Cloud and Edge Computing Security Challenges, Demands, Known Threats, and Vulnerabilities

Ohood M. AlMendah, Dr. Sabah M. Alzahrani

College of Computers and Information Technology, Taif University, Saudi Arabia

Email:{ ohood.cs@hotmail.com , sa.sabah@tu.edu.sa }

Abstract

In recent years, Cloud and edge computing have got much attention because of the ever-increasing demands. There are many future technologies and advantages for systems to move towards clouds based on information keep methods. This includes a simple IT substructure and administration, and an effective distant approach from anyplace in the global with the steady computer network connections and efficient cost that cloud engineering can give. The privateness and security situations associated with the cloud need additional search. Scientists have presented prospective methods to these situations in antecedently published researches.

This proposed paper makes a study of cloud and edge security challenges and demands, known threats, and vulnerabilities. The paper's purpose is to investigate the various elements of cloud and edge computing with the recent developments in edge computing, the current privacy and security issues these schemes aspect. Then provides a novel categorization of the modern security methods that be in these fields. This examination introduces different security threats to the cloud and edge computing services also discusses open issues and suggests future directions.

Keywords: Cloud computing, Security challenges, Resources, Services, Edge computing.

1. Introduction

In the past periods of time, cloud and edge computing have been in the trend in order to their engineering functions, data storage and network administration [1]. It performs all these functions in central data centers. It has profited acceptance of people and communities being an economic and efficient service, as well as its growing demand in various fields [2]. This has also produced an efficient worldwide expansion of cloud and edge computing. It can present the right quantum of assets in a precise geographical localization. It still augmented the productiveness of the communities by losing the amount of housework needed for IT teams [3]. These result from increasing cloud computing security, performance and reliability [4]. Edge computing is a newcomer in the computing landscape [5]. It brings cloud computing services and facilities nearer to the customers and features sped up the process and fast request echo time [6]. Presently advanced applications based on the internet such as monitoring, VR, and security observing need accelerated process and fast reaction time [7]. Typically, any customer uses his apps on his phone device with little resource, while it executes the main service and process on cloud servers. Cloud computing problems can be solved through the next three models of computing: Fog Computing [8], Cloudlets [9], and Mobile Edge Computing [10]. Cloud and edge computing have carried as many gains as much other technology applications [11]. For example, it makes it achievable to keep a high quantity of different information and services. Moreover, this application solutes the problem of constricted assets and decreased the price of assistance by jointing precious assets through many people. Asset dependability and execution need the framework to be strong versus security warns [12]. In later ages, cloud and edge computing has got the greatest important contents in security research [13].

This research includes data-keeping safety, network security, and software system security. The author in [11] presents the conception of Cloudlets to solute the interval trouble of righting the clouds utilizing computer assets accessible in the localized network. Likewise, Edge Computing Mobile supplies off-load process, app services, and store close final-customs.

The hopeful characteristics of advanced engineering are navigation assist, site consciousness, ultra-minimum potency, and user nearness [12]. These advanced computing features make it suited for various futurity apps such as industry mechanization, realistic VR, smart home, intelligent sea observing and data analysis as present in Figure 1. Edge computing instrumentations such as access points, routers, station host and various services [13].

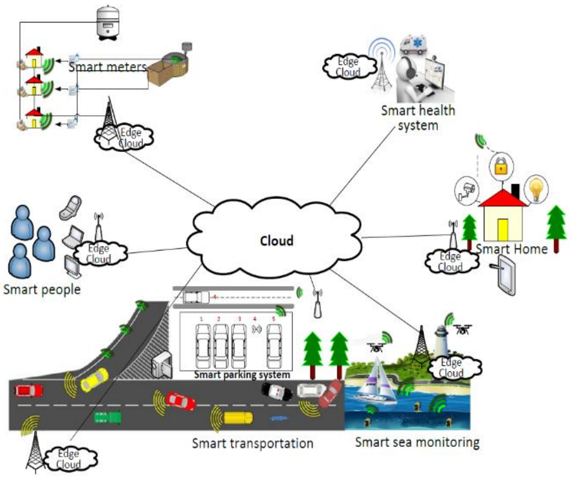

Figure 1. Cloud computing and edge computing applications architecture [14].

