Cloud Services and Cloud Perspectives: A Review

Article *in* IOP Conference Series Materials Science and Engineering · March 2021

DOI: 10.1088/1757-899X/1090/1/012078

CITATIONS
3

READS
1,014

3 authors:

Shaymaa taha Ahmed
University of Diyala
19 PUBLICATIONS **56** CITATIONS
SEE PROFILE

Ban Jawad
Savitribai Phule Pune University
7 PUBLICATIONS **18** CITATIONS
SEE PROFILE

Qusay Kanaan Kadhim
Technical University of Malaysia Malacca
25 PUBLICATIONS **115** CITATIONS
SEE PROFILE

Cloud Services and Cloud Perspectives: A Review

Cloud Services and Cloud Perspectives: A Review

Shaymaa Taha Ahmed[1,*], Ban Jawad Khadhim[2], Qusay Kanaan Kadhim[3]

[1,2] Department of Computer Science, College of Basic Education University of Diyala, Diyala, Iraq
[3] Middle Technical University, Baghdad, Iraq

[*] Email: Shaymaa.taha.ahmed@basicedu.uodiyala.edu.iq & qusaykn@gmail.com

Abstract. Cloud computing is a popular paradigm in information technology and computing as it offers numerous advantages in terms of economical saving and minimal management effort to many organizations agencies. Although elasticity and flexibility brings tremendous benefits, it still raises many information security challenges that have created a barrier against adopting this agile Cloud computing. This paper provides a review study on the cloud computing as well identifying 25-key factors to fulfil better practice in cloud computing and way of making the environment of the cloud computing more qualified to many organizations agencies.

Keywords: Cloud, Computing, Cloud Services, Cloud Factors

1. Introduction

The future is a promising cloud computing infrastructure style that can deploy large-scale applications is an advantage effective method of cost [1].Cloud computing enables users to access a variety of conquerable facilities such as data storage, processing, infrastructure, and applications [2]. Ability cloud the quantum of users to access cloud services to hold systems secure and daily growing in cloud medium [3]. The multiplicity of computing technology is valuable by government institutions using services and projects based on cloud computing for run applications in cloud computing [3]. The structure of operations is based on working on distributed, unorganized and complex environments of services that include a range of services provided and thus joining the cloud by a different method. For example, the firms that are using cloud-computing technology and process mobile devices can implement the equipment wireless for trade checking, recovery, detection, commercial intrusion detection systems [4]. Meanwhile, mobile cloud computing is a business model, which will compute the tasks distributed A large number of Cloud computers of resources, so that cloud users can Computer power, data storage management and cloud information services on-demand [5]. Relying on the continuous growth of network bandwidth cost, under the mature conditions, clients can connect with cloud users limited in cloud computing and data storage through some protocols and servers by translating the mouse and keyboard as input to data cloud through thin clients, the client then returns results. The cloud provides organizations with data storage functionality. Sharing cloud resources is better than expanding your own platforms. Enterprise and enterprise cloud computing provides a reliable, flexible data system and a profitable cloud infrastructure in terms of spending [6] . aside from the cloud on the student user's need to place them dynamically scaled, internet cloud resources of the Internet accused, the cloud has not only transformed the method cloud services are delivered, the business of information technology based

companies during the life cycle has seen less time to develop applications that serve users in all organizations [7]. Cloud Computing works in innovating new ways to change the feature of saving information completing applications. Software and data management through computer working on hosting information on the cloud combine them form groups of servers and computers connected to the Interne [8]. However, in reality cloud challenge is a broad subject, and any policy mix standards, technologies, and mitigation protection controls cloud information's storage, cloud platforms, and the cloud of possible services malicious insider and outsider threats in the cloud environments [9]. Furthermore, the current research in cloud computing challenge paid attention on the provision of use mitigation control technology through a set of issues in the cloud to store data securely, encourage user confidence in the use of cloud must work on the stability of services, cloud platform and data delivery, cloud trust, sensitive confidentiality and cloud information [10]. More recently, the literature witnessed a surge of studies from various disciplines in the cloud challenge management, however slight is well-known about the challenge elements that effect cloud computing adoption services [11].

2. Cloud Computing

Cloud computing share cloud ownership of infrastructure and applications that provide a cloud over the Internet. Providing the user with services for cloud computing services, providing a product that meets the needs of the user and is aware of the problem involved in the use of this service provided. Therefore, the services provided are developed by tracking cloud networks and analysing applications and services provided by the cloud to users [12]. Additionally, cloud computing service provides better compatibility, scalability and network connectivity on demand for many computing resources including servers, cloud network components, operating systems, software applications, cloud virtualization resources (sharing and pooling resource), and cloud services [13]. In common, cloud computing represents a broad growth of dispersed computing, parallel computing besides network computing. The cloud computing is the result of applications of conceptual combination of Utilities cloud Computing, cloud Virtualization data, Software as a Service (SaaS), Infrastructure as a service (IaaS) and Platform as a Service (PaaS)[14] . Cloud attribute to software implementation, and infrastructure that the network provide that is used to these services in a cloud data centre [8] .However, fast software development in the using Cloud, computing technology leads to deploying and more the cloud services to network pool. The Cloud computing provides a range of services (CSPs) [15].

