that on-demand right of entry, data and transactions are more freely held in reserve on the Internet than on device entities. An independent server controls mobile cloud applications, which are then sent to the user's device. In the worldwide mobile market, these applications represent a fast expanding segment.

2. Cloud based on delivery models

As indicated in Fig. 2, cloud computing servers establish three services defined primarily as Infrastructure as a service (IaaS), Software as a service (SaaS), and Platform as a service (PaaS). IaaS is the provision of computer infrastructure as a service, typically in the form of a platform virtualization environment. This core cloud computing approach provides processors and other resources in the form of considerable or generally virtual machines. While SaaS delivers applications to millions of clients via browser. It is frequently utilized in enterprise resource planning (ERP) systems and individual resource organization systems. Yahoo and Google are two applications that provide this type of service. Finally, PaaS provides a framework as a service layer upon which software applications can be built consistently and reliably. Forrester Research defines PaaS as an externally hosted service that provides a comprehensive framework for developing, managing, and activating applications. Cloud Foundry, Microsoft Azure, Amazon Elastic Beanstalk, Google App Engine, EngineYard, and Mendix are all examples of PaaS [5, 6].

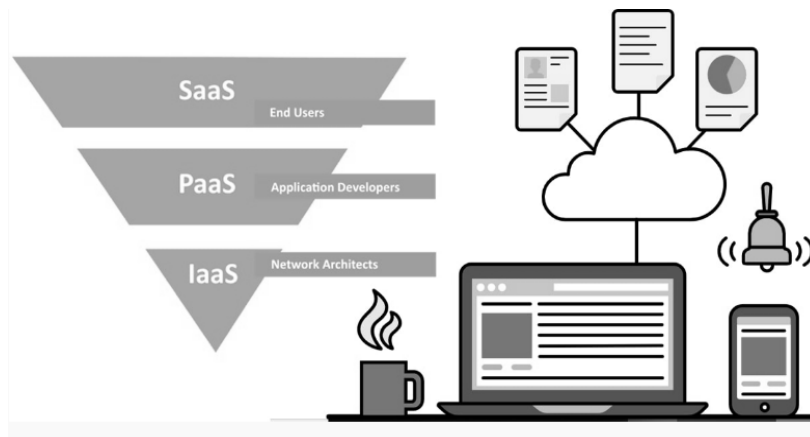


Figure 2. Delivery models of cloud services

In most cases, cloud computing consists of three fundamental components: servers, data centers, and clients [11]. They are all connected via the internet and are accessible as network setups.

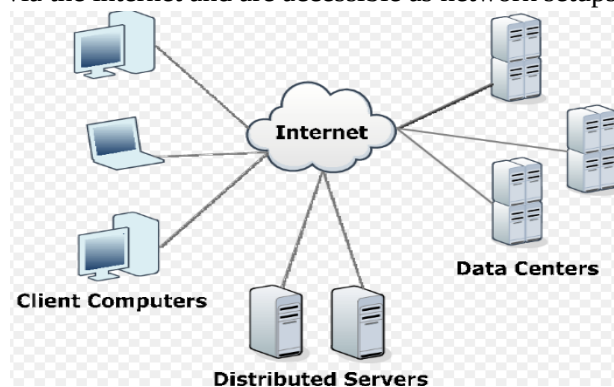


Figure 1. Straightforward cloud computing network

2.1. Data centers and distributed servers

Typically, data centers house the services that buyers desire at any time. They are typically a large room that contains all of the servers that provide these services and support their functioning. It is as well potential to incorporate virtual servers that reduce the overall number of physical servers and the resulting gap. Distributed servers are a term that refers to groupings of servers that are not physically located in the same location. There is no issue if these servers are compromised; as a user, you will perceive note no difference. Distributed servers offer more elasticity because their location and direct connectivity to the internet are irrelevant. There is an option to create a backup of other servers. Additionally, there are no constraints on the intensification of cloud service settings [11, 12].

2.2. Clients

Clients are typically represented by standard laptops or desktop PCs. Other types of clients are possible at the moment, including mobile phones (PDA). PDAs represent a significant amount of weight when it comes to cloud computing [9]. They offer significant mobility to anyone attempting to reach the cloud. As a general rule, there are three distinct types of clients to differentiate: thin, mobile and thick. Mobile clients are constantly accompanied by mobile phones. Thin clients are run on separate software and hardware. Whatever a user views, the server recognizes it, not his personal hard disk and operating system. In comparison, thick clients make use of their hard disks and access the cloud via a web browser on a frequent basis [11, 13].