These Edge instruments enactment as a structure connecting clever phone devices to the clouds. Various papers [15,16,17] studied different characteristics of Edge and cloud computing such as the fogging technique while many papers concentrate on the advanced computing area such as Mobile Edge computing that concentrates on special app areas.

Nevertheless, no global review has been concluded that covers all characteristics of Edge and cloud computing, such as Fog, Cloudlet and Mobile-Edge computing [18].

The major objective of the paper:

a) vide a review of the advantages of cloud computing, security threats, challenges, and recent computing.

b) An overview of all aspects of Edge computing and present its advantages and limitations.
c) Define the fundamental requirements for visualizing the field of advanced computing.
d) Make a comparison between Cloud Computing and Edge Computing.

The need of Edge Computing while Cloud Computing if it is available.

Cloud models	**Benefits**	**Deficiency**
Private cloud	Specific organization. Ability to modify and customize. High secure	High costs needs IT experts. More expensive
Public cloud	High reliability and scalability easy use low cost	Unreliable Low secure
Hybrid cloud	Pliable infrastructure Cost controls speed is quicker	Potential challenges in application and data merge. Lack of vision.

Table 1. A comparison between private, public and hybrid clouds.

The last of this survey is prepared as follows. A background is provided on key security services and key technologies known in the cloud and edge computing the section 2. Section 3 encompasses main different between Cloud and Edge Computing. Section 4, present a Cloud security issues approaches. The paper conclusion and the future work present in Section 5.

2. Survey Overview

This section introduces the basic concepts of cloud computing and edge computing then presents the main difference between them. The aim of this section is to give a strong foundation for the research objective.

2.1 Cloud Computing

A cloud computing can be classified in to its privacy. Cloud computing has a three kinds, namely private cloud, public and hybrid clouds [19]. In a private clouds it deals with an enterprise information center. The resources are allocated to one or several organizations and work between jobs. For this cause, the substructure is closely held and managed by the self-enterprise in these clouds [20]. Defining the relationship between customers and suppliers and discovering security risks is much easier. In the public cloud, the companies, governments, or institutions have and run public clouds. Furthermore, communities can add unblock accession online or other entrance in this form. In such a cloud, some defy arise in the resources locate and property discovery. It is precise hard to defend assets from different invasions and onsets.

Nevertheless, the third approach, Hybrid Clouds, is the most preferable in parts of features. This approach provides a private cloud linked to more than one exterior could service, however, information and applications are linked and centrally administrated. It should be noted that the security process of a hybrid cloud is better trustworthy than a public cloud if the structure is arriving over the internet cloud.

Nevertheless, every preparation model has special features and abuses [21]. In fact, every distribution model has its own specified benefit and harm regarding user experiments. The private cloud provides complete control over the user's experiment. However, sometimes, the public cloud does not control the user experience and the hybrid cloud recognizes that controlling the user experience depends on the understanding entered with the user [22]. Table 1 shows the main benefits and the main deficiency of private, public and hybrid clouds**.**

2.2 Edge Cloud Computing

Edge cloud computing leads information, systems, and computing services distant from the cloud servers to the boundary of the network [23]. Self-satisfied supplies and system developers can utilize advanced computing applications by offer services to customs closest to them. Edge cloud computing is described by rising bandwidth, lowest latency, and real-time arrival to scheme info that can be utilized by several systems [24]. A service supply can produce Radio Access Network available to the edge customers by open attain to novel services and systems. Advanced computing alters many modern services for scheme and consumers [25]. Terminal computing utilization situations are entity services, virtual reality, and information caching and video analytics. Hence, these modern computing normative and preparation of Edge frameworks turn into major enablers of additional income streams for vendors, third party and functions. There are some applications where edge computing can be more useful in the real world, such as streaming services, autonomous vehicles and smart Homes. Edge cloud computing can aid reduce dependency on the clouds and enhance the data processing rate. Also, there are actually many recent IoT instruments that have the process and store power availability. The transition to advanced process power allows these devices to be used to their whole potential. A Study [26] discusses key warnings and public security problems: data breach, IP and ARP spoofs, DNS poisons, SQL, LDAP and Os injections and zombie. A paper [27] elaborated on reviewed DDoS attacks and decrease approaches in cloud computing environments.