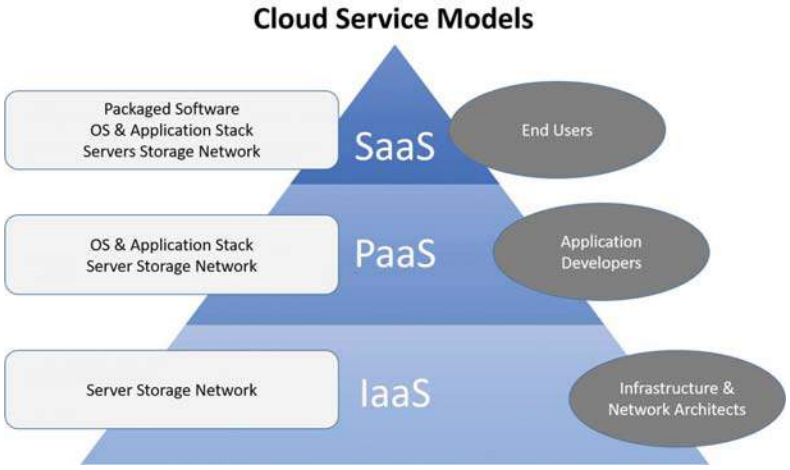

Figure 1. Cloud service models [16]

Figure 1. Categories cloud service resources through cloud computing platform is important for service IaaS infrastructure services, PaaS and SaaS platform services applications and services [16]. There are several key challenges within the cloud computing environment , which include mobility and application

security issues , cloud security services and applications issues, cloud security data issues , cloud security issues and cloud security platform [17].

3. Cloud Services

The cloud technology implementation provides several advantages to the public sector and at the heart of them is cutting costs. Generality government organizations chiefly in the developing countries are committed in take on the cloud technology because of the growth of cloud adoption in E-government services[18]. Additionally, the providers of the cloud computing service always update their services and system, which in case leave no negative impact on the services [19].Nevertheless, nowadays, the sudden traffic volume has come to forefront as a new challenge to the users of the e-government services. This problem often occurs when the government organizations and some internet companies are in the construction of data centres. Therefore, it must be in accordance with the peak value of planning capacity[20]. The majority of past studies with regard to cloud challenge in services were concern in discovering the cloud issues leaving a large body of the literature. Yet, the literature still lacks to adequate studies in the cloud challenge management, especially in government services. However, those studies address this issue generally. In other words, the past studies in cloud computing adoption focus in the general factors that area associated with service quality rather than specifying on challenge management. Free few studies investigate the determinants of cloud computing challenge adoption based on users' service perspective. Research by [21]. Investigates the important challenge factors that affect cloud computing challenge adoption by Saudi government departments. A model proposed for three groups, Cloud Challenge Risks Category Social, Factors category, and Perceived Cloud Challenge was tested by using the SPSS and mean tools. The overall results shows that those three groups have positive effect on the cloud challenge adoption [22].Table .1, summarizes the literature gap and suggests for future trend. Indeed, past literature still lack to adequate research in cloud challenge control based on users' perspective. Even though, there are few studies attempted to explore the critical factors that are associated with cloud control challenge such as [23].This study narrowed the focus on three limited groups and used average test only. However, in this research, cloud-computing challenge will extend to include a large size of control factors that address and mitigate cloud-computing issues. In addition, the fuzzy model with algorism is used which is more rigor than average test [24].

Table 1. The literature gap and the research trend

Concept	Details
The literature gap	Lack to adequate research in cloud challenge management based on users' perspective. Lack to rigor analysis methodology
The objective of this study	In this research, cloud-computing challenge will be extended to include factors that address cloud challenge management issues comprehensively. In addition, the analysis will be undergone by rigor statistical analysis tool which is fuzzy regression with algorism will be used which is more rigor than average test.

4. Cloud Perspectives Factors

Cloud computing technology rush is making and the effect is felt all crossways in government organisation. Therefore, controlling challenge of cloud computing issues are playing significant part in the IT plans [25] . Although some challenge controls and policies are devised for each element of cloud computing, an empirical model of cloud computing challenge management through quantitative measurements is important to examine the cloud computing controls on challenge issues[13].

Table 2. Database search

Journal Type	Search results	Filters	Filters	years
Web of science	201	77	48	2016
SCOPUS	177	31	27	to
Another	33	5	3	2020
Total	411	113	78	

The review Table 2 highlights the control factors that mitigate cloud-computing issues in government's services. The review provides identify 25- key factors to avoid the challenges or to reduce the challenges for adoption of cloud computing.

4.1. Developing authentication models in the Cloud

Cloud service providers (CSP) and Cloud User can be distinguished [3]. This must not be confused with user authentication, a component of the character management system [26]. However, cloud data storage does not affect data authentication analysis to determine whether it should be accepted in evidence [27]. The question is whether the document is what it means. E-mail is no additional or fewer reliable because it is stored behind the corporate firewall or data stored in the cloud [7]. The question, therefore, is whether it has been stored in court, and the law court can expectation that it has not been changed since it was sent or received. Authentication mechanisms will be increased or reduced to accommodate cloud threat patterns for cloud computing users in their cloud computing environments [10].

4.2. High Availability of Cloud Services

The organisations deal with some applications for tasks where this can indicate a break for the difference between CPS and clients [4]. In addition, cloud providers must be aware of these stringent availability requirements and be prepared to deliver this information with full assurance. Standardize the participation of cloud users and information resources should be in accordance with the availability of resources, this means that the levels of information available from developers to design approve and maintain the models[15] . This measure is significant for a high degree of automation and availability across multiple data centre environments [5]. In addition, the availability is far reaching through which a full range of computing resources can be accessed and usable [28]. The loss may be partial or complete, depending on whether the availability is temporary or permanent

4.3. Using Cloud Multi-Tenant Infrastructure Model

When looking at the cloud computing environment, the term "multiple leases" allows cloud users to share their infrastructure and database in order to take advantage of the performance and cost that comes with economies of scale [29]. In addition, shared computing resources may face threats to data loss, or data privacy [30].The multi-part leasing of machine-based virtual cloud infrastructure, together with fine details of bodily resources are shared among guest virtual machines, may result in new sources of cloud threat [31].In addition organisations using cloud technology to understand data challenge controls in multi-tenant cloud environments are very important organisations or institutions [30].