2.3. Users

Naturally, users will appear after the clients. With no users, there is no reason for a cloud to be existent. Four distinct types of users can be classified using cloud technology [3,11]:

- Developers of web browser infrastructure - Providers of services

- Specialists in stipulation and integration

The cloud's (Internet-infrastructure) developers are the experts who expand and maintain the cloud. These developers should ensure the integrity of the connected services and build them completely [14]. Their responsibility is to provide an easy interface to end customers while keeping intricacy issues to a minimum.

Service authors or makers are quite distinct from developers, despite the fact that their tasks sometimes overlap. Whereas developers focus on providing all services, writers focus on entity services that may be used directly. However, if developers are not required to understand cloud technology patterns, they can focus only on providing acceptable flexibility to employ services [14].

Integration and provisioning specialists are now fully concentrated on end-user solutions. Their responsibilities include interacting with end users and attempting to meet their requirements. As previously said, the ultimate relevance is placed on the end user. They believe that their cloud services would have simple and uncomplicated interfaces, as well as sustainable and informational terms. Additionally, kids should be isolated from all potential hazards. As a result, it is critical to offer security in a cloud environment, as will be discussed more in this paper. These limits do not result in any divergence for these users. Numerous customers can sign up for cloud services in a matter of hours, or for years. These disparate end users must cobble together identical services, as they will likely incorporate identically critical data streams into the cloud. Additionally, the service is governed by a Service Level Agreement (SLA) [10,11].

The SLA is incorporated into the service agreement between the two parties. This agreement demonstrates that only one party is obligated to provide these types of services to the other. For example, it describes not just performance conformance but also security and safety compatibility.

As previously said, cloud computing consists of three layers: SaaS (software), PaaS (Platform), and IaaS (Infrastructure) (infrastructure). All of these acronyms conclude with the phrase "as a Service," implying that all tiers provide a variety of services to end consumers [5].

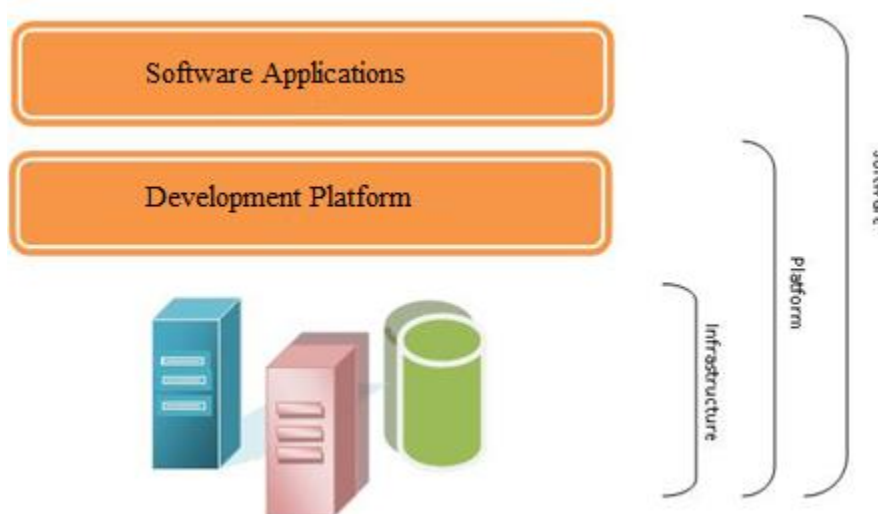


Figure 2. Outline of layers in cloud computing of SaaS, PaaS in addition to IaaS

3. Cloud computing in comparison with other technologies

The definition of cloud computing may overlap with that of other technologies. This section discusses the importance of appropriately defining cloud computing and its distinctions from other comparable technologies. Generally, these technologies predate cloud computing and are more well-known to the general public. As such, it is critical to distinguish it from cloud computing.

Autonomic computing systems are extremely likely to be involved in cloud computing. This computer structure is unique in terms of its operation mechanism. The goal of autonomous computing is to make systems available for autonomous work [15]. Specifically, they are capable of self-administration. They must coordinate and repair failures on their own. The autonomic computing system bears a strong resemblance to cloud computing in that it, too, utilizes large computer systems that are regulated at a higher level by humans.

The distinction between grid computing and cloud computing is more complex, although it is straightforward to understand. Grid computing concentrates on large-scale computation, while cloud computing offers services at both large and small sizes. Grid computing maintains a steady level of performance, but cloud computing's primary feature is that it provides performance as needed [16].

With a mainframe, an additional dissimilarity is obvious, but there are also some matches. A mainframe can be represented visually as a cloud. Nonetheless, it's logical that a mainframe grants access to staff employees in large organizations where the mainframe is completely central. That is where cloud computing, in addition to its performance, differs. While mainframes always deliver superior performance, cloud computing delivers it on-demand [7,8].