DDoS technique is a broad denial of service called DoS effect, the variation being the size of the attacks actuation its vulnerabilities, and the attackers number trying to attack the servers. There are three kinds of DDoS attacks, which are application-layer, massive, and protocol attacks. Several kinds of DDoS attacks are UDP, SYN, ICMP and HTTP floods [28]. The belongings of DDoS are lack of business, lack of goodwill, and loss of revenue to product owners. Authors [29] concentrate on the factors that impact cloud security: the data cloud, OS, memory and transaction management. They classify cloud security challenges such as data and privacy issues, infect applications, and confidentiality problems.

They also designed a multi-layer framework for solving cloud security issues which include Virtual Monitoring, Cloud Data, Cloud Storage and Virtual Machine Layers. Authors [30] have categorized cloud security issues into issues of data storage, identity management and access control, and contractual and legal issues. It also categorizes issues into data storage issues: data privacy, integrity, recovery and vulnerabilities, improper media sterilization and data backup. Identity Management and Access Control: A malicious intruder and an outside intruder. Contractual and Legal Issues: Service Level Agreements and Legal Matters. A study [31] surveyed the issues and challenges of cloud security. This study shows Browser based on vulnerabilities like SSL certificate phishing, spoof, and browser cache attacks. The integration data is influenced by low cryptography and a deficiency of powerfulness over the audit, permission, and authentications. It further discusses data theft and loss. Powerless passwords, key recorders, and other deceitful techniques affect recognition theft. Authors [32] discuss the main threats of cloud computing. A threat is information breaches, loss of data and interfaces, unsecured APIs, denial of serving, and account passage hijacking. Furthermore, a social application attack, malware injection attack and phishing attacks are granted. It also describes safety algorithms for Platypus and MD5 in the paper. Authors [33] focus on secured data and the main issues of privacy. They describe security as a collection of privacy, prevention of unauthorized disclosure of information, safety, preventing a modification of unauthorized and its accessibility, and preventing unauthorized withholding of data.

The great challenges in cloud computing are resource security, control, and management. We can divide cloud security into four parts: security systems, cloud server tracking, data privateness, avoidance of illegal insider processes and hijacking services. Network. The authors [34] enlist the next issues of secure cloud computing: data theft, rest, and loss and natural disasters. It furthermore examines privateness and usage issues. Authors in [35] surveyed safety challenges in service bringing forms. Data safety challenges in the SaaS technique are cross-site scripting, approach power fails, Operating Systems and SQL entry defects, cross-site request fraud, cookie tampering, unsecured store and unsecured configuration.

Secure issues of Networks such as incursion, packet analysis, and vulnerabilities in session direction, and uncertain SSL ownership configuration, are valid in the SaaS framework. A paper discussed [36] security in cloud computing issues has been cleared, identified and discovered by the Cloud Security Alliance. Multiple rentals were noted as the key security challenges. Authors in [37] introduce dual main categories of cloud security: Cloud Storage and Cloud Account Security. Cloud Account Security stands for the unity of data stored on untrusted servers. Cloud Account Security shows account validity made by untrusted cloud servers. A basic new Security Cloud protocol has been presented and its processes are discussed extensively in this study. It summarizes three kinds of attacks in this paper. Storage, account, and privacy cheats attack models. It also performed a safety and performance analysis to show the skillfulness of the designed protocol. Security Cloud eliminates each storage and computing challenges of cloud computing. Authors [38] Provides a classification of security challenges, classification of the DDoS attacks and defense techniques in cloud environments. This paper apparently represented the technique of the DDoS attacks and its defensive measure. They also discuss several security issues of the cloud in this study. Potential safety challenges in the cloud service bringing frameworks are DoS, DNS server, IP-based, impersonation, Cross-VM attacks, data breaches, privateness violations, seance hijacking, access control infraction, and physical impairment to infrastructure.

Finally, the powerfulness and failure of DDoS defense techniques have been listed.

3. Key Differences Between Cloud Computing and Edge Computing

Edge computing is a new modern version of cloud computing that minimizes response time by transferring services closer to the final user. Edge computing reduces a load of clouds by giving edge networks the services and resources. Even so, advanced computing constructions cloud by enhancing service to the final user for time lag-sensitive applications [39]. Like the cloud, the providers offer applications for Edge service, data, and storage services to final users.