4.4. Better Cloud Compatibility and Scalability for Cloud Services

The development potential is very important for development teams, so the project must have sufficient capacity to grow with the business process and demands without causing problems for existing applications [32]. This can enable the enterprise to leverage its volume after one server to hundreds of servers minus[33]. The volume enables the government to obtain the largest cloud computing resources to perform temporary intensive computing tasks when needed without re-investing in redundant computing capabilities to meet the high non-recurring demand [15].Cloud services can be used in this manner efficiently and at a known cost Because of its fast capacity and easy deployment, yet the cloud service provides a highly scalable environment to handle the load better [34].

4.5. Need to Virtualization Technology in Cloud Computing Environments

Cloud Virtualization solved the problem of scalability to a certain extent due to its ability to cloud and distributed nature[35]. In addition, it also helps the person in charge of the data centre to manage the server with absolute ease by using some programming interfaces for easy-to-use applications. Therefore, many facets of this technology are available, but they have emerged mainly as a winner in the integration and optimization of data centres [36].In adding, the program can be upgraded and maintained without user notice because the VM can be migrated from one host device to another while it is running. All these provide a high increase in flexibility and efficiency. Virtualization is an important aspect of real software deployment [37]. However, the typical distributed virtualization system is divided into three main parts - a node Organisation, computing node, shared data storage [38].

4.6. Implement Automated Tools and Develop Application Portability

The service provider provides information upon request to resolve the cloud from another service provider [24].The implementation use of automated version controls reduces risk in cloud computing[12]. In addition, cloud infrastructure is a combination of two or more clouds private, community or public[39]. Integrated with standard or proprietary technologies that enable data transfer and applications e.g., cloud bursting for load balance between clouds [25]. The cloud line is composed of two or additional clouds. The clouds represent unique entities but at the same time are closely related to each other in a standard way. The enabling the required data as well as loading the application [28].

4.7. Review service-level agreements

Services may require increased complexity of Service Level Agreements (SLS) covering emerging challenge issues as well as cloud challenge such as data availability, data integrity, and confidential sensitive data [40]. However, cloud computing consists of virtual computers, widely interconnected on the basis of Egyptian-level agreements (SLA) that were established through negotiations between the consumer and the service provider [41].Thus establishing a level of compliance with cloud providers and agreeing on some SLAs (service level) and ensuring that data is not protected in privacy [42]. The may experience application developers with a range of negative scenarios, each with its own identity without a solution based on the identity of the claim [19].

4.8. Flexibility Access to Data on Cloud Storage

Applications to control access to the clouds stay the essential flexibility and scalability to provision a big number of workers and capitals in a dynamic and mixed environment, with cooperation and info exchange needs [43]. A cloud vendor often offer services to directly access cloud storage of mobile client applications, or our services in the cloud forms a gateway to access cloud storage [44].Cloud computing flexibility offers greater flexibility than previous computing methods by supporting a wide variety of technologies and structures [29]. Application to control access to the cloud flexibility and scalability necessary to support a large number of users and resources in a dynamic and heterogeneous environment, cooperation and information exchange needs [45].

4.9. Create, Deploy, Develop, and Implement Policies and Procedures for the Cloud

Focus on synchronization, plans and procedures in the development process, allowing the transfer of tasks[46]. Risk management planning is both effort and organizational, drawing together risk policies, practices and procedures organized in a holistic and coherent manner that will address the peculiar nature of risks to the project [24]. Develop appropriate standard operating procedures [47]. In this proliferation, operational challenge changes from the hands of either one group to another or cloud vendor [48]. Therefore, it is responsible for what must be padded out. Different departments, users and management areas have different policies and a range of bets. To avoid caution must be leaked data when the responsibility changes from the hands [35] .

4.10. Challenge Cloud Infrastructure Need to Trust Computing and Cryptography

Data need be endangered in a consistent way with policies, both in the organisation's computing centre or the cloud. There is no stock service contract covering the range of cloud services available and the

needs of different organizations [49].Moreover, it is important to reduce the costs of running efficiently on encrypted data [50].Reputation Manager is responsible for managing a database of cloudlets and dozens of reputations. Whenever a mobile user interface with a small cloud shake, the user can evaluate the small cloud shake, by offering an assessment of the director directly reputation, or by a small cloud shake [49]. In either case, the owner of the small cloud shake may not modify the classification.

4.11. Data Protection and Integrity for the Cloud

Cloud data storage characteristically resides in a communal environment with the same location with data from other clients [51]. Organizations transmission subtle data and organize data in a cloud, therefore, must represent the means by which data access is controlled and data challenge is maintained [24]. Data integration with the assigned parts of the assigned [21].After an instance in the services container parts, the instance of the service will usually make use of additional parts the end of the year, which include for example databases and transaction screens [52].

4.12. Enhancing Cyber Challenge Systems

It is necessary to reduce risks such as cyber-attacks [53]. Thus, the successful implementation of the risk assessment for this comprehensive cyber challenge requires the development of measures to measure the characteristics of information challenge on data confidentiality, data integrity and data availability [54]. Another challenge is to determine what should be automated responses, and thus potentially be manipulated by attackers, which still makes human decision-making fundamentally. A behavioural element to assess the risks of cyberspace challenge represents rationality constrained by human agents, environmental noise and decision-making process [55].