Additionally, the comparison was conducted using peer-to-peer technologies. The reason for this is that a whole cloud of users consists of both "clients" and "servers" [17], a distinction that is also significant. Clients do not perform any service provisioning in cloud computing.

The final comparison that will be made is with service-oriented computing. Off topic, cloud computing refers to service-oriented computing. Nonetheless, service-oriented computing places a greater emphasis on SaaS-based solutions. As previously said, cloud computing is focused on providing computer services regardless of their technique.

4. Cloud computing advantages

It is self-evident that cloud computing provides significant advantages to those who utilize it. This section will explain what these benefits essentially are. Typically, the benefits we emphasize are for the collection of end users. As previously said, the primary benefit for any end user is unquestionably the ease with which cloud computing can be implemented at any moment. It is an organism that operates on a pay-as-you-go basis. To begin, there is no significant space requirement for each piece of gear to be installed. Additionally, no maintenance is required for any of the hardware [11, 18].

It is the applications, not the technology, that enable the benefits to be realized. The cloud is teeming with ready-to-use applications, and even better, the data employed in these applications is at all times accessible from everywhere on the world [19].

An SLA verifies that quality evaluations are conducted prior to cloud access. These SLAs are critical for users and can result in increased maintenance costs if an association obtains all software and infrastructure on its own.

Not only are datacenters regarded an indirect advantage, but they are also critical since they are often located in specially designated places to reduce maintenance costs, particularly in low-income countries [19].

Concentrating deeper on cloud users reveals more tangible benefits. As is obvious at the moment, scalability is the primary benefit. As an organization anticipates a tipping point in its IT use, they simply get additional IT services from the cloud. This exemplifies the allure of cloud computing. It's quite simple; as large organizations engage in cloud computing, individuals can also imagine a high level of security [11].

As a result, cloud computing enables the grouping of financial and performance benefits. The financial benefit refers to the charges that must be paid when an association requires added IT services to achieve the performance benefits. Additional performance is gained when it is required and directly improves the association's performance.

5. Some concerns of cloud computing

The modern technologies may be accompanied by risks and unknown elements. Somewhat analogous to cloud computing. By definition, organizations that are heavily reliant on information technology outsource their operations. Several of them may be involved in their heart dealings. These associations are projected to face significant threats in the event that their analytical data is exposed to the exterior world under conditions of inadequate security. Additional problems regarding privacy and legal issues must be considered [3].

Catteddu [20] also distinguished between distinct risks and categorized them into four broad groups. There are three categories: technology difficulties (which are comparable to security issues), legal issues, and

organizational and policy challenges that are particularly relevant to vendors. These problems or issues are distinct from the previously discussed privacy concerns.

While legal difficulties vary by country, there is a general expectation that not every organization will be authorized to use public clouds. Clearly, there will be an increase in the use of private clouds. In the following discussion, privacy, technological, and security issues will be briefly discussed in light of their continued relevance to users [3].

Cloud computing security can be grouped into seven distinct categories. These threats are a representation of the customer's mentality. The association does not handle data. This logically generates a substantial amount of risk, as there is an appearance of subcontracting. This results in the association ceding any type of security to the subcontracting association [21, 22]. It is therefore critical for users to be familiar with risk management methods in advance. Ultimately, the user is still accountable. Providers must adhere to certain security standards, however these may be insufficient for anyone seeking to cause harm to an association. As such, it is critical to be aware with the methods followed by the supplier. Additionally, it is required for the user to protect the connection between the association and the provider.

As previously noted, the cloud's physical location is irrelevant [11]. As a result, as a purchaser, you will never be aware of the whereabouts of your information at any one time. They can include their services functioning in other countries that have their own legal difficulties. This can be generated in accordance with another nation's security rules, jeopardizing the association's operation in the cloud service environment.

Numerous associations can be run concurrently utilizing a single practical cloud. For instance, it's not difficult to imagine that when sixty disparate firms access the cloud, the data will become completely filled by all organizations.

This results in a slew of security concerns. For instance, if you are unaware of the location of your data, what would happen in the event of a natural disaster? The provider must have a back-up plan in place for when such calamities occur. These preceding concerns must be discussed with a cloud provider.

There must be challenges that cloud computing cannot address, such as determining who has right of entry on the provider side. The provider can determine which employees have access. They do not, however, have access control. Anyone with the association's login credentials can access the cloud and all of its data.