Although this symmetry in service, there are many significant differences between these two emergent computing models. The major variance between terminal and cloud computing is the location of the servers. The services are computed in the edge networks, while the service is in the clouds inside the internet. The availableness of services in the cloud inside the Internet relies on the multiple hop space among the final user of the servers in the cloud. A safely higher distance between a phone device and cloud server results in a higher time interval in cloud computing compared to the lower time interval set in high-end computing. Likewise, cloud computing has risen noise while peripheral computing has indistinct noise.

As opposed to cloud computing, edge computing aware of the location and provides advanced mobility help. The edge uses a distributive server model comparison with cloud computing that employs a localized model. The potential for attacks of data on the road is advancer in cloud computing than in edge computing resulting from the prolonged way to the servers. The target individuals of cloud computing are the public users on the internet, while the marked subscribers of edge computing are the terminal users. In contrast to the general scale of cloud computing, advanced computing limits, Edge devices have restricted capableness that produces them little ascendable than the clouds. The emergence of advanced computing is not recommended as a complete alternative to cloud computing.

The differences between them can be compared, such as those between racing cars and SUVs which have different purposes and uses. To conclude the main differentiation of the two types, Table 2 presents the main comparisons.

Edge computing is expanding cloud computing as it brings computing services nearer to final users at the edges of the networks. Edge's imagination was formulated to direct the latency rising services of delay-sensitive and frameworks that aren't completely managed inside the model of cloud computing. These applications program has the next needs:

- Extremely low and expected latency.
- Locating awareness.

- Navigation help.

Based on [40], Edge computing is a standalone pattern consisting of much heterogeneous device distribution that connects to the system and performs any computation project such as store and process. Any project can still help the provision based on rental service wherever the individual rents a system and gets motivators in resumption. Fog computing extends the cloud models that bring both services and resources to the backbone networks into the end network [41]. It is a virtual computing system that provides storing and network service in the terminal network. Cloudlet and Mobile-Edge Computing form some similar concepts to the fog computing paradigm. Cloudlet and Mobile-Edge computing only provide services to mobile device users with the flexibility to use locally available resources. However, Fog relies on devices designed by Cisco that possess computational capabilities along with normal device functions such as router and switches.

Differen ce	**Cloud Computing**	**Edge Computing**
Programm-ing Language	The Actual programming is well suitable for clouds, because it makes it a single target platform and uses a single programming language.	Multiple programming platforms can be used, each with different run times.
Security	Requires a lower strong security plan.	Edge computing needs a solid security plan, allowing advanced authentication processes and proactive attack

		remediation.
Suitable Companies	Cloud computing is best suited to enterprises and organizations that deal with large storage of data.	Edge computing is ideal for operations with high latency concerns. Thus, mid-sized companies with budgetary constraints can use edge computing to economize financial resources.

Table 2. A comparison between Cloud Computing and Edge Computing.

4. Cloud security challenges and issues

Although cloud computing has brought a variety of useful services, it also includes many security threats and challenges. Since a lot of information is transmitted across the network and stored in specific resources in the cloud, there are many vulnerabilities that malicious actors can exploit. In this section, we discuss the security state of cloud environments. Security policies consider measures needed to avoid attacks by taking precautionary measures.

These criteria must get the active situation in the clouds without compromising execution and authenticity [42]. The security policies operate based on regulatory authorities and incorporate various service level agreements, client management issues, and prior trust.

Most communities have attempted to concentrate on consumers. Client administration problem as one of the most important concerns in cloud security encompasses many aspects including customer experiences, customer-centered privacy, customer authentication system, and customer service level agreement.

Clients expect their service providers to know their own demands, personal circumstances, and life's difficulties. To provide better services, service providers must know the needs of their customers and provide them with customized solutions. Customer expertise makes a critical goal in using the cloud. This expertness creates organizations capable of offering outputs and services accepted to any consumer. For illustration, there are some cloud profits traced from a people's activity history and their connection to the provider. In recent years, the cloud based on services have enhanced consumer expertise in the marketplace so that many companies are in trouble due to the deficiency of a cloud-found customer framework, while selecting a secure cloud helper institution, will be hard for customers with expertise in safety regions.

