# Challenges of cloud computing use: A systematic literature review

*Ibtissam* M'rhaoaurh[1,*], *Chafik* Okar[2], *Abdelwahed* Namir[1], and *Nadia* Chafiq[3]

[1]Laboratory of Technological Information and Modelisation (LTIM), Faculty of Sciences Ben M'Sik, University Hassan II Casablanca, Morocco
[2]Laboratory of Analysis and Modeling Systems for Decision Support (LAMSAD), University Hassan 1st, EST Berrechid, Morocco
[3]Multidisciplinary Laboratory in Sciences and Information, Communication, and Education Technology (LAPSTICE), Faculty of Sciences Ben M'Sik, University Hassan II Casablanca, Morocco

**Abstract.** Background: In recent years, cloud computing has grown vastly. Cloud computing represents a new model for IT service delivery and it typically provides over-a-network, on-demand, self-service access, which is dynamically scalable and elastic, using pools of often virtualized resources. However, this new paradigm is facing diverse challenges from many fronts. Methods: We conducted a systematic literature review of potential challenges of cloud computing. Documents that described challenges of cloud computing were collected of routinely. We grouped identified challenges in taxonomy for a focused international dialogue on solutions. Results: Twenty-three potential challenges were identified and classified in three categories: policy and organizational, technical and legal. The first three categories are deeply rooted in well-known challenges of cloud computing. Conclusions: The simultaneous effect of multiple interacting challenges ranging from technical to intangible issues has greatly complicated advances in cloud computing adoption. A systematic framework of challenges of cloud computing will be essential to accelerate the use of this technology for working well in fact and in order to face with respect to mitigating IT-related cloud computing risks. Keywords: Cloud Computing, Challenges, Systematic literature review

## 1 Background

Recently, Cloud computing has emerged as a buzz word in the ICT industry [1]. Cloud computing has been captivating since 2007 the interest of the Information and Communications Technology community ensuing in a massive amount of industry developments [2]. It has been appreciated as a significant step after Grid computing towards realizing this utility computing, where computing resources are delivered as subscription utility service just such as water and electricity [2]. From business perspective, it is widely viewed as an economic model for renting computing resources [6]. It enables companies to adopt ready-to-use application services through a "pay-as-you go" model that saves cost, resources and time.

Cloud computing has been quickly making spectacular advances in different domains for developing, designing. Besides, a various set of applications like social networking sites, scientific workflow systems, multiplayer gaming portals, and enterprise applications are deploying [7, 27].

According to the National Institute of Standards and Technology (NIST) [3], "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*".

This definition is constituted of cloud architectures, security, and deployment strategies. Specially, five essential elements of cloud computing are precisely identified as shown in below [3]:

*On-demand self-service*: Allows the consumer to be capable of availing real time distant computing resources (such as CPU time, network storage, software use, and so on) according to needs, and without depending upon human intervention.

*Broad network access*: All the resources must be available and accessible to the user universally and simply through the network (e.g. Internet), whatever the customers use (mobile phones, laptops, PDAs, and workstations).

*Resource pooling*: For the purpose of serving multiple consumers using either the multi-tenancy or the virtualization model, the supplier's computing resources are pooled together, with diverse physical and virtual resources dynamically attributed and reassigned conforming to consumer need. Economies of scale and

* Corresponding author: mrhaouarhibtissam12@gmail.com

specialization are two important factors, that pool-based computing paradigm rely on, in order to be set up. The effect of a pool-based model is that physical computing resources become 'invisible' to clients, who in general do not have control or knowledge over the exact location, formation, and originalities of these resources (e.g. database, CPU, etc.) . For example, consumers can't indicate the location where their data will be stocked in the Cloud.

*Rapid elasticity*: One of the characteristics of the cloud computing is the elasticity of the resources. This characteristic allows the users to find quickly new resources so as to be able to answer a rise or a descent in sudden load. It is never obvious to plan the resources

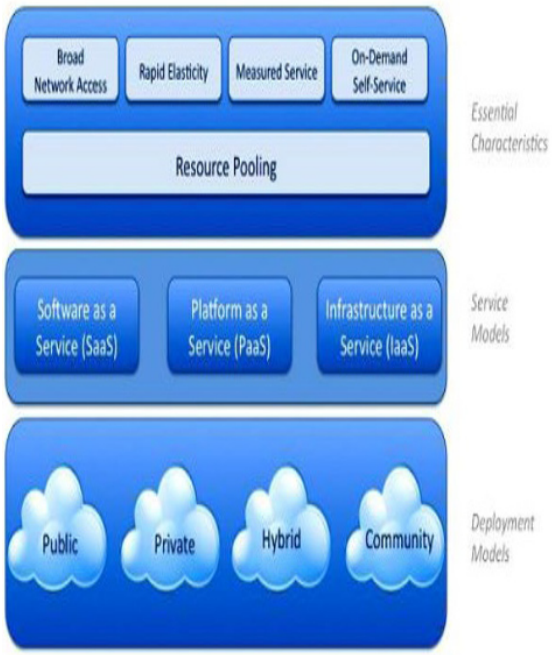


**Fig. 1.** NIST defined Essential characteristics, Service models and Deployment models

which will be vital for the implementation of any IT service, in particular when this need is constantly evolving. The cloud computing so offers a way to release the computing resources necessary for an evolution or for a peak of use of this service.