Numerous security subjects are likely to have incomplete privacy concerns. These concerns are highly logical since they are inextricably linked. The degrees of handled security resolve privacy in one way or another. As a result, it is ineffective to completely reclassify these subjects. Privacy concerns exist since the infrastructure is partially owned by a provider. Probably vital information, such as personal information, is distributed in the cloud environment since it is outside the association's screening range and is risky because they cannot identify who is accessing the cloud. They must obtain assurances from the provider that the right of entry is accessible and operated solely by authorized recruits.

An additional point of contention is how the cloud is operated; it is critical that not everyone has the same level of access to and visibility into all data in the cloud. The in chief administration requires information that is not required of a typical employee. Additionally, they should provide extra information terms. It is risky for any member of staff to be able to identify vital information from non-critical information, as this could be straightforwardly disclosed to the outside world [3, 11].

6. Security of cloud computing

Numerous issues remain unresolved in the debate on this subject. Pearson [23], using a dialogue model of many security problems, illustrates methodically the limits that must be considered in order to protect users and customers.

It is critical that the cloud has a high degree of transparency. Each user requesting access to the cloud must provide a rationale for the data they wish to access, how they intend to use it, and why they intend to use it. Without a doubt, the complete cloud user's activity must be verified and clarified. Without this level of control, data can simply be disclosed to competitors such as Pearson [23]. Additionally, users must only display information that is necessary to fulfill their requirements in this scenario. Additionally, it must provide no information other than that which is necessary to carry out the obsessions that a user desires, as determined by the user's category. All transactions conducted in a cloud environment must adhere to a data limit. Clearly

defined successes require only a specific data quantity with the possibility of predefinition. This restriction identifies who attempts to harm an association in the cloud environment. Following that, a linkage must be established, bordered by activities and data that must be fulfilled in the system. It would simply connect connected data to a certain cloud activity.

While consumers desire to be aware of their personal privacy, they must be able to discern between personal and non-personal data. Thus, it is not only necessary for personal data to be correct, but also for users to be unable to observe the personal data of other users. Finally, as previously indicated, there must be someone in charge of ensuring that everything occurs as planned. There should be certain jobs that verify that all routine actions are carried out by each and every user.

7. Cloud computing services in real life

To any extent, the cloud environment is not only a hypothetical understanding. It is currently being used by a variety of folks in addition to the expressive activities they engage in. For instance, consider social media platforms such as Facebook; it is one of the most widely used community media platforms and also makes use of cloud computing. As such, it qualifies as software as a service (SaaS). Each and every user on the Facebook platform can access their personal information using the "Facebook application." They do not, however, have the capacity to edit anything about this "program." As a result, the service provider retains complete control of the Facebook application [1-3, 24-25]. Another well-known and significant sample to discuss is Google Docs. It is feasible to produce a personal word, excel, or PowerPoint document through the online Google docs tool. At that point, this document is cached on the server. This server also saves any updates or alterations to this document. Google's word processing transactions are completely free and need no purchase. Google makes the term central processing unit available to anybody who want to utilize it. Additionally, the suitability of including personal papers in the word processor online and accessing it from any location. Additionally, there is the option to share papers with other users who access the cloud. In a cloud environment, other users have the ability to modify your documents if they have the necessary access. Together with the content you uploaded, they have real-time access to cloud-based word processing.

IBM and Amazon are two well-known cloud computing service providers. They provide comprehensive solutions that are more than just SaaS. Additionally, they provide infrastructure and Platform as a Service (PaaS). While Facebook and Google focused mostly on gratis (free) cloud computing services, Amazon and IBM offer extra absolute solutions. Their clients receive additional security care because their hub commerce is processed via cloud computing.

8. Conclusion

The cloud is a word that is frequently used to refer to the internet. Cloud computing refers to the capability of the internet to supply high-demand computing services like storage and processing power. Have you ever wondered where your Facebook posts or emails are kept? To be sure, it is the cloud. Cloud computing has a significant impact on our lives in numerous ways that we are unaware of. It has had a profound effect on not only our personal lives, but also on how corporates manage their data and consumers. Cloud computing has significantly improved our healthcare infrastructure and is quietly altering the technical lexicon.

The disadvantage is that customizing choices will be restricted. Cloud computing is less expensive owing to economies of scale, and – as with any outsourced activity – you frequently get what you pay for. Reduced selection at a significantly reduced price: this is a feature, not a bug. A cloud provider may not match your legal necessities and that firms must consider the benefits and hazards of cloud computing. Cloud computing limits the cloud vendor's control over the back end infrastructure. Frequently, cloud providers determine management policies that restrict what cloud users can do with their setting out. Cloud users' ownership and managing their programs, data, and services are likewise limited. This takes account of data limits, which are imposed on cloud users by cloud vendors when they allocate a quantity of bandwidth to each customer. These bandwidth allocations are frequently shared with other cloud customers.

References

- [1] L. Schubert, A. Tsitsipas, and K. Jeffery, "How cloud computing, IoT and multicore systems affect software engineering principles," in 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2018.
- [2] S. Juman TP, "Advantages and security challenges of cloud computing– overview," International Journal of Computer Science and Mobile Computing, vol. 9, no. 12, pp. 76–85, 2020.
- [3] J. Bakker, "The benefits of cloud computing in IT intensive organizations", Erasmus University Publisher, 2014.
- [4] D. Catteddu, "Cloud computing: Benefits, risks and recommendations for information security," in Web Application Security, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 17–17.
- [5] Cloud Computing – Demystifying SaaS, PaaS and IaaS by Cloudtweaks. Available at: <http://www.cloudtweaks.com/2010/05/cloud-computing-demystifying-saas-paas-and-iaas/> [Visited 05-10-2021]
- [6] P. Mell, T. Grance, "The Nist Definition of Cloud Computing", Recommendations of the National Institute of Standards and Technology, *NIST special publication, 2011 National Institute of standards and technology*, vol.145, no.6, 2009.
- [7] N. Cody, "Above the clouds," in Reflect & Write, New York: Routledge, 2021, pp. 89–89.
- [8] L. M. Vaquero, L. Roderio-Merino, J. Caceres, and M. Lindner, "A break in the clouds: Towards a cloud definition," Comput. Commun. Rev., vol. 39, no. 1, pp. 50–55, 2008..
- [9] R. Buyya, S. Pandey, and C. Vecchiola, "Cloudbus toolkit for market-oriented cloud computing," in Lecture Notes in Computer Science, Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 24–44.
- [10] C. Miyachi, "What is 'Cloud'? It is time to update the NIST definition?," IEEE Cloud Comput., vol. 5, no. 3, pp. 6–11, 2018.
- [11] N. Antonopoulos and L. Gillam, Eds., Cloud computing: Principles, systems and applications. Cham, Switzerland: Springer International Publishing, 2018.
- [12] T. Wood, S. Prashant, A. Venkataramani and M. Yousif, Black-box and Gray-box Strategies for Virtual Machine Migration, *4th USENIX Symposium on Networked Systems Design & Implementation*, pp.229-242, 2007.
- [13] E. Shih, P. Bahl, and M. J. Sinclair, "Wake on wireless: An event driven energy saving strategy for battery operated devices," in Proceedings of the 8th annual international conference on Mobile computing and networking - MobiCom '02, 2002.
- [14] M. A. Vouk, "Cloud computing — Issues, research and implementations," in ITI 2008 - 30th International Conference on Information Technology Interfaces, 2008.
- [15] S. R. White, J. E. Hanson, I. Whalley, D. M. Chess, and J. O. Kephart, "An architectural approach to autonomic computing," in International Conference on Autonomic Computing, 2004. Proceedings, 2004.
- [16] R. Buyya and M. Murshed, "GridSim: A toolkit for the modeling and simulation of distributed resource management and scheduling for grid computing," arXiv [cs.DC], 2002..
- [17] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," Comput. Commun. Rev., vol. 31, no. 4, pp. 149–160, 2001.
- [18] L. Wang et al., "Cloud computing: A perspective study," New Gener. Comput., vol. 28, no. 2, pp. 137–146, 2010.
- [19] C. Vecchiola, S. Pandey, and R. Buyya, "High-performance cloud computing: A view of scientific applications," in 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009.
- [20] D. Catteddu, "Cloud computing: Benefits, risks and recommendations for information security," in Web Application Security, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 17–17.

- [21] A. Yasar Arafath, "Cloud computing security and its challenges," *i-manag. J. Cloud Comput.*, vol. 7, no. 2, p. 20, 2020.
- [22] R. Hirschheim, A. Heinzl, and J. Dibbern, Eds., *Information systems outsourcing: Towards sustainable business value*. Berlin, Germany: Springer, 2016.
- [23] S. Pearson, "Taking account of privacy when designing cloud computing services," in *2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 2009.
- [24] T. Abd, Y. S. Mezaal, M. S. Shareef, S. K. Khaleel, H. H. Madhi, and S. F. Abdulkareem. "Iraqi e-government and cloud computing development based on unified citizen identification." *Periodicals of Engineering and Natural Sciences*, vol.7, no. 4, pp.1776-1793, 2019.
- [25] Y. S. Mezaal, et al., "Cloud computing investigation for cloud computer networks using clouddanalyzer", vol.96, no.20, pp. 6937-6947, 2018.