Trust is the most serious part of supports to form concerned relations potent. For trust has received little attending in cloud computing, and as an outcome,

deficiency of trust and perceptive in cloud services has reasoned enormous limitation for cloud computing acceptance. This limitation produced a spread between acceptance and invention and effect users of cloud computing doubt this another property of computing. To structure this spread, assurance related to computing must be accepted from a technology and business position [43].

The fast growing of the Edge computing category has opened up the demand for dynamical evaluation frameworks that can appropriate the modifying prospects by dramatic a correct scale between the user's prospects of choice of aided, little time lag and cost, and the service provider's price and functional skillfulness. It is a difficult project to create dynamical and quick evaluation framework, as one pricing model may not be successful for the conflict of many clients. It is also difficult to supply best evaluation framework for heterogeneous Edge computing schemes that can message common payments for service supplies and consumers.

Nevertheless, the evaluation possibility for cloud services [44]. Enhanced cloud security provides a secure information infrastructure. However, considering the human factor of cloud security is a necessity for organizations. To characterize the human role in the security aspect of the cloud, humans can create diverse innovations and solve all problems. In cloud systems, the level of human access to the system varies, so an employee or customer with an administrator access level can play an important role in providing or destroying the system's security. To fix security threats and eliminate vulnerabilities, and technological flaws, human errors and behaviors must definitely be considered. With an increased focus on human behavior, a pattern of vulnerability can be found. After that, social engineering attacks will be monitored and studied in more detail. The more network applications, the more digital crime. Digital forensics plays a vital role in protecting and recovering operational data. Digital forensics is the process used to reveal and interpret electronic data. As the number of users increases in the digital world, it is more likely that illegal malicious users will exploit cloud services. It spread this issue more widely when customers bring in their access devices, including Windows PC, MAC, iPhone and Android smartphones.

However, digital forensics has faced many challenges including the wider scope and the increase in the amount of styles operational in the cloud, which makes it hard to collect and encode information from the various OS on several platforms. Give to a lately publicized study [45], some administrations are interested in their personal and sensitive data held by companies. They are worried that these institutions may utilize the information for aims different than the purposes for which it was collected. Based on this paper, over 93% of companies utilize cloud services at the time, just 23% of them completely trustable public clouds to save their information data safe. While movable to IaaS, the highest serious felt of relevant authorizations is to have steady safety monitoring that provides merged safety with centralized administration over all the cloud infrastructure and conventional data centers. Nevertheless, though confidence services in the public cloud continue to modify over years, published papers on cloud security could ever be presented.

The major interest of cloud customers is how their information is utilized as it is achievable for despiteful information positions to effort this information. A third party can attest, account, and permit secret information and defend the data versus forbidden despiteful individuals. Thus, once it loses the quality of the third party, the cloud situation will be seriously vulnerable and it will cooperate with several security characteristics. In reality, the start period for the limitation is where providers don't experience whereof the resources have given their information of storage their information [46]. So, this issue can be saluted with the next steps. First, the information presented by cloud providers should be encoded using symmetrical keys encryptions techniques. In this stage, TTP petitions and keeps the secure keys to execute data confirmation tasks. At last, the service user can ask for the secret key and implement a process task.

5. Conclusion and The Future Work

Cloud services are present a critical concern of the company's being, as they provide a tremendous chance to speed up business activity through its skill to rapidly expand, letting be flexible in using resources,

And giving new chances for cooperation. In reality, the cloud carries several advantages to organizations, governments, and even states. Regardless of providing many benefits, clouds are quite vulnerable to several security issues. Edge computing and cloud computing are different technologies that cannot replace each other. Edge technology has been accepted by many organizations because of overcoming minor issues of cloud computing. However, it hasn't been proven as it isn't the only solution to the hurdles that IT vendors face. The main objective of this paper is to display all the security issues in cloud environments and to give suitable solutions to fix these difficulties. This survey tries to display several security problems, attacks, and vulnerabilities that hinder the acceptance of edge and cloud computing.

This study gives suitable data for future analysts to understand the cloud computing model and terminal computing and to advance the research to solve unaddressed problems. The future scope purpose is to explore research directions in cloud computing and edge computing.

References

[1] Sittón-Candanedo, Inés, et al. "A review of edge computing reference architectures and a new global edge proposal." *Future Generation Computer Systems* 99 (2019): 278-294.

[2] Alemzero, David Ajene, et al. "Assessing the perceived impact of exploration and production of hydrocarbons on households perspective of environmental regulation in Ghana." *Environmental Science and Pollution Research* (2020): 1-13.

[3] Matinmikko-Blue, Marja, et al. "White Paper on 6G Drivers and the UN SDGs." *arXiv preprint arXiv:2004.14695* (2020).

[4] Varshney, Shefali, Rajinder Sandhu, and P. K. Gupta. "QoS based resource provisioning in cloud computing environment: a technical survey." *International Conference on Advances in Computing and Data Sciences*. Springer, Singapore, 2019.

[5] Galambos, Peter. "Cloud, fog, and mist computing: Advanced robot applications." *IEEE Systems, Man, and Cybernetics Magazine* 6.1 (2020): 41-45.

[6] Priyanka, E. B., S. Thangavel, and Xiao-Zhi Gao. "Review analysis on cloud computing based smart grid technology in the oil pipeline sensor network system." *Petroleum Research*(2020).

[7] Li, Xin, et al. "Internet of Things to network smart devices for ecosystem monitoring." *Science Bulletin* 64.17 (2019): 1234-1245.

[8] Ghobaei-Arani, Mostafa, Alireza Souri, and Ali A. Rahmanian. "Resource management approaches in fog computing: A comprehensive review." *Journal of Grid Computing* (2019): 1-42.

[9] Yang, Song, et al. "Cloudlet placement and task allocation in mobile edge computing." *IEEE Internet of Things Journal* 6.3 (2019): 5853-5863.

[10] Bai, Tong, et al. "Latency minimization for intelligent reflecting surface aided mobile edge computing." *IEEE Journal on Selected Areas in Communications* 38.11 (2020): 2666-2682.

[11] Sabella, Dario, et al. "Edge Computing: from standard to actual infrastructure deployment and software development." *ETSI White Paper* (2019).

[12] Simelane, Sibongile, N. Thirupathi Rao, and Debnath Bhattacharyya. "Significant Security Aspects in Cloud Computing Based Data Centers."

[13] Garg, Sahil, et al. "Edge computing-based security framework for big data analytics in VANETs." *IEEE Network* 33.2 (2019): 72-81.

[14] Khan, Wazir Zada, et al. "Edge computing: A survey." *Future Generation Computer Systems* 97 (2019): 219-235.

[15] Abbas, Nasir, et al. "Mobile edge computing: A survey." *IEEE Internet of Things Journal* 5.1 (2017): 450-465.

[16] Mach, Pavel, and Zdenek Becvar. "Mobile edge computing: A survey on architecture and computation offloading." *IEEE Communications Surveys & Tutorials* 19.3 (2017): 1628-1656.

[17] de Assuncao, Marcos Dias, Alexandre da Silva Veith, and Rajkumar Buyya. "Distributed data stream processing and edge computing: A survey on resource elasticity and future directions." *Journal of Network and Computer Applications* 103 (2018): 1-17.

[18] Elazhary, Hanan. "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms:

Disambiguation and research directions." *Journal of Network and Computer Applications* 128 (2019): 105-140.

[19] Tabrizchi, Hamed, and Marjan Kuchaki Rafsanjani. "A survey on security challenges in cloud computing: issues, threats, and solutions." *The Journal of Supercomputing* (2020): 1-40.

[20] Rajabion, Lila, et al. "Healthcare big data processing mechanisms: the role of cloud computing." *International Journal of Information Management* 49 (2019): 271-289.

[21] Chanal, Poornima M., and Mahabaleshwar S. Kakkasageri. "Security and Privacy in IoT: A Survey." *Wireless Personal Communications* 115.2 (2020): 1667-1693.

[22] Krämer, Michel, Sven Frese, and Arjan Kuijper. "Implementing secure applications in smart city clouds using microservices." *Future Generation Computer Systems* 99 (2019): 308-320.

[23] Khan, Muhammad Khurram, et al. "IEEE Access Special Section Editorial: Mobile Edge Computing and Mobile Cloud Computing: Addressing Heterogeneity and Energy Issues of Compute and Network Resources." *IEEE Access* 8 (2020): 163769-163774.

[24] Alkhalaileh, Mohammad, et al. "Data-intensive application scheduling on mobile edge cloud computing." *Journal of Network and Computer Applications* 167 (2020): 102735.

[25] Gill, Sukhpal Singh, et al. "Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges." *Internet of Things* 8 (2019): 100118.

[26] Schmitt, Daryl W. "A Framework for Cyber Vulnerability Assessments of InfiniBand Networks." (2019).

[27] Hezavehi, Sasha Mahdavi, and Rouhollah Rahmani. "An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing environments." *Cluster Computing* (2020): 1-19.

[28] Vishwakarma, Ruchi, and Ankit Kumar Jain. "A survey of DDoS attacking techniques and defence mechanisms in the IoT network." *Telecommunication Systems* 73.1 (2020): 3-25.

[29] Kumar, Rakesh, and Rinkaj Goyal. "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey." *Computer Science Review* 33 (2019): 1-48.

[30] Thaduri, Adithya, et al. "Cybersecurity for eMaintenance in railway infrastructure: risks and consequences." *International Journal of System Assurance Engineering and Management*10.2 (2019): 149-159.

[31] Gou, Zhaolong, Shingo Yamaguchi, and B. B. Gupta. "Analysis of various security issues and challenges in cloud computing environment: a survey." *Identity Theft: Breakthroughs in Research and Practice*. IGI Global, 2017. 221-247.

[32] Zhang, Tianwei. *Detection and mitigation of security threats in cloud computing*. Diss. Princeton University, 2017.

[33] Ogonji, Mark Mbock, George Okeyo, and Joseph Muliaro Wafula. "A survey on privacy and security of Internet of Things." *Computer Science Review* 38 (2020): 100312.

[34] Dey, Nilanjan, et al., eds. *Big data analytics for intelligent healthcare management*. Academic Press, 2019.

[35] Sridhar, S., and S. Smys. "A survey on cloud security issues and challenges with possible measures." *International Conference on Inventive Research in Engineering and Technology*. Vol. 4. 2016.

[36] Kumar, Shyam Nandan, and Amit Vajpayee. "A survey on secure cloud: security and privacy in cloud computing." *American Journal of Systems and Software* 4.1 (2016): 14-26.

[37] Raji, Abdulmajeed Atoyebi, and Murtada Malik Adam Elhaj. "Enhancing Public Cloud Security by Developing a Model For User Authentication and Data Integrity Checking."

[38] Kalkan, Kubra, Gurkan Gur, and Fatih Alagoz. "Defense mechanisms against DDoS attacks in SDN environment." *IEEE Communications Magazine* 55.9 (2017): 175-179.

[39] Zhang, Haoyu. "Resource Management for Advanced Data Analytics at Large Scale." (2018).

[40] Yousefpour, Ashkan, et al. "All one needs to know about fog computing and related edge computing paradigms: A complete survey." *Journal of Systems Architecture* 98 (2019): 289-330.

[41] Sookhak, Mehdi, et al. "Fog vehicular computing: Augmentation of fog computing using vehicular cloud computing." *IEEE Vehicular Technology Magazine* 12.3 (2017): 55-64.

[42] Wang, Haoxin, et al. "Architectural Design Alternatives based on Cloud/Edge/Fog Computing for Connected Vehicles." *IEEE Communications Surveys & Tutorials* 22.4 (2020): 2349-2377.

[43] Adelaar, R. L. *Cloud computing technology in manufacturing firms-Identifying adoption factors, challenges, and corresponding solutions*. MS thesis. 2020.

[44] Aazam, Mohammad, Sherali Zeadally, and Khaled A. Harras. "Offloading in fog computing for IoT: Review, enabling technologies, and research opportunities." *Future Generation Computer Systems* 87 (2018): 278-289.

[45] Oliveira, Fábio, et al. *A cloud-native monitoring and analytics framework*. Technical Report RC25669, IBM Research, 2017.

[46] Sauerwein, Clemens, et al. "An analysis and classification of public information security data sources used in research and practice." *Computers & security* 82 (2019): 140-155.