*Measured Service*: With view to measure the usage of these resources for each individual consumer via its metering capabilities, the cloud infrastructure can use appropriate mechanisms despite of the fact that computing resources are pooled and shared by multiple customers (i.e. multi-tenancy)[36].

As per NIST mainly the Service Model consists of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (as shown in Fig. 1).

Software-as-a-service provides business processes and applications [9] that enable clients to use cloud services running on cloud infrastructure [10] through either a thin client interface, like a Web browser. For instance, Google offers services such as Web applications with similar functionality to traditional office suites, including Gmail, Google Calendar, and Docs, among others. Customers do not need to control or manage the underlying infrastructure design for the reason that all new installations (software and hardware) are automatically updated by application vendors.

Platform-as-a-service delivers a computing platform as an integrated solution, solution stack or services like hardware, operating systems (OSs), and storage through an Internet connection. PaaS enables customers to develop, test, and deploy IT services over a cloud platform. By abstracting the complexity of software and infrastructure, this concept facilitates accordingly the efficient and quick development of Web applications. This model assists businesses in leasing virtual IT services through which to run existing applications, as well as to develop, test, or deploy a new application [10, 11, 12].

Infrastructure-as-a-service is a virtual delivering of computing resources in the form of servers, hardware, networking, and storage services. Rather than installing and purchasing the required resources in their own data center, Clients lease these resources as needed; they don't need to control the underlying cloud infrastructure [13]. IaaS generates potential benefit through controlling and paying for the amount of resources demanded by customers [14].

Moreover, The Cloud model comprises four deployment models:

Private cloud is a cloud computing model that involves a distinct and secure cloud based environment in which only the specified client can operate. By utilizing an underlying pool of physical computing resource and within a virtualized environment, private clouds will offer computing power as a service. However, under the private cloud model, the cloud (the pool of resource) is only accessible by a unique organization, hence providing that organization with confidentiality and greater control. But data transfer cost [15] from local IT infrastructure to a Private Cloud is still rather considerable.

Community clouds are controlled and shared by multiple organizations and support a particular community that has shared interests, such as mission, policy, security requirements and compliance considerations. It may be maintained by the organizations or a third party and may exist at on or off premise, and the members of the community share access to the data and applications in the community cloud. Community cloud users therefore seek to exploit economies of scale while minimizing the costs related to private clouds and the risks related to public clouds [3].

Public cloud is the most known model of cloud computing to many clients is the public cloud model, under which cloud services are offered in a virtualized environment, built via pooled shared physical resources, and available over a public network like the internet. To some degree they can be determined in contract to private clouds which ring-fence the pool of underlying computing resources, creating a distinct cloud platform which is operated solely within a singular organization.

Public clouds deliver services to multiple customers using the same shared infrastructure [3].

Hybrid cloud is a combination of two or more clouds (private, community, or public) that stay unique entities but are related together by standardized or proprietary technology that allows data and application portability. Concerning applications with lacking rigid security, legal, compliance and service level requirements can be deployed in the public cloud, while maintaining business-critical data and services in a protected private cloud [3].

In spite of the widespread adoption of cloud computing, practitioners and researchers have been actively reporting issues and challenges with this new paradigm. Some of the challenges have the aspects of being crucial like issues with confidentiality and security. Other issues such as suboptimal performance and limited bandwidth are a natural result of pushing the barriers of this new model to achieve more [16]. Unless these barriers are better understood, solutions may remain inefficient. We conducted a systematic literature review of potential challenges of cloud computing and used this evidence to group these barriers in a taxonomy that can be used as a framework to facilitate an international dialogue on solutions and instruments. The objective of our research is to gain an understanding of the type of issues and challenges that have been emerging.

## 2 Methods

In this section, we present the research steps followed to perform this review. We conducted a systematic review according to Kitchenham and al. guidelines [18] to elaborate the review methodology in detail and identify documents that reported on challenges of cloud computing. The challenges were defined as obstacles that could impede or delay the adoption of cloud computing or that could limit the usage of cloud computing in companies. As per these authors, the research methodology for systematic review should contain different strategies that are employed for searching the most significant research works like search strings and the chosen digital libraries. At last, the existing studies selection is realized through set criteria.

The following search string represents our generic search query used for this SLR.

("cloud computing" OR "cloud" OR "cloud technologies") AND ("issues" OR "challenges" OR "barriers" OR "threats" OR "limits" OR "risks" of cloud computing).

Additional documentation was identified through a variety of databases (such as ACM Digital Library, IEEE Explore, DBLP, Google Scholar, Science Direct, Scopus, Springer, Taylor & Francis and Wiley Online Library) as shown in Table 1.

