International Journal of
Distributed Computing and Technology

ISSN: 2455-7307
Volume 10, Issue 2, 2024
July—December
DOI (Journal): 0.37628/IJDCT

https://journalspub.com/journal/ijdct

Review IJDCT

A Simplified Review on Cloud Computing Security Vulnerabilities

Rajesh Yadav*

Abstract

Cloud computing is the joint source of the computer system resources that are verily configured as well as the high-level services that can be delivered via the internet with minimal effort of the respective administrator. However, these advantages along with the security concerns are also quite prevalent. It is very important for the customers to know the risks and vulnerabilities in cloud services that might exist while considering counter measures before moving storage, applications, and computing to the cloud. In the cloud, the development of risks comes together with the source of the vulnerabilities and the most effective measures which should then be spread through restricting in-cloud reinforcement steps. This review paper talks about the vulnerabilities that are likely to creep in and the measures to combat them. Also, it suggests a list of preventive measures that can be taken by focusing on each hazard. The paper also discusses various types of clouds – private, public and hybrid cloud and services like SaaS, IaaS and PaaS that are provided by the cloud. A tabular representation of vulnerabilities and problems associated with it gives an easy understanding to user and helps them to decide what measures can be taken for prevention and safety.

Keywords: Cloud computing, security vulnerabilities, cloud service provider, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), security systems

INTRODUCTION

The "cloud" is defined as a collection of hardware, connectivity, storage, connectivity, and services used to provide multiple computing domains as a service over a network or over the internet. The idea dates to the twentieth century. It provides software and platforms as a service. It is highly adaptable and affordable. Many services run on the cloud, including email, web conferencing, and customer relationship management (CRM). Google Docs, Microsoft One Drive, and Dropbox are examples of free or affordable online storage for consumers. The cloud provides both remote services for customers, allowing them to store data on the network and work without common equipment. The cloud provides a variety of services to customers, including accountability, flexibility, reliability, efficiency, and critical features. Cloud computing is also known as distributed network computing [1]. It delivers information, services, and applications to customers over the internet. The cloud provides ample data storage, allowing users to share and store data faster.

***Author for Correspondence**
Rajesh Yadav
E-mail: ry280888@gmail.com

Assistant Professor, Department of Computer Science, SIES College of Arts, Science & Commerce (Empowered Autonomous), Mumbai, Maharashtra, India

Received Date: September 7, 2024
Accepted Date: September 15, 2024
Published Date: November 13, 2024

Citation: Rajesh Yadav. A Simplified Review on Cloud Computing Security Vulnerabilities. International Journal of Distributed Computing and Technology. 2024; 10(2): 26–34p.

According to NIST (National Institute of Standards and Technology), cloud computing is defined as "a method for enabling appropriate, on-demand network access to a shared pool of computer resources that may be quickly configured and made available with minimal organizational effort" [2].

When a consumer wants to use well-known social networking sites such as Facebook or Twitter, they merely need an internet connection to log in. These websites allow users to exchange images, movies, and other multimedia information late in 2007. Here are definitions of cloud computing:

- Cloud computing is a style of computing where massively scalable IT-related capabilities are provided "as a service" across the internet to multiple external customers;
- A pool of abstracted, highly scalable, and managed infrastructure capable of hosting end customer applications and billed by consumption;
- An emerging computing paradigm where data and services reside in massively scalable data centers and can be ubiquitously accessed from any connected devices over the internet [3].

Now what we know about the idea is realized. Due to the integration of the cloud ecosystem, security is considered one of the most important issues. For example, cloud data is stored remotely, and the owner cannot access it directly. Security is a major issue towards the introduction of cloud computing reporting due to the lack of clarity on how to achieve full reliability [4]. In a threat environment, customers may need to share and store their computing devices on cloud servers, thus losing control over physical security [5]. Unfortunately, the cloud service provider (CSP) manages and owns the servers. It is possible for the CSP to directly edit user data. Customer information may be disclosed to other customers requiring knowledge or consent. Security has become a major concern in cloud computing. This paper discusses vulnerabilities and defenses for security-related issues.

In the cloud, the cloud provider is responsible for implementing and maintaining effective security measures. To dispel consumer concerns about this issue, some consumers point to sources which indicate that their information and requests are properly protected [6]. To experience the full model of the software, the previous automatic authentication settings and security challenges should be fixed. To ensure that only authorized users have secure access to these virtual images, security layers are provided and managed together with the virtual machine hypervisor. Gateways provide data access and storage through the cloud. Cloud storage can store large amount of information. The cloud automation model consists of multiple data centers. Monitoring, operation and management of wide-area network (WAN) data is performed by a Network Operations Center (NOC). The use of cloud computing is plagued by security concerns. Cyber-attack is one of the biggest problems in network and data security [7].

In recent years, cloud computing has received a lot of attention to understanding its security challenges. Threats to the organization's security can come from both inside and outside the company. Users are not aware of the occurrence of unexpected internal risks [8]. According to the Cybersecurity Surveillance Survey of 607 organizations, government officials, experts and consultants, insiders cause 22% of cyberattacks [1]. Unauthorized and inadvertent disclosure of sