# Cloud Computing: Potential Risks and Security Approaches

Hassen Ben Rebah[1(✉)] and Hatem Ben Sta[2,3]

[1] Higher Institute of Technological Studies, Mahdia, Tunisia
ben_rebah_h@yahoo.fr
[2] SOIE Lab, LR11ES03, Higher Institute of Management,
University of Tunis, 2000 Tunis, Tunisia
hatem.bensta@gmail.com
[3] Higher Institute of Computer Science, University of Tunis El Manar,
2080 Tunis, Tunisia

**Abstract.** Cloud Computing is a new technology, widely used in different areas, allowing easy and on-demand access through the internet to a shared set of configurable computing resources. The adoption of this new technology within companies is restricted by security constraints. In this paper, we present the most significant risks that could affect organizations intending to deploy Cloud technology and security measures to be in place to reduce the impact of risks based on a literature review.

**Keywords:** Cloud computing · Potential risks · Counter-measure · Threat

## 1 Introduction

Cloud Computing is a new processing scheme in which computer processing is performed in the Internet "Cloud" [1]. This new technology based on virtualization has become essential in the progress and provision of IT services for organizations. It is considered by them as a method to raise automatically their abilities of storing, deploying web services, database management and sharing data without affording in new infrastructure, training new employer, or licensing new software. In spite of all this advantages, clients are still not enthusiastic to deploy their business in the cloud [2] since it presents new security issues which has not been well realized [3] and which needs to be carefully evaluated before any engagement in this area [4]. According to a survey conducted by Fujitsu Research Institute in 2010, 88% of potential cloud consumers are afraid of who has access to their data, and demanded more caution of what goes on in the backend physical server [5]. The main contribution presents the potential risks related to cloud computing environment and security measures to reduce the impacts of these risks based on literature review.

This paper is divided into two sections: the first section presents Cloud Computing technology: its models, its services and its characteristics. The second section presents the potential risks related to this technology and the safety measures to be in place to reduce the impacts of these risks. It contains also a literature review of previous research involving several evidence classifications of risks that affected the cloud environment. Finally, we will wrap up our paper with a conclusion.

T.F. Bissyande and O. Sie (Eds.): AFRICOMM 2016, LNICST 208, pp. 69–78, 2018.
https://doi.org/10.1007/978-3-319-66742-3_7

## 2 Cloud Computing

According to the National Institute for Standards and Technology (NIST)[1], cloud computing is a model for enabling ubiquitous, convenient and 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 a minimal management effort or service provider interaction [6].

### 2.1 Cloud Computing Architecture

Cloud computing is composed of two sections: the front end and the back end. These latters are connected with each other through a network infrastructure, normally the Internet. Front end is that the user can see, it includes the hardware and software equipments necessary to access the cloud (e.g. Web browsers like Internet Explorer or Firefox) and the back end is composed of cloud computing services such as servers, data storage and various computers. Traffic control operations, administration system and user request are managed by a central sever. It keeps some rules and uses particular software named middleware. This last permits networked computers to communicate with each other [7, 8]. End user is able to use the cloud computing services via the Internet network from any location (home, work, etc.) and through any device (phone, laptop, etc.). Generally, these services are governed by a service-level agreement (SLA) between customer and cloud service provider (CSP), it specifies requirement, quality of service, cost, etc.

### 2.2 Cloud Computing Characteristics

Cloud computing has five key characteristics as described by Melland Grance:

- On-demand self service: a consumer can one-sidedly provide computing capabilities when necessary automatically without contacting the hosting provider [6, 8].
- Broad network access: the hosted application is available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as laptop, Smartphone, etc. [6, 8].
- Resource pooling: the provider's computing resources are shared to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand [6, 8].
- Rapid elasticity: cloud service can be rapidly and elastically provisioned and released to quickly scale up or down commensurate with demand [6, 8].
- Measured service: cloud computing resource can be monitored, controlled, and reported providing transparency for both the provider and the consumer of the utilized service. Cloud computing services use a metering capability which allows to control and optimize resource use based on pay per use model [6, 8].

[1] http://www.nist.gov.

### 2.3 Cloud Computing Deployment Models

Cloud computing represents four deployment models:

- Private cloud: the cloud infrastructure is set up for exclusive use by a specific organization which incorporates many consumers such us business units [9, 10].
- Community cloud: the cloud infrastructure is shared by a specific community of consumers from organizations that have the same interests such as mission and policy [9, 10].
- Public cloud: The cloud infrastructure is made available to a big number of consumers and owned by a service provider [9, 10].
- Hybrid cloud: The cloud infrastructure is a composition of two or more different cloud (private, community, or public) that remain unique entities [9, 10].

### 2.4 Cloud Computing Service Models

Cloud computing offers three types of services:

- Software as a Service: the ability provided to the user is to use the provider's applications running on a cloud infrastructure. The applications are available to various clients through a thin client interface such as a web browser [6, 11].
- Platform as a Service: the capacity allowed to the user to deploy on the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, etc. [6, 11].
- Infrastructure as a Service: The ability available for the user to provide him with IT infrastructure (processing, storage networks, etc.) [6, 11].

## 3 Security Problems in Cloud Computing

The immaturity of cloud computing technology has posed many issues such as security [12, 13], virtualization [14], network [15] and fault tolerance problems [16]. But security issues are the most important ones for the consumer who is seeking a comfortable service in terms of integrity privacy, availability, etc. According to a research conducted in 2009 by Fujitsu on problems of cloud computing from the user viewpoint which revealed that security problems are the most important ones with 73% [1]. The security problems associated with cloud computing is being treated by different organizations and several studies done by many researchers. These latters have classified them in different dimensions. Cloud Security Alliance (CSA) is a non-profit American organization formed to advance the use of the best practices for providing security assurance within cloud computing and provide education on the uses of cloud computing to help secure all others forms of computing [17]. This organization defined in 2010 a guideline that describes necessary security considerations for performing critical tasks on a cloud computing divided into 13 domains (e.g. Governance and enterprise risk management, compliance and audit, application security, Identity and access management, virtualization, etc.) [1]. The European Network and Information Security Agency (ENISA) estimated in a report submitted en 2009 35 types of security risks in cloud computing [18]. Gartner 2008 fixed seven security issues that must be verified by the customer before choosing a cloud computing provider (e.g. privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability) [19]. [11, 20] presented a categorization of security issues for cloud computing focused on its service models (SaaS, PaaS, and IaaS) who identified the main liabilities in this type of systems, the most important risks found in the literature and all available counter-measures for these threats and vulnerabilities. [17] gave the key security issues in cloud computing environment (e.g. data transmission, network security, data privacy, data integrity, etc.) and presented some recommendations to reduce the impacts of these risks. [21] provided two categorizations of security issues related to cloud computing (threats for cloud service users and threats for cloud service providers) based on analysis of its technical components. This classification was also justified by [22] through a systematic literature review.

## 3.1 Potential Risks Related to Cloud Computing

In the literature, there are many definitions of the term “risk”. According to the ISO/CEI 13335-1:2004 risk means “The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence”. With threat means “a potential cause of an incident that may result in harm to a system or organization” and vulnerability means “a weakness of an asset or group of assets that can be exploited by one or more threats” [23].

In 2009, ENISA presented a report in which it suggested the most nine influential risks on organizations mentioned below:

**Loss of governance:** when using the cloud infrastructure, the cloud client gives supervision to the cloud provider on various issues [24]. This loss of governance relies on the cloud service models for example in case of IaaS, organization cedes hardware and network management to the provider, while SaaS also cedes OS, application, and service integration in order to give a turnkey service to the cloud service customer. This loss of control can result a lack of confidentiality, integrity and availability of data [21].

**Lock-in:** lock-in means incapability of the cloud user to move from one provider to another or migrate data and services back to an in-house IT environment. This introduces a reliance on a specific cloud provider for service provision, especially if data portability, as the most important feature, is not enabled [24]. According to [21], this risk can also affect a cloud provider (Supplier Lock-in) when several supplier-dependent modules or workflows are used for integration or functionality extension.

**Isolation failure:** multi-tenancy and shared resources are a two essential feature of cloud computing based on the virtualization technology. Although this technology is utilized by many providers to maximize the use of hardware [25] but it has many gaps because it is not designed to offer strong isolation properties for a multi-tenant architecture [26]. In fact, it leads hackers to a full access to the host and cross-VM side channel attacks to take out information from the specific VM on the same machine [22]. Also, data from multiple occupiers is saved in a shared database, the threat of data leakage among these occupiers is high [27].

**Compliance risks:** traditional service providers are subject to external audits and security certifications. If a cloud service provider does not adhere to these security audits, then it results an obvious decrease in client trust [28]. This risk arises because of lack of governance over audits and industry standard assessments [17]. Organizations which implement the audit and compliance to the internal and external processes search to get certification. These enterprises may be put at risk since cloud computing service providers may not be capable to show evidence of their own compliance with the necessary needs or may not permit an audit by cloud customer [29].

**Data location:** generally, when a customer uses the cloud, he does not know the exact location of his data and he also does not have any supervision over the physical access techniques to that data. The majority of cloud service provider possesses data centers in many places in the world. This situation can be considered as an issue in several cases [30]. On the one hand, the cloud provider should not only store and process data in specific jurisdictions but should also respect the privacy regulations of those jurisdictions in different countries all over the world [31]. On the other hand, it is hard to determine the appropriate security procedures are in place to protect customers' data [32].

**Management interface compromise:** the customer management interface that cloud providers give is accessible through the internet. These interfaces offer users the possibility to access to a large set of resources. This may pose a real menace if web browser vulnerabilities are there. This includes customer interfaces supervising many virtual machines and, more than that, cloud provider interfaces supervising the operation of the entire cloud system [18].

**Data protection:** cloud computing shows various data protection risks for both cloud customers and providers. In some cases, it may be difficult for the cloud user to effectively check the data handling practices of the cloud provider and, therefore, to be certain that the data is handled in a legal way. This issue is more complicated in cases of multiple transfers of data, e.g. between federated clouds. An organization cannot verify how a cloud provider handles its data and thus cannot establish either the practices employed are lawful or not. Data flowing from the Internet is full of malware and packets intended to lure users into unknowing participation in criminal activities. Although this defiance is more difficult, some cloud providers have obtained certified levels regarding to data handling [24].

**Insecure or incomplete data deletion:** in fact, the user who can erase data is in relation with the separation issue which is defined by multi-tenant usage mode [33]. In a public cloud, a user can ask the provider to delete completely some of his data. This request can be impossible or undesirable because the copies of data are on multiple disks belonging to many data centers located in several countries around the world and are shared with other customers [34]. In this case, data is supposed to be removed completely from the cloud but according to the physical characteristics of storage support, the data still exit and may be restored. This problem can be considered as a major risk to the users [35].

**Malicious insider:** this risk which is well-known to most organizations is a result of staff hired by cloud service providers. Those employees are offered a level of access that may enable them to get confidential data and complete control over the cloud services without any risk of detection. Cloud Service Providers show little or no transparency on how they hire employees, how they give them access to cloud resources or how they monitor them. Bad insiders can directly affect financial consequences and productivity of organizations [26, 36].

The table below represents the list of risks mentioned above classified in terms of their types and their impacts to the organizations. The impact is listed as "Medium" which is scored as1and "High" which is scored as 2 (Table 1).

**Table 1.** Classification of potential risks of cloud computing

| Risk | Type | Impact 1: Medium - 2: High |
|---|---|---|
| Loss of governance | Organizational | 2 |
| Lock-in | Technical | 1 |
| Isolation failure | Technical | 2 |
| Compliance risks | Organizational | 2 |
| Management interface compromise | Technical | 2 |
| Data protection | Technical | 1 |
| Insecure or incomplete data deletion | Technical | 2 |
| Malicious insider | Technical | 2 |
| Data location | Technical | 2 |

### 3.2 Counter-Measure of Potential Risks

The successful implementation of cloud computing technology requires the development and implementation of several security management policies and mechanisms. In the following table, we present some safety measures to reduce the impacts of potential risks of cloud computing mentioned above.

In Table 2, with reference to a literature review, we have listed the measures of security that must be applied by cloud service providers and the organizations to reduce the impacts of the potential risks of cloud computing.

**Table 2.** Risks and counter-measure

| Risk | Counter-measure |
|---|---|
| Loss of governance | • Execute carefully Service Level Agreements (SLA)<br>• Define clearly the role and responsibility between cloud service provider, cloud service user, data owner related to data ownership, access control, infrastructure maintenance<br>• Secure and maintain properly all documents which should be available to the customer at all times<br>• Define common frameworks for certification such as COBIT or ISO [4, 29, 36] |

(*continued*)

**Table 2.** (*continued*)

| Risk | Counter-measure |
|---|---|
| Lock-in | • Promote standardized technology and Application Programming Interface (API)<br>• Use Free Libre Open Source Software (FLOSS) which accompanied increasingly standardization initiatives such as Apache CloudStack, OpenStack and Eucalyptus<br>• Develop applications based on a generic functional base such as LibCloud or Deltacloud in the case of IaaS and SimpleCloud in the case of PaaS<br>• Choose a specialist technical operator (Technical cloud brokers) that avoids lock-in and uses simultaneously several cloud services<br>• Establish an exit strategy<br>• Implement the hybrid cloud model which can solve the problem of compatibility issue [22, 29, 36–38] |
| Isolation failure | • Implement a better security practices for installation/configuration<br>• Monitor environment for illegal changes/activity<br>• Develop strong authentication and access control for administrative access and operations<br>• Promote Service Level Agreements for patching and vulnerability remediation<br>• Conduct vulnerability scanning and configuration audits<br>• Use effective encryption methods to guarantee data isolation between clients [22, 26, 29, 36] |
| Compliance risks | • Conduct internal and external audits regularly on a basis to verify cloud service provider to match terms, standards and regulations<br>• Ensure that cloud service provider should give evidence that data, saved only in geographic locations, allowed just by a formal contract (SLA)<br>• Ensure that requirements meet the data location<br>• Comply location with well-defined laws and regulations<br>• Incorporate and document laws and regulations formally in governance policies [17, 29, 36, 39] |
| Management interface compromise | • Provide remote access with a secure protocol<br>• Patch completely web browser vulnerabilities before providing remote access<br>• Promote a strong authentication strategy (avoid only a simple authentication by password)<br>• Plan periodic and efficient OS and hardware hardening procedures on the cloud system [26, 29] |
| Data protection | • Ensure that cloud service provider abides by all the regulations, including HIPPA and FISMA, within the same country, regarding cloud security<br>• Make sure that cloud service provider has to meet the legal systems under different jurisdictions without so much visibility where the data resides and how it is set up through various legal jurisdictions [22] |

(*continued*)

**Table 2.** (*continued*)

| Risk | Counter-measure |
|---|---|
| Insecure or incomplete data deletion | • Ensure that the provider should define policies to set up procedures for the destruction of persistent media before getting rid of it<br>• Ensure that providers should define very strong encryption strategies [22, 26] |
| Malicious insider | • Require transparency in all information security and management practices in addition to compliance reporting<br>• Determine and report security breach notification processes<br>• Promote strict supply chain management and conduct a comprehensive-supplier assessment<br>• Make sure that human resource requirements are part of legal contracts [26, 29, 36] |
| Data location | • Offer information to consumers about where their data stored and processed<br>• Ensure that cloud service provider should guarantee safe operation of the cloud data center to grant a secure physical location for customers' data<br>• Verify that the cloud service provider should store and process data in specific jurisdictions and respect the privacy regulations of those jurisdictions [36, 40, 41] |

## 4 Conclusion

Cloud computing is an economic and technological revolution in which computing resources are provided as a service over the Internet. However, adoption of this technology remains low due to of several safety problems related to virtualization technology, deployment models, service models and network architecture. In this paper, we have focused on the potential risks related to cloud computing and we suggested a number of controls that could be considered for the mitigation of these controversial issues. Several studies have demonstrated that the adoption of hybrid cloud computing can be an effective strategy for a wide variety of companies which are more concerned with security. What are the limitations of this model? And does it really meet the growing needs of security companies?

## References

1. Okuhara, M., Shiozaki, S.T.: Security architectures for cloud computing. Fujitsu Sci. Tech. J. **46**, 397–402 (2010)
2. Kuyoro, S.O., Ibikunle, F., Awodele, O.: Cloud computing security issues and challenges. Int. J. Comput. Netw. **3**, 247–255 (2011)
3. Wang, Q., Wang, C., Li, J., Ren, K., Lou, W.: Enabling public verifiability and data dynamics for storage security in cloud computing. In: European Conference on Research in Computer Security, pp. 355–370 (2009)

4. Brender, N., Markov, I.: Risk perception and risk management in cloud computing: results from a case study of Swiss companies. Int. J. Inf. Manag. **33**, 726–733 (2013)
5. Fujitsu Research Institute, Personal data in the cloud: A global survey of consumer attitudes. http://www.fujitsu.com/downloads/SOL/fai/reports/fujitsu_personal-data-in-the-cloud.pdf
6. Mell, P., Grance, T.: The NIST definition of cloud computing (v15), National Institute of Standards and Technology (NIST) (2009). http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
7. Jadeja, Y., Modi, K.: Cloud computing - concepts, architecture and challenges. In: International Conference on Computing, Electronics and Electrical Technologies (2012)
8. Saggar, R., Saggar, S., Khurana, N.: Cloud computing: designing different system architecture depending on real-world examples. Int. J. Comput. Sci. Inf. Technol. **5**, 5025–5029 (2014)
9. Zissis, D., Lekkas, D.: Addressing cloud computing security issues. Future Gener. Comput. Syst. **28**, 583–592 (2012)
10. Al Morsy, M., Grundy, J., Müller, I.: An analysis of the cloud computing security problem. In: Proceedings of APSEC 2010 Cloud Workshop (2010)
11. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**, 1–11 (2011)
12. Begum, F.: Cloud computing and its security concerns a survey. Int. J. Res. **3**, 1082–1088 (2014)
13. Raj, B.J.: Cloud computing security issues in infrastructure as a service. Int. J. Adv. Res. Trends Eng. Technol. **2**, 246–250 (2015)
14. Shwetha, S.: Survey on security issues and problems in cloud computing virtual machines. Int. J. Comput. Sci. Inf. Technol. **4**, 755–760 (2013)
15. Patidar, P., Bhardwaj, A.: Network security through SSL in cloud computing environment. Int. J. Comput. Sci. Inf. Technol. **2**, 2800–2803 (2011)
16. Bala, A., Chana, I.: Fault tolerance- challenges, techniques and implementation in cloud computing. Int. J. Comput. Sci. Issues **9**, 288–293 (2012)
17. Padhy, R.P., Patra, M.R., Satapathy, S.C.: Cloud computing: security issues and research challenges. Int. J. Comput. Sci. Inf. Technol. Secur. **1**, 136–146 (2011)
18. European Network and Information Security Agency (ENISA). https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
19. Gartner. http://www.infoworld.com/article/2652198/security/gartner–seven-cloud-computing-security-risks.html
20. Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B.: An analysis of security issues for cloud computing. J. Internet Serv. Appl. **4**, 1–13 (2013)
21. Lee, K.: Security threats in cloud computing environments. Int. J. Secur. Appl. **6**, 25–32 (2012)
22. Latif, R., Abbas, H., Assar, S., Ali, Q.: Cloud computing risk assessment: a systematic literature review. Future Inf. Technol. **276**, 285–295 (2013)
23. The Great Seal of the seal of approval. https://law.resource.org/pub/in/bis/S04/is.iso.iec.13335.1.2004.pdf
24. Kulkarni, G., Gambhir, J., Patil, T., Dongare, A.: A security aspects in cloud computing. In: IEEE 3rd International Conference on Computer Science and Automation Engineering, pp. 547–550 (2012)
25. Pearson, S., Benameur, A.: Privacy, security and trust issues arising from cloud computing. In: IEEE Second Conference on Cloud Computing Technology and Science (2010)
26. Shah, H., Anandane, S.S., Shrikanth, S.: Security issues on cloud computing. Int. J. Comput. Sci. Inf. Secur. **11**, 25–34 (2013)

27. Hashizume, K., Rosado, D.G., Medina, E.F., Fernandez, E.: An analysis of security issues for cloud computing. J. Internet Serv. Appl. **4**, 1–13 (2013)
28. Chou, Y., Oetting, J.: Risk assessment for cloud-based IT systems. Int. J. Grid High Perform. Comput. **3**, 1–13 (2011)
29. Tripathi, A., Mishra, A.: Cloud computing security considerations. In: IEEE International Conference on Signal Processing, Communications and Computing, pp. 1–5 (2011)
30. Kleber, V., Schulter, A., Westphall, C.B., Westphall, C.M.: Intrusion detection techniques for grid and cloud computing environment. IT Professional IEEE Comput. **12**, 38–43 (2010)
31. Julisch, K., Hall, M.: Security and control in the cloud. Inf. Secur. J. Global Perspect. **19**, 299–309 (2010)
32. Khajeh-Hosseini, A., Sommerville, I., Bogaerts, J., Teregowda, P.: Decision support tools for cloud migration in the enterprise. In: IEEE International Conference on Cloud Computing, pp. 541–548 (2011)
33. Adineh, M., Hariri, N.: Risks identification and ranking in information technology projects based on cloud computing. Kuwait Chapter Arab. J. Bus. Manag. Rev. **3**, 216–277 (2014)
34. Ayala, L.C., Vega, M., Vargas, L.M.: Emerging threats, risk and attacks in distributed systems: cloud computing. Innov. Adv. Comput. Inf. Syst. Sci. Eng. **152**, 37–51 (2013)
35. Rahul, S.S., Rai, J.K.: Security & privacy issues in cloud computing. Int. J. Eng. Res. Technol. **2**, 1–6 (2013)
36. Youssef, E.A., Alageel, M.: A framework for secure cloud computing. Int. J. Comput. Sci. Issues **9**, 487–500 (2012)
37. Viseur, R., Charlier, E., Van de borne, M.: Comment gérer le risque de lock-in technique en cas d’usage de services de cloud computing? 16ème colloque CREIS-TERMINAL (2014)
38. Hwang, K., Li, D.: Trusted cloud computing with secure resources and data coloring. IEEE Comput. Soc. **14**, 14–21 (2010)
39. Rittinghouse, J.W., Ransome, J.F.: Cloud Computing: Implementation, Management, and Security, pp. 301–308. CRC Press, Boca Raton (2010)
40. Julisch, K., Hall, M.: Security and control in the cloud. Inf. Secur. J. Glob. Perspect. **19**, 299–309 (2010)
41. Kumar, A.: World of cloud computing & security. Int. J. Cloud Comput. Serv. Sci. **1**, 53–58 (2012)