**Table 1.** Electronic data sources

| Electronic database | Url |
|---|---|
| ACM Digital Library | http://dl.acm.org/ |
| IEEE Explore | http://ieeexplore.ieee.org/ |
| DBLP | http://dblp.uni-trier.de/ |
| Google Scholar | https://scholar.google.com/ |
| Science Direct | http://www.sciencedirect.com/ |
| Springer | http://www.springer.com/ |
| Scopus | https://www.scopus.com/ |
| Taylor & Francis | http://taylorandfrancis.com/ |
| Wiley Online Library | http://onlinelibrary.wiley.com/ |

With the regard to make this research up-to date and well-intentioned in the area of cloud computing quick search strategy is used. For this end in order to add recent 2015–2017 publications, we have used the quick search strategy for this research by using the filtering tools in the databases. After using the quick search strategy, we considered the publication from 2008 to 2017 overall for the reason that cloud computing publications started around 2008.

As shown in Fig. 2, the initial search resulted in a total of 800 studies, which were condensed to 200 studies on the basis of their titles, and 100 studies on the base of their abstracts. After that, 100 selected studies were reviewed thoroughly for obtaining a final list of 60 studies on the basis of their content.

Sixty studies were ultimately involved in this review. These studies were primarily read and an initial list of challenge descriptions was extracted. This list was grouped into preliminary categories. Challenge descriptions then classified and generalized within their categories. A final taxonomy and description of barriers were established. For each barrier, we also categorized available evidence to identify knowledge gaps.

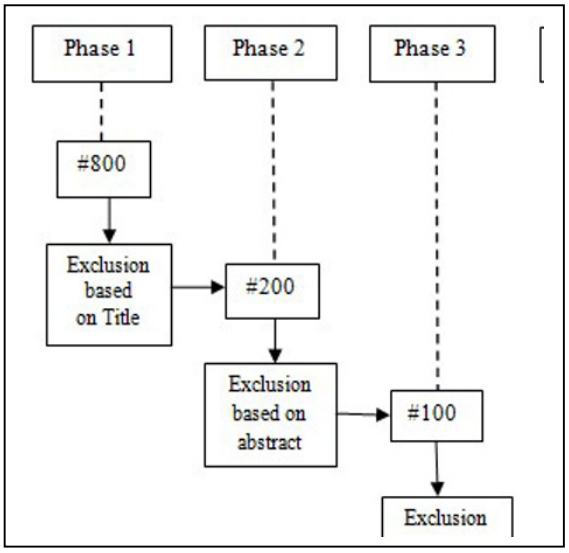


**Fig. 2.** Study selection process

## 3 Results

We identified 23 potential issues of cloud computing and classified these in taxonomy of three categories, according to the organization European Union Agency for Network and Information Security (ENISA) [19, 20, 21, 34, 58]: policy and organizational, technical and legal issues (Table 2). These issues and categories represent a landscape of challenges that is highly dynamic, interconnected, and hierarchical.

Policy and organizational issues

These are business-related IT issues that companies may confront when considering cloud computing service providers [68]. Such issues include lock-in, loss of governance, Compliance challenges, supply chain failure [22].

*Lock-in* vendor lock-in is one of the principal interests declared by IT experts when considering a move from one provider's cloud environment to another [16,20,23]. Lock-in refers to the incapability of a client to move their data and/or programs away from a Cloud Computing risks cloud computing service provider. It is generally the result of proprietary technologies that are incompatible with those of rivals [12, 32, 35, 73].

*Loss of governance*: When adopting Cloud services, the Cloud Customer necessarily concedes control to the Cloud provider on a number of issues which may impact security [20, 21, 58, 67, 73].

*Compliance challenges* customers are accountable for the security of their solution, as they can choose between providers that enable to be analysed by 3rd party organizations that control levels of security and providers that don't [10, 45, 60].

*Supply chain failure* As per ENISA [58], a Cloud provider can deploy parts of its production chain to third parties, or even, as part of its service, use other Cloud Providers. Thus, a potential for cascading failures is produced [20].

Technical issues

These issues for the most part are well understood as part of resilient challenges of cloud computing adoption and continue to form a major obstacle to the availability and use of this technology [78]. They are specified by the failures associated with the technologies and services furnished by the Cloud service vendor [68].

*Malicious insiders* A malicious insider in the cloud might get hands on an unusual quantity of information and on a widely scale [64] and produce various kinds of damage to a Cloud Customers' assets [9, 12, 19, 20].

*Shared technology* Cloud service providers offer their services in a scalable way by sharing infrastructure, platforms, and applications. This way, the threat of shared vulnerabilities exists in all delivery models of Cloud computing [34, 39, 40].

*Encryption* is considered a major risk in cloud computing environments is deficient encryption and key management of data [44-45].

*Multi-tenancy* is a natural result of trying to achieve economic benefit in Cloud Computing by using virtualization and allowing resource sharing [62-63]. However, it is a technological issue in Cloud computing [27, 33, 45, 61].

*Resource and service management* One of the important features of cloud computing is the capacity of obtaining and releasing resources on-demand [20]. The purpose of a service supplier in this situation is to allocate and de-allocate resources from the cloud [23]. Nevertheless, it is not obvious how a service provider can achieve this goal [19, 27, 46].

*Service level agreement (SLA):* it is necessary for customers to have guarantees from suppliers on service offer. Typically, these are offered via Service Level Agreements (SLAs) discussed between the providers and customers [79]. The very first problem is to determine SLA particularizations just like that has a convenient level of granularity expected by a customer from a provider [10, 16, 23].

*Denial of service attacks (DOS)* are attacks meant to impede users of a cloud service to have the ability to access their applications or their data. The attacker (or attackers, as is the case in distributed denial-of service (DDoS) attacks) attacks typically flood servers, systems or networks with traffic by way of obliging the prevents legitimate users to consume inordinate quantities of finite system resources like memory, processor power, disk space or network bandwidth[20, 21, 23]. Consequently, this produces an intolerable system slowdown and leaves all of the victim cloud service perplexed and furious as to why the service isn't responding [9, 12, 19, 42, 43, 73, 77].

*Insecure interfaces and APIs:* with the aim of managing and interacting with cloud services, cloud computing providers offer consumers a set of software interfaces or APIs to exploit [23]. Using these interfaces, provisioning, management, orchestration, and monitoring are all executed. The security of these basic APIs impacts the availability and security of general cloud services. Moreover, companies and third parties

often depend on these interfaces to provide value-added services to clients. This announces the intricacy of the new layered API; it also raises risk [6, 42, 43, 73].

*Data loss or leakage* For both consumers and organizations, perpetually losing one's data is terrifying. Due to causes other than malicious attackers, data stored in the cloud can be obviously lost [10-21]. Any accidental removal by the cloud service vendor, or bad, a physical disaster could lead to the permanent leakage of clients' data [42-45].

*Integrity* The integrity of applications, networks, databases and system software in a shared, globally available cloud environment is threatened by much vulnerability when not adequate and timely patched [4, 9, 16, 28, 54, 67].

*Natural disaster* such as earthquakes, flooding, and tsunamis can impact the infrastructure of a Cloud vendor [20, 21, 24]. Thus, a Cloud Customers might be affected by natural disasters taking place far away from its own location [33, 34, 41, 50].

*Availability* means that the data, service, as well as infrastructure are being accessible to authorized clients immediately after a demand has been made. Availability issues may happen at the customer end or the service

**Table 2.** Evidence for issues of cloud computing adoption

| Category | Issue | Study reference |
|---|---|---|
| Policy and organizational | 1. Lock-in | [12, 16, 20, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 35, 67, 73] |
| | 2. Loss of governance | [20, 21, 58, 67, 73] |
| | 3. Compliance challenges | [10, 19, 21, 33, 41, 44, 45, 47, 58, 60, 67] |
| | 4. Supply chain failure | [20, 58] |
| Technical | 5. Malicious insiders | [9, 12, 19, 20, 23, 24, 26, 27, 33, 34, 37, 38, 39, 40, 41, 42, 43, 73, 76] |
| | 6. Shared technology | [9, 12, 20, 34, 39, 40, 49] |
| | 7. Encryption | [19, 33, 40, 44, 45] |
| | 8. Multi-tenancy | [10, 12, 26, 27, 33, 45,61, 68, 70] |
| | 9. Resource and service management | [19, 20, 23, 24, 27, 46] |
| | 10. Service level agreement (SLA) | [10,16, 23, 24, 27, 28, 33, 45, 47, 48, 49, 50, 51, 74] |
| | 11. Denial of service (DOS) | [9, 12, 19, 20, 21, 25, 27, 29, 37, 38, 41, 42, 43, 73, 77] |
| | 12. Insecure interfaces and APIs | [6, 24, 26, 37, 38, 39, 40, 41, 42, 43, 73] |
| | 13. Data loss or leakage | [10, 19, 20, 21, 26, 27, 34, 37, 40, 42, 45] |
| | 14. Integrity | [4, 9, 16, 22, 23, 24, 25, 28, 33, 34, 38, 41, 44, 45, 50, 53, 54] |
| | 15. Natural disaster | [20, 21, 24, 33, 34, 41, 50] |
| | 16. Availability | [4, 15, 23, 25, 27, 28, 29, 33, 37, 38, 39, 41, 43, 44, 45, 46, 53, 55, 63] |
| | 17. Loss of backups | [4,20, 40, 41, 53, 58, 65, 66, 67, 73] |
| | 18. Data transfer bottlenecks | [15, 23, 24, 36] |
| | 19. Interoperability | [16, 26, 27, 28, 35, 39, 45, 47, 48, 56, 57, 68, 69] |
| Legal | 20. Legal jurisdiction | [16, 19, 20, 21, 23, 24, 33, 34, 36, 67, 73] |
| | 21. Data privacy and protection | [9, 10, 16, 19, 20, 23, 24, 27, 33, 34, 41, 44, 45, 52, 53, 55, 63, 67, 69, 75] |
| | 22. Licensing risk | [15, 19, 20, 29, 58] |
| | 23. Subpoena and e-discovery | [19, 20, 58, 67] |

vendor's end. When a single provider manages a cloud computing service, this way creates a potential environment for a single point of failure [53, 63, 67].

*Loss of backups* The ability to recover data is salient in business that this is not a guarantee of cloud computing [65]. Rather than retrieval, this model depends on heavy backup, which could result privacy issues, as this is likely to lead to uninformed consent. A critical threat is that of 'data loss or leakage' where original data is deleted and cannot be recovered [40]. Data may also be lost due to dishonest media or data being recorded without a link [66, 67, 73].

*Data transfer bottlenecks* arises when bandwidth is unable to accommodate huge quantities of system data at designated data transfer rate speeds [23]. Businesses that use cloud computing have to redesign their present technology into new structures of information from being able to care dynamic and great amounts of information, new filing system and storage technologies [15, 24, 36].

*Interoperability* is the capability of two or more systems work together in order to transfer information and use that transferred data [16-26]. This risk makes difficult for firms to combine their IT systems in the cloud and get productivity gains and cost savings [28, 35, 39].

Legal issues:

These consist of the IT-related issues that are legal in nature, and can also have a negative impact on companies using cloud computing services [16].

*Legal jurisdiction* Converting to Cloud Computing implicates legal restraints [16, 19, 20]. Considering Cloud Computing providers can be multi-national, it is crucial that such vendors are aware of and stand for by national regulations where they do business [36, 67, 73].

*Data privacy and protection*: Privacy is one of the longest standing and most essential interests with cloud computing [59]. Furthermore, it is a major issue in cloud computing for the reason that its very nature involves storing unencrypted data on a machine owned and operated by someone other than the original owner of the data [8, 67, 69].

*Licensing risk* there is also a challenge that firms may pay more than intended to license software on systems hosted by cloud computing service vendors [15, 19, 20, 29, 58].

*Subpoena and e-discovery* If computer systems are confiscated by law enforcement authorities or through civil suits, the centralization of storage and shared location of physical hardware reveal more risk of undesired data divulgence to cloud computing customers [19-20].

## 4 Discussions

Using a systematic review of evidence from reviewed literature, we identified 23 real or potential barriers grouped in taxonomy of policy and organizational, technical and legal issues. Checking the criticality of the situation, many of the significant reports by the organizations including CSA, NIST, and European Union Agency for Network and Information Security (ENISA) etc. have been published to focus the effect of aforestated issues. Reports published by these research major organizations are based on their area of specializations, for example, CSA published reports on the security challenges. These reports are highlighting the risks that are applicable to the cloud computing.

As per [58], most of these threats surround privacy, security and service issues. In other words, above presented threats directly or indirectly impact the confidentiality and security of Cloud resources as well as services at various layers.

Nevertheless, privacy and security risk are considered as a major obstacles to cloud computing adoption that are acting as deterrent and retarding its development [80].

According to table 2, the issues that are addressing data protection and privacy, lock-in, multi-tenancy, availability, integrity, malicious insiders and interoperability have been characterized as essential.

Thus, Most technical issues are deeply embedded in much larger challenges of use of cloud computing. Some solutions are being developed as part of addressing some of aforementioned issues [27]. For instance, to overcome the challenges of privacy and protection, two studies [71, 72] present an architecture adopting data location strategies, trusted cloud services, and trusted service vendors. In order to handle the issues of regulatory compliance, a study [71] propose a concept of cloud market. By means of this, users can exchange with the market and demand resources conforming to the applications' needs through the cloud broker. Furthermore, to avoid vendor lock-in, a layered architecture was proposed by [17]. This architecture offers a unified resource model from different cloud environments.

Political and legal issues will require a different approach. Compared to technical challenges, these challenges are less tangible and transparent and will need to be clearly outlined.

Levels of evidence were also different for each issue. The most challenges were very well documented while no empirical evidence was available for other barriers such as supply chain failure, subpoena and e-discovery and data transfer bottlenecks. In-depth formative research is needed to expand the evidence base of these barriers. As knowledge on these challenges will increase, so will opportunities for solutions.

## Conclusion

Cloud computing is one of the most advanced digital related technologies, which can bring various business benefits to organizations. Despite several benefits constraints exist with the use of this model impacting on service provision and use of this technology, instead of the conventional in-house technologies, which are physically owned and managed on premises. Thence, a considerable amount of literature on this subject has been published in a nearly short time period. In this research work, the issues of cloud computing adoption are collected and classified in a taxonomy of three categories policy and organizational, technical and legal issues. Thus, these challenges must be addressed by the researchers for making cloud computing work well in reality and in order to further gain the confidence of cloud subscribers.

## References

1. R. Buyya, J. Broberg, A. M. Goscinski, "*Cloud Computing: Principles and Paradigms*". ISBN: 978-1-119-14340-6. 664 pages, June (2015).
2. N. Grozev, R. Buyya, "Inter-Cloud architectures and application brokering: taxonomy and survey. Software – practice and experience. Published online 12 December (2012) in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/spe.2168.
3. P . Mell, T. Grance, "The NIST Definition of Cloud Computing, National Institute of Standards and Technology", Information Technology Laboratory, Technical Report Version **15**, (2009).
4. Subashini S., Kavitha V. "A survey on security issues in service delivery models of cloud computing". In: *Journal of Network and Computer Applications* **34**, pp.1-11, (2011).
5. R. Buyya, CS. Yeo, S. Venugopal, J. Broberg, I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility". *Future Generation Computer Systems,* **25**(6), pp.599–616, (2009).
6. G. Lewis, "Basics about cloud computing". Technical Report September, Software Engineering Institute – Carnegie Mellon, (2010).
7. R. Buyya, S. Pandey, C. Vecchiola, "Cloudbus toolkit for market-oriented cloud computing". In *Cloud Computing*, Jaatun M, Zhao G, Rong C (eds) ed:, **5931**. Springer: Berlin / Heidelberg, pp.24–44, (2009).
8. Y. Hu and G. Bai, "A systematic literature review of Cloud Computing in ehealth". In: *Health Informatics-An International Journal (HIIJ)* **3**(4), November (2014).
9. C. Modi et al., "A survey on security issues and solutions at different layers of cloud computing".

*The Journal of Supercomputing*, **63**(2):561–592, (2013)

10. S. Hamouda, "Security and privacy in cloud computing". In *Cloud Computing Technologies, Applications and Management (ICCCTAM), IEEE 2012 International Conference on*, (2012)
11. N. Fernando, SW. Loke, W. Rahayu, "Mobile cloud computing: a survey". *Future Generation Computer Systems* (2013), **29**(1), pp. 84–106.
12. S. Iqbal, M.L.M. Kiah, NB. Anuar, B. Daghighi, Wahab AWA., S. Khan, "Service delivery models of cloud computing: security issues and open challenges". Published online 30 August 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1585.
13. H. Qi et al. Sierpinski triangle based data center architecture in cloud computing. The *Journal of Supercomputing* (2014); **69**(2) , pp.887–907.
14. A.S. Ibrahim et al. Cloudsec: a security monitoring appliance for virtual machines in the iaas cloud model. in Network and System Security (NSS), IEEE 2011 5th International Conference on, (2011)
15. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A Berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.
16. Y. Ghanam, J. Ferreira, F. Maurer. Emerging Issues & Challenges in Cloud Computing— A Hybrid Approach. *Journal of Software Engineering and Applications*, **5**, pp. 923-937, (2012).
17. D. Petcu, G. Macariu, S. Panica, and C. Crăciun, "Portable cloud applications—from theory to practice". In: *Future Generation Computer Systems*, **29**, pp. 1417–1430, (2013).
18. B. Kitchenham, O.P. Brereton, D. Budgen, M. Turner, J. Bailey, S. Linkman, "Systematic literature reviews in software engineering—a systematic literature review". Inform.Softw.Technol. **51**(1), pp. 7–15, (2009).
19. C.L. Liu, W.H. Chen and D.K. Tung, "Identification of Critical Security Issues for Cloud Computing". Applied Mechanics and Materials **145**, pp. 272-276, (2012).
20. C. Daniele, and H. Giles, "Cloud Computing Benefit, risk and recommendations for information security", edited by ENISA, E.U (2009), in press.
21. N. Brender, I. Markov, "Risk perception and risk management in cloud computing: Results from a case study of Swiss companies". In: *International Information Management* **33**, no (5), pp.726-733, (2013).
22. G. Grispos, T. Storer, and W.B.Glisson, "Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics". In: *International Journal of Digital Crime and Forensics*, **4**(2) pp.28-48, (2012).
23. B.B. Rad, T. Diaby, M. E. Rana, "Cloud Computing Adoption: A Short Review of Issues and Challenges". *ICEEG 2017: Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government*, (2017).
24. A. O. Akande, N. A. April, J.P. Van Belle. "Management issues with cloud computing". *ICCC '13: Proceedings of the Second International Conference on Innovative Computing and Cloud Computing*, (2013).
25. A. Chandran, C. K. Shyamala, "Data Management Issues in Cloud Integrated Computing: A Big Picture". *International Conference on Advanced Computing and Communication Systems (ICACCS - 2017)*, Coimbatore, INDIA, (2017).
26. P. Harsh, F. Dudouet, R.G. Cascella, Y. Jegou, and C. Morin, "Using Open Standards for Interoperability Issues, Solutions, and Challenges facing Cloud Computing". *6th International DMTF workshop on Systems and Virtualization Management (SVM 2012) / CNSM (2012).*
27. M.A. Chauhan, M.A. Babar and B. Benatallah, "Architecting cloud-enabled systems: a systematic survey of challenges and solutions". In: *Software: Practice & Experience*, (2016).
28. A. Cardoso, P. Simões, "Cloud computing: Concepts, technologies and challenges". *ViNOrg 2011, CCIS 248*, Springer-Verlag Berlin Heidelberg, pp.127-136, (2012).
29. V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P. Sai Kiran, "Research Issues in Cloud Computing" *Global Journal of Computer Science and Technology*, **1**(11), (2011).
30. J. Guillén, J. Miranda , Murillo J.M,, and Canal C., "A service-oriented framework for developing cross cloud migratable software," *Journal of Systems and Software*, **86**, pp. 2294–2308, (2013).
31. J. Opara-Martins, R. Sahandi and F. Tian, "Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective". In: *Journal of Cloud Computing: Advances, Systems and Applications* **5**(4), (2016).
32. R. Sahandi, A. Alkhalil, J. Opara-Martins, "Cloud Computing from SMEs Perspective: A Survey Based Investigation". *Journal of Information Technology A Publication of the Association of Management* XXIV(1) , pp.1–12, (2013).
33. K. Ullah, and M. N. A. Khan, "Security and Privacy Issues in Cloud Computing Environment: A Survey Paper." *International Journal of Grid and Distributed Computing* **7**(2), pp.89–98, (2014).
34. A. Caldarelli, L. Ferri and M. Maffei, "Expected benefits and perceived risks of cloud computing: an investigation within an Italian setting". *Technology Analysis & Strategic Management*, **29**(2), pp. 167-180, (2017).
35. R. Otuka, D. Preston and E. Pimenidis, "The use and Challenges of Cloud Computing Services in

SMEs in Nigeria". In: *Proceedings of the European Conference on Information Management*, pp.325, (2014).

36. I. Senarathna, W. Yeoh, M. Warren and S. Salzman, "A Conceptual Model for Cloud Computing Adoption by SMEs in Australia". Delivery and Adoption of Cloud Computing Services in Contemporary Organizations, pp.100-128, ( 2015).
37. S. Chhabra, V.S. Dixit, "Cloud Computing: State of the Art and Security Issues". In: *ACM SIGSOFT Software Engineering Notes*, **40** (2), (2015).
38. R. Barona, E.A. Mary Anita, "A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats". In: *International Conference on circuits Power and Computing Technologies [ICCPCT]*, (2017).
39. J. Singh, "Study on Challenges, Opportunities and Predictions in Cloud Computing". In: *International Journal Modern Education and Computer Science*, **3**, pp. 17-27, (2017).
40. CSA (2010). Top ten threats in cloud computing. Cloud Security Alliance, (2010).
41. [41] S.M. Shariati, Abouzarjomehri, M.H. Ahmadzadegan, "Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection". In: *2nd international conference on knowledge-based engineering and innovation*, (2015).
42. CSA (2013). The Notorious Nine: Cloud Computing Top Threats in 2013. Cloud Security Alliance, (2013).
43. G. Ramachandra, M. Iftikhar, F.A. Khan, "A Comprehensive Survey on Security in Cloud Computing". *The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017)*.
44. M. Carroll, A. Merwe, P. Kotzé, "Secure Cloud Computing Benefits, Risks and Controls". In: *Information Security South Africa (ISSA),* pp. 1-9, (2011).
45. R. Prasad Padhy, M. Ranjan Patra, S. Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges". In: *International Journal of Computer Science and Information Technology & Security*, (2011).
46. Q. Zhang, L. Cheng and R. Boutaba, "Cloud computing: state-of-the-art and research challenges". In: *Journal of Internet Services and Applications*, **1**(1), pp.7-18, (2010).
47. S. O. Kuyoro, F. Ibikunle and O. Awodele, "Cloud Computing Security Issues and Challenges". In: *MIPRO* (2010).
48. T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges". In: *24th IEEE International Conference on Advanced Information Networking and Applications*, (2010).
49. K. Mualla, D. Jenkins, "Evaluating Cloud Computing Challenges for Non-Expert Decision-Makers". In: *International Journal of Digital Information and Wireless Communications (IJDIWC)* **5**(4), pp. 285-296 The Society of Digital Information and Wireless Communications, (2015).
50. S. Kumar and R.H. Goudar, "Cloud Computing-Research Issues, Challenges, Architecture, Platforms and Applications: A survey". In: *International Journal of Future Computer and Communication*, **1**(4), (2012).
51. J.H. Morin, J. Aubert and B. Gateau "Towards Cloud Computing SLA Risk Management: Issues and Challenges". In: *45th Hawaii International Conference on System Sciences*, (2012).
52. K. Popović, Ž. Hocenski, "Cloud Computing security issues and challenges". In: *MIPRO* (2010).
53. O. Ali, J. Soar, J. Yong, "Challenges and Issues that are Perceived to Influence Cloud Computing Adoption in Local Government Councils". In: *Proceedings of the IEEE 21st International Conference on Computer Supported Cooperative Work in Design*, (2017).
54. A. Monjur and A.T. Litchfield "Taxonomy for Identification of Security Issues in Cloud Computing Environments". In: *Journal of Computer Information Systems*, **58**(1), pp.79-88, (2016), DOI: 10.1080/08874417.2016.1192520.
55. M. Zaigham, "Data Location and Security Issues in Cloud Computing". In: *International Conference on Emerging Intelligent Data and Web Technologies*, (2011).
56. M.G. Avram (Olaru), "Advantages and challenges of adopting cloud computing from an enterprise perspective". In: *The 7th International Conference Interdisciplinarity in Engineering (INTER-ENG 2013).*
57. P. Goyal, "Enterprise Usability of Cloud Computing Environments: Issues and Challenges". In: *2010 Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, (2010).
58. E. Cayirci, A. Garaga, A. Santana de Oliveira and Y. Roudier, "A risk assessment model for selecting cloud service providers" In: *Journal of Cloud Computing: Advances, Systems and Applications*, **5**(14), (2016).
59. B. Gatewood, "Clouds on the information horizon: How to avoid the storm". Information Management (15352897), **43**(4), pp. 32-36, (2009).
60. D. Yimam and E.B. Fernandez, "A survey of compliance issues in cloud computing". In: *Journal of Internet Services and Applications*, **7**(5), (2016).
61. H. AlJahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, J. Xu, "Multi-Tenancy in Cloud Computing". In: *IEEE 8th International Symposium on Service Oriented System Engineering*, (2014).
62. P. Saripalli, and B. Walters, "QUIRC: a quantitative impact and risk assessment framework for cloud security," *IEEE 2nd International Conference on Cloud Computing* (2010).

63. A. Wayne Jansen," Cloud hooks: security and privacy issues in cloud computing," *Proceedings of the 44th Hawaii International Conference on System Sciences* (2011).
64. A. Duncan, S. Creese, M. Goldsmith, "Insider Attacks in Cloud Computing". In: *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, (2012).
65. P. Hemant, N. P. Chawande, A. Sonule and H. Wani, "Development of servers in cloud computing to solve issues related to security and backup". In: *Proceedings of the IEEE International Conference on Cloud Computing and Intelligence Systems*, pp. 158- 163, (2011).
66. O. Ali, J. Soar and J. Yong, "An investigation of the challenges and issues influencing the adoption of cloud computing in Australian regional municipal governments". In: *Journal of Information Security and Applications*, **27**/**28**, pp. 19-34, (2016).
67. N. Gonzalez, C. Miers, F. Redıgolo, M. Simplıcio, T. Carvalho, M. Naslund and M. Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing". In: *Journal of Cloud Computing: Advances, Systems and Applications*, **1**(11), (2012).
68. R. Latif, H. Abbas, S. Assar, and Q. Ali "Cloud Computing Risk Assessment: A Systematic Literature Review". In: *Future Information Technology*, Lecture Notes in Electrical Engineering, **276**, pp. 285-295, (2014).
69. S. Pearson, A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing". In: *2nd Int Conference on Cloud Computing Technology and Science* (2010).
70. J. Zhu, D. Li, J. Wu, H. Liu, Y. Zhang, J. Zhang, "Towards bandwidth guarantee in multitenancy cloud computing networks". In *Network Protocols (ICNP), 2012 20th IEEE International Conference*, (2012).
71. R. Buyya, S. Pandey, and C. Vecchiola, "Cloudbus toolkit for market-oriented cloud computing," In *Cloud Computing*, ed: Springer, pp. 24–44, (2009).
72. P. Belimpasakis and S. Moloney, "A platform for proving family oriented RESTful services hosted at home". In: *Consumer Electronics, IEEE Transactions on*, **55**, pp. 690–698, (2009).
73. A. Naim, "Cloud Computing: Technology, Security Issues and Solutions". In: *2nd International Conference on Anti-Cyber Crimes (ICACC)*, (2017).
74. A. Shawish, M. Salama, "Cloud Computing:Paradigms and Technologies". F. Xhafa and N. Bessis (eds.), Inter-cooperative Collective Intelligence: Techniques and Applications, Studies in Computational Intelligence 495, DOI: 10.1007/978-3-642-35016-0_2, Springer-Verlag Berlin Heidelberg, (2014).
75. G. Sumit, "Public vs Private vs Hybrid vs Community -Cloud Computing: A Critical Review". I.J. *Computer Network and Information Security*, **3**, pp. 20-29, (2014), DOI:10.5815/ijcnis.2014.03.03
76. A. Duncan, S. Creese, M. Goldsmith, "An overview of insider attacks in cloud computing". In: *Concurrency And Computation: Practice And Experience*, **27**, pp. 2964–2981, (2014) in Wiley Online Library. DOI: 10.1002/cpe.3243.
77. T.K. Damenu, C. Balakrishna, "Cloud Security Risk Management A Critical Review". In: *9th International Conference on Next Generation Mobile Applications, Services and Technologies*, (2015)
78. A. Dutta, G. C. A. Peng and A. Choudhary, "Risks in Enterprise Cloud Computing: The Perspective of it Experts", *Journal of Computer Information Systems*, **53**(4), pp. 39-48, (2013), DOI: 10.1080/08874417.2013.11645649
79. M. Ahmed and A. T. Litchfield, "Taxonomy for Identification of Security Issues in Cloud Computing Environments", *Journal of Computer Information Systems*, **58**(1), pp. 79-88, (2018), DOI: 10.1080/08874417.2016.1192520
80. D. Zissis, D. Lekkas, "Addressing cloud computing security issues". *Future Generation Computer Systems,* **28**, pp. 583–592, (2012)