4.13. Change Management and Incident Response Procedures (Plan)

The organisation requirements to assess its CSP capability to provide sufficient event retort as well as its own incident response procedures to disrupt the system and data theft scenarios [54]. Cloud service plans are developed by candidates according to user requirements, which often include an incident response plan [26]. Incident response is a different important view to enhance challenge and privacy in the cloud [52].

4.14. Hypervisor Complexity

Hypervisor wants towards stay locked depressed and hard-bitten by using the best practices [11]. The core concerns of corporate and cloud virtual users must be sound management of the conformation and processes as well as the physical challenge of the server that hosts the Hyper Server cloud [56]. The programs that are run in host machines are called to create and manage machines as a Hyper Server or virtual cloud-monitoring device [57].

4.15. Cloud Reduce Denial of Service (DoS) Attack

The renunciation of facility attack encompasses fullness of the target with requirements to stop it from replying to legitimate requests in a timely method [58] . The attacker typically uses manifold computers [59].Availability is a requirement that data storage and operations are protected and prevented from denial of service to authorized cloud users [52].

4.16. Understand the Fundamental Technologies

The cloud service benefactor uses governance services counting the insinuations of the relevant technical panels on the system's challenge and data privacy system, in relation to the software development of the system and to all components of the organisation [60].The benefits, which are technology functions, are able to change dramatically during software development projects because basic technologies are rapidly changing [6].

4.17. Services are Fully Managed and Delivered by a Third Party in Cloud Computing

The Organisations then companies are losing control over how they secure cloud computing environments[15]. Then enables organizations to use cloud computing platform and important business

function environments that need to find an answer to these questions from [33].The safe is my cloud data and in SQL, and kept my private data in the cloud and in SQL, other clients can access SQL My data, how all this affects my compliance requirements, whether there is a challenge management involving my data [27]. my data is backed up and kept for enough time [14].

4.18. Reducing Cost and Carbon Footprint for Cloud Services

The nature of on-demand cloud service allows organizations to reduce costs, while also providing a reduction of cloud developers since the cloud services and control by the provider. In addition, to protect user privacy through expensive techniques computationally [61].This will reduce the carbon footprint resulting from the different forms of transport currently in use. Given these, there will be a reduction in e-waste and carbon emissions [62]. Moreover, reducing capital expenditures - lower hardware costs, licensing, maintenance and overhead costs [5].

4.19. Controls Need to Composite Cloud Services

The cloud providers can be formed through overlapping and coatings with additional cloud services. The SaaS provider can build its services on the cloud services of AAAs or IAAS [63]. The level of availability of data from the cloud software as a service and then build on the availability of those services [64]. Cloud services that use third-party cloud providers to outsource or subcontract some of their own cloud services should raise concerns, including the scope of third-party control, responsibilities involved, remedies and available asylum problems should occur [59].

4.20. Speed of Cloud Deployment and Ease Integration

The cloud can be deployed path in a very small period [65]. The same cross, the introduction of a new-fangled user into the cloud occurs instantly and rapidly, eliminating waiting periods [64]. Also, the integrity of cloud applications occurs automatically in users of cloud installations and business developments are certified to choose required cloud services and requests that suit their favourites, while spending minimal effort in integrating and customizing those applications [59]. Cloud service providers community support projects can meet cloud resource requirements much [36].

4.21. Decreased effort in management technology in Cloud Computing

Cloud computing is able to allow the organisation to attention more time on goalmouths [66]. Most cloud service aids are based on a unified basis that has already been created by IT that facilitates better support [67]. This basis also makes cloud computing capitals easier to provide, which in turn paves the way for a more consistent technology upgrade and accelerated completion of IT reserve demands[68]. In fact, the low voltage management technology in cloud computing is important to alleviate the problem using more tools and techniques [24].

4.22. Managing Cloud Data Confidentiality and Increasing Auditability

The encryption deployment, VLAN, firewalls although greatest companies outsource workforce and many companies that use external email services to grip subtle data; challenge is one of the most important objections frequently cited to cloud computing [32]. Forecasters and cynical companies ask, the would trust their core data out there somewhere [69]. Encryption can be used to secure transmission, which is a process of translating encrypted text into a shadow text [51].

4.23. Implement Application Level for Data Caching

The portable restrictions such as bandwidth limit, dormancy, sporadic connection, etc. often enhance collecting on the movable device or the adoption of cloud-level application services in cloud computing [70]. Using the request level cache services to reduce roundtrips to cloud storage [71].Though, new programming languages previously provide a key by permitting data caching finished a moveable device, and this allows the cloud request to continue employed if the, joining has lost moments [70].

4.24. Usability and Biometric System for Cloud Computing Environment

Although vital challenge is a very promising technology, the challenges slow down its growth and spread [72]. However, encryption that encrypts data using biometric features improves data challenge and overcomes major administrative and confidentiality issues [73].In order to maintain this record, this research needs separate biometrics in different locations which is a very expensive and maintenance process also associated with a burden. May be located in locations in different locations throughout the country, so the presence of so many devices require an increased cost[74].Biometrics are high-tech devices used to measure some physical properties for individual pursuit, such as fingerprints or retinal patterns. Biometrics measures are often combined with other procedures, such as PINs, to determine delegation rights [75].

4.25. Cryptography and Steganography

In this, it uses a unified approach of encrypting and hiding information because it will provide two-way challenge to the data that is sent to the network cloud[76]. First, the data gets converted to an encrypted format by using a cryptographic algorithm and then this encrypted data format is converted back into a rough image by using the hide information. Hiding information also hides the presence of a message, thus ensuring that the chances of data being tampered with are slim [67]..However, the Encryption Challenge Policy provides an encryption feature that provides that will be converted into readable data [43]. Furthermore, the encrypted data is difficult to read until the decryption is executed, but there are techniques that indicate that encrypted data can be converted into readable form using appropriate keys [77].Cloud computing today uses a cryptographic process to enhance online challenge such as digital signature, e-commerce and to validate transactions [78].

5. Conclusions

The adoption of cloud computing provides continuous benefits such flexibility of their businesses in terms data storage, exchange, transform which enable them to upgrade their profitability, interoperability, capability, and scalability that can distribute multiple applications cost-effectively. Despite the advantages of the cloud computing these advantages do not offer better security in security challenges, includes lack of trust in data security and privacy, integrity, confidentiality, and availability. For this reason, this paper investigates previous literature in achievement of best practices in cloud services based on their impact and severity on critical assets. To help better understand the current cloud computing adoption decision factors. In this work, we examine and investigate identifying 25-key factors to fulfil better practice in cloud computing. Furthermore, assist organizations in creation the right decision on whether to adoption the cloud computing.

6. Reference

[1] S. SaaDey, S., Sampalli, S., & Ye, Q. mpalli, "Security & Privacy Issues in Mobile Cloud Computing," *Int. J. Bus. Cyber Secur.*, vol. 1, no. 1, pp. 31–43, 2016.

[2] M. A. Mohammed Al-khafajiya, Thar Bakera, Hilal Al-Libawyb, Zakaria Maamarc and Y. Jararwehe, "Improving Fog Computing Performance via F og-2- F og Collaboration," *Futur. Gener. Comput. Syst.*, vol. 100, pp. 266–280, 2019.

[3] Q. K. Kadhim, R. Yusof, and H. S. Mahdi, "A Review Study on Cloud Computing Issues," in *1st International Conference on Big Data and Cloud Computing (ICoBiC) 2017*, 2018, pp. 1–11, doi: 10.1088/1742-6596/1018/1/012006.

[4] A. Iqbal and R. Colomo-Palacios, "Key Opportunities and Challenges of Data Migration in Cloud: Results from a Multivocal Literature Review," *Procedia Comput. Sci.*, vol. 164, pp. 48–55, 2019, doi: 10.1016/j.procs.2019.12.153.

[5] N. Anciaux *et al.*, "Personal Data Management Systems: The security and functionality standpoint," *Inf. Syst.*, vol. 80, pp. 13–35, 2019, doi: 10.1016/j.is.2018.09.002.

[6] K. Kaur, S. Garg, G. S. Aujla, N. Kumar, J. J. P. C. Rodrigues, and M. Guizani, "Edge Computing in the Industrial Internet of Things Environment: Software-Defined-Networks-Based Edge-Cloud Interplay," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 44–51, 2018, doi: 10.1109/MCOM.2018.1700622.

[7] H. S. M. Alsultani, Q. Kanaan, and I. Y. Khudhair, "Empirical investigation of TCP incast congestion in Wireless cloud computing networks," *J. Comput. Sci.*, vol. 14, no. 5, 2018, doi: 10.3844/jcssp.2018.663.672.
[8] Q. K. Kadhim, R. Yusof, H. S. Mahdi, and S. R. Selamat, "The effectiveness of random early detection in data center transmission control protocol-based cloud computing networks," *Int. J. Commun. Antenna Propag.*, vol. 7, no. 5, 2017, doi: 10.15866/irecap.v7i5.10104.
[9] Q. Duan, "Cloud service performance evaluation: status, challenges, and opportunities – a survey from the system modeling perspective," *Digit. Commun. Networks*, vol. 3, no. 2, pp. 101–111, 2017, doi: 10.1016/j.dcan.2016.12.002.
[10] A. Sufian, A. Ghosh, A. S. Sadiq, and F. Smarandache, "A Survey on Deep Transfer Learning to Edge Computing for Mitigating the COVID-19 Pandemic: DTL-EC," *J. Syst. Archit.*, vol. 108, no. April, p. 101830, 2020, doi: 10.1016/j.sysarc.2020.101830.
[11] D. A. Tamburri, M. Miglierina, and E. Di Nitto, "Cloud applications monitoring: An industrial study," *Inf. Softw. Technol.*, vol. 127, no. March, 2020, doi: 10.1016/j.infsof.2020.106376.
[12] Q. Kanaan, H. S. Mahdi, and H. K. Ail, "Storage Architecture for Network Security in Cloud Computing," *Diyala J. Pure Sci.*, vol. 14, no. 1, pp. 1–17, 2018.
[13] S. T. Ahmed, C. Science, and B. Education, "Innovative Queue Management Mechanism for Congestion Control in Wireless Cloud Computing Environment," *Jour Adv Res. Dyn. Control Syst.*, vol. 10, no. May, pp. 1208–1214, 2018.
[14] M. Shorfuzzaman and M. Masud, "Leveraging a Multi-Objective Approach to Data Replication in Cloud Computing Environment to Support Big Data Applications," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 3, pp. 418–429, 2019.
[15] Ali, Mazen, and Hassanein., "A proposed hybrid model for adopting cloud computing in e-government," *Futur. Comput. Informatics J.*, vol. 3, no. 2, pp. 286–295, 2018, doi: 10.1016/j.fcij.2018.09.001.
[16] M. G. Azam, "Application of cloud computing in library management: innovation, opportunities and challenges," *Int. J. Multidiscip.*, vol. 4, no. 1, pp. 2–11, 2019, doi: 10.5281/zenodo.2536637.
[17] D. G. Arce, "Cybersecurity and platform competition in the cloud," *Comput. Secur.*, vol. 93, p. 101774, 2020, doi: 10.1016/j.cose.2020.101774.
[18] B. J. Khadhim[1], S. T. Ahmed, and R. M. Abdulqader, "Transmission Control Protocol (TCP) Incast and Outcast Issues in Cloud Computing," *J. Adv. Res. Dyn. Control Syst. - JARDCS*, vol. 13, no. May, pp. 2026–2032, 2019.
[19] P. Prajapati and P. Shah, "Review on Secure Data Deduplication: Cloud Storage Security Issue," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 4, no. 11, pp. 1–12, 2020, doi: 10.1016/j.jksuci.2020.10.021.
[20] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "Current State of Cloud Computing Adoption - An Empirical Study in Major Public Sector Organizations of Saudi Arabia (KSA)," *Procedia Comput. Sci.*, vol. 110, 2017, doi: 10.1016/j.procs.2017.06.080.
[21] M. O. Alassafi, A. Alharthi, R. J. Walters, and G. B. Wills, "A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies," *Telemat. Informatics*, vol. 33, no. 3, pp. 996–1010, 2017, doi: 10.1016/j.tele.2017.04.010.
[22] I. Systems *et al.*, "Challenges of Cloud Computing Adoption Model for Higher Challenges of Cloud Computing Adoption Model for Higher Education Level in Zanzibar," *Procedia Comput. Sci.*, vol. 161, pp. 1046–1054, 2019, doi: 10.1016/j.procs.2019.11.215.
[23] K. Jakimoski, "Security techniques for data protection in cloud computing," *Int. J. Grid Distrib. Comput.*, vol. 9, no. 1, pp. 49–56, 2016, doi: 10.14257/ijgdc.2016.9.1.05.
[24] S. T. A. Raddam Sami Mehsen, Teeb Hussein Hadi, "Integrated Circuit Security Risk Management Framework in Government Agencies," *J. Southwest Jiaotong Univ.*, vol. 54, no. 1–9, pp. 17–23, 2019.
[25] S. T. Ahmed, R. S. Mehsen, and T. H. Hadi, "A structural model fuzzy multiple regression analysis to cloud computing security issues," *International Journal of Advanced Science and Technology*, vol. 29. 2020.
[26] Minahil, M. F. Ayub, K. Mahmood, S. Kumari, and A. K. Sangaiah, "Lightweight authentication

protocol for e-health clouds in IoT based applications through 5G technology," *Digit. Commun. Networks*, no. October 2019, pp. 1–10, 2020, doi: 10.1016/j.dcan.2020.06.003.

[27] S. Iqbal, M. L. M. Kiah, N. B. Anuar, B. Daghighi, A. W. A. Wahab, and S. Khan, "Service delivery models of cloud computing: security issues and open challenges," *Secur. Commun. Networks*, vol. 9, no. 17, pp. 4726–4750, 2016, doi: 10.1002/sec.1585.

[28] T. Branco, F. De Sá-Soares, and A. L. Rivero, "Key Issues for the Successful Adoption of Cloud Computing," *Procedia Comput. Sci.*, vol. 121, pp. 115–122, 2017, doi: 10.1016/j.procs.2017.11.016.

[29] I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Eng. Sci. Technol. an Int. J.*, vol. 21, no. 4, pp. 574–588, 2018, doi: 10.1016/j.jestch.2018.05.010.

[30] S. Azouzi, Z. Brahmi, and S. A. Ghannouchi, "Customization of multi-tenant learning process as a Service with Business Process Feature Model," *Procedia Comput. Sci.*, vol. 126, pp. 606–615, 2018, doi: 10.1016/j.procS.2018.07.295.

[31] T. Yan, J. Liu, Q. Niu, J. Chen, S. Xu, and M. Niu, "Network security protection technology for a cloud energy storage network controller," *Glob. Energy Interconnect.*, vol. 3, no. 1, pp. 85–97, 2020, doi: 10.1016/j.gloei.2020.03.007.

[32] B. Sonkoly *et al.*, "Scalable edge cloud platforms for IoT services," *J. Netw. Comput. Appl.*, vol. 170, no. July, 2020, doi: 10.1016/j.jnca.2020.102785.

[33] L. A. Tawalbeh and G. Saldamli, "Reconsidering big data security and privacy in cloud and mobile cloud systems," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 6, no. 7, pp. 1–10, 2019, doi: 10.1016/j.jksuci.2019.05.007.

[34] M. Hosseini, A. Masoud, and A. Sahafi, "A survey study on virtual machine migration and server consolidation techniques in DVFS-enabled cloud datacenter : Taxonomy and challenges," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 32, no. 3, pp. 267–286, 2020, doi: 10.1016/j.jksuci.2018.07.001.

[35] E. Torre *et al.*, "A dynamic evolutionary multi-objective virtual machine placement heuristic for cloud data centers," *Inf. Softw. Technol.*, vol. 128, no. December 2019, 2020, doi: 10.1016/j.infsof.2020.106390.

[36] K. Al-Zoubi and G. Wainer, "Fog and cloud collaboration to perform virtual simulation experiments," *Simul. Model. Pract. Theory*, vol. 101, no. October 2019, p. 102032, 2020, doi: 10.1016/j.simpat.2019.102032.

[37] J. S. J. Rajasingh and J. Reeves Wesley, "Step into the cloud or stop with virtualization - The project manager's dialectic dilemma," *Procedia Comput. Sci.*, vol. 172, no. 2019, pp. 1077–1083, 2020, doi: 10.1016/j.procs.2020.05.157.

[38] S. Tabassam, "Security and Privacy Issues in Cloud Computing Environment," *J. Inf. Technol. Softw. Eng.*, vol. 07, no. 05, pp. 1–6, 2017, doi: 10.4172/2165-7866.1000216.

[39] S. R. Jena, R. Shanmugam, K. Saini, and S. Kumar, "Cloud Computing Tools: Inside Views and Analysis," *Procedia Comput. Sci.*, vol. 173, no. 2019, pp. 382–391, 2020, doi: 10.1016/j.procs.2020.06.045.

[40] M. Rojszczak, "CLOUD act agreements from an EU perspective," *Comput. Law Secur. Rev.*, vol. 38, p. 105442, 2020, doi: 10.1016/j.clsr.2020.105442.

[41] I. Odun-Ayo, B. Udemezue, and A. Kilanko, "Cloud service level agreements and resource management," *Adv. Sci. Technol. Eng. Syst.*, vol. 4, no. 2, pp. 228–236, 2019, doi: 10.25046/aj040230.

[42] T. Halabi and M. Bellaiche, "A broker-based framework for standardization and management of Cloud Security-SLAs," *Comput. Secur.*, vol. 75, pp. 59–71, 2018, doi: 10.1016/j.cose.2018.01.019.

[43] P. S. Challagidad and M. N. Birje, "Efficient Multi-authority Access Control using Attribute-based Encryption in Cloud Storage," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 840–849, 2020, doi: 10.1016/j.procs.2020.03.423.

[44] T. Yan *et al.*, "Distributed energy storage node controller and control strategy based on energy storage cloud platform architecture," *Glob. Energy Interconnect.*, vol. 3, no. 2, pp. 166–174,

2020, doi: 10.1016/j.gloei.2020.05.008.
[45] S. Bertocco, P. Dowler, S. Gaudet, B. Major, F. Pasian, and G. Taffoni, "Cloud access to interoperable IVOA-compliant VOSpace storage," *Astron. Comput.*, vol. 24, pp. 36–44, 2018, doi: 10.1016/j.ascom.2018.05.003.
[46] S. J. E. Taylor *et al.*, "The CloudSME simulation platform and its applications: A generic multi-cloud platform for developing and executing commercial cloud-based simulations," *Futur. Gener. Comput. Syst.*, vol. 88, pp. 524–539, 2018, doi: 10.1016/j.future.2018.06.006.
[47] B. M. Balachandran and S. Prasad, "Challenges and Benefits of Deploying Big Data Analytics in the Cloud for Business Intelligence," *Procedia Comput. Sci.*, vol. 112, pp. 1112–1122, 2017, doi: 10.1016/j.procs.2017.08.138.
[48] L. Karim, A. Boulmakoul, A. Mabrouk, and A. Lbath, "Deploying Real Time Big Data Analytics in Cloud Ecosystem for Hazmat Stochastic Risk Trajectories," *Procedia Comput. Sci.*, vol. 109, pp. 180–187, 2017, doi: 10.1016/j.procs.2017.05.322.
[49] A. A. A. Ari *et al.*, "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges," *Appl. Comput. Informatics*, vol. 5, no. 7, pp. 1–12, 2019, doi: 10.1016/j.aci.2019.11.005.
[50] M. Pau *et al.*, "A cloud-based smart metering infrastructure for distribution grid services and automation," *Sustain. Energy, Grids Networks*, vol. 15, no. 2018, pp. 14–25, 2018, doi: 10.1016/j.segan.2017.08.001.
[51] U. Narayanan, V. Paul, and S. Joseph, "A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment," *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2020, doi: 10.1016/j.jksuci.2020.05.005.
[52] N. Krumm and N. Hoffman, "Practical estimation of cloud storage costs for clinical genomic data," *Pract. Lab. Med.*, vol. 21, no. September 2019, p. e00168, 2020, doi: 10.1016/j.plabm.2020.e00168.
[53] D. W. Chadwick *et al.*, "A cloud-edge based data security architecture for sharing and analysing cyber threat information," *Futur. Gener. Comput. Syst.*, vol. 102, pp. 710–722, 2020, doi: 10.1016/j.future.2019.06.026.
[54] K. Muniasamy, S. Srinivasan, J. Vain, and M. Sethumadhavan, "Formal methods based security for cloud-based manufacturing cyber physical system," *IFAC-PapersOnLine*, vol. 52, no. 13, pp. 1198–1203, 2019, doi: 10.1016/j.ifacol.2019.11.361.
[55] V. Kakkad, H. Shah, R. Patel, and N. Doshi, "A comparative study of applications of game theory in cyber security and cloud computing," *Procedia Comput. Sci.*, vol. 155, no. 2018, pp. 680–685, 2019, doi: 10.1016/j.procs.2019.08.097.
[56] A. M. Abdelmoniem, B. Bensaou, and A. J. Abu, "SICC: SDN-based incast congestion control for data centers," in *IEEE International Conference on Communications*, 2017, doi: 10.1109/ICC.2017.7996826.
[57] D. De, C. Germán, B. Reyes, and J. Vega, "Cloud Computing Virtualization," *Int. J. Comput. Appl. Technol. Res.*, vol. 6, no. 7, pp. 290–292, 2017, [Online]. Available: http://manglar.uninorte.edu.co/bitstream/handle/10584/7374/Analisisdelaradio.pdf?sequence=1.
[58] K. Bhushan and B. B. Gupta, "Hypothesis Test for Low-rate DDoS Attack Detection in Cloud Computing Environment," *Procedia Comput. Sci.*, vol. 132, pp. 947–955, 2018, doi: 10.1016/j.procs.2018.05.110.
[59] K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D. G. Narayan, "Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 2297–2307, 2020, doi: 10.1016/j.procs.2020.03.282.
[60] D. Garg, J. Sidhu, and S. Rani, "Improved TOPSIS: A multi-criteria decision making for research productivity in cloud security," *Comput. Stand. Interfaces*, no. December, pp. 1–18, 2019, doi: 10.1016/j.csi.2019.02.002.
[61] J. Patsavellas and K. Salonitis, "The carbon footprint of manufacturing digitalization: Critical literature review and future research agenda," *Procedia CIRP*, vol. 81, pp. 1354–1359, 2019,

doi: 10.1016/j.procir.2019.04.026.
[62] S. K. Addya, A. K. Turuk, B. Sahoo, M. Sarkar, and S. K. Biswash, "Simulated annealing based VM placement strategy to maximize the profit for Cloud Service Providers," *Eng. Sci. Technol. an Int. J.*, vol. 20, no. 4, pp. 1249–1259, 2017, doi: 10.1016/j.jestch.2017.09.003.
[63] H. B. Zhou, J. J. Zhang, Z. Z. Liu, D. Nie, W. Q. Wu, and V. H. C. de Albuquerque, "Research on Circular Area Search algorithm of multi-robot service based on SOA cloud platform," *Appl. Soft Comput. J.*, vol. 88, p. 105816, 2020, doi: 10.1016/j.asoc.2019.105816.
[64] L. Gupta, R. Jain, A. Erbad, and D. Bhamare, "The P-ART framework for placement of virtual network services in a multi-cloud environment," *Comput. Commun.*, vol. 139, no. March, pp. 103–122, 2019, doi: 10.1016/j.comcom.2019.03.003.
[65] J. Cuenca-Alba *et al.*, "ScipionCloud: An integrative and interactive gateway for large scale cryo electron microscopy image processing on commercial and academic clouds," *J. Struct. Biol.*, vol. 200, no. 1, pp. 20–27, 2017, doi: 10.1016/j.jsb.2017.06.004.
[66] K. S. S. Kumar and N. Jaisankar, "An Automated Resource Management Framework for Minimizing SLA Violations and Negotiation in Collaborative Cloud," *Int. J. Cogn. Comput. Eng.*, pp. 0–15, 2020, doi: 10.1016/j.ijcce.2020.09.001.
[67] N. A. Azeez and C. Van der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egypt. Informatics J.*, vol. 20, no. 2, pp. 97–108, 2019, doi: 10.1016/j.eij.2018.12.001.
[68] A. Ali, D. Warren, and L. Mathiassen, "Cloud-based business services innovation: A risk management model," *Int. J. Inf. Manage.*, vol. 37, no. 6, pp. 639–649, 2017, doi: 10.1016/j.ijinfomgt.2017.05.008.
[69] K. Brandis, S. Dzombeta, R. Colomo-Palacios, and V. Stantchev, "Governance, Risk, and Compliance in Cloud Scenarios," *Appl. Sci.*, vol. 9, no. 2, pp. 1–21, 2019, doi: 10.3390/app9020320.
[70] C. M. Geeta *et al.*, "SDVADC: Secure Deduplication and Virtual Auditing of Data in Cloud," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 2225–2234, 2020, doi: 10.1016/j.procs.2020.04.240.
[71] U. K. M. Sadique and D. James, "A Novel Approach to Prevent Cache-based Side-Channel Attack in the Cloud," *Procedia Technol.*, vol. 25, no. Raerest, pp. 232–239, 2016, doi: 10.1016/j.protcy.2016.08.102.
[72] K. A. Shakil, F. J. Zareen, M. Alam, and S. Jabin, "BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 32, no. 1, pp. 57–64, 2020, doi: 10.1016/j.jksuci.2017.07.001.
[73] C. Hahn and J. Hur, "Efficient and privacy-preserving biometric identification in cloud," *ICT Express*, vol. 2, no. 3, pp. 135–139, 2016, doi: 10.1016/j.icte.2016.08.006.
[74] H. Ben Hassen, N. Ayari, and B. Hamdi, "A home hospitalization system based on the Internet of things, Fog computing and cloud computing," *Informatics Med. Unlocked*, vol. 20, p. 100368, 2020, doi: 10.1016/j.imu.2020.100368.
[75] S. C. Satapathy, V. Bhateja, A. Joshi, S. Kumari, D. C. S. Lamba, and A. Kumar, "Performance Analysis of Adaptive Approach for Congestion Control In Wireless Sensor Networks," *IOSR J. Comput. Eng.*, vol. 19, no. 3, pp. 71–78, 2017, doi: 10.9790/0661-1903047178.
[76] M. O. Rahman, M. K. Hossen, G. Morsad, and A. Chandra, "An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Technique," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 18, no. 9, pp. 85–93, 2018.
[77] M. Sohal and S. Sharma, "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 7, no. 9, pp. 117–128, 2018, doi: 10.1016/j.jksuci.2018.09.024.
[78] H. F. El-sofany and S. A. El-seoud, "Studying Security of Data in Cloud Computing Through Cryptographic Approach," *Springer Int. Publ. Interact. Collab. Learn. Adv. Intell. Syst. Comput.*, vol. 544, no. August, pp. 434–444, 2017, doi: 10.1007/978-3-319-50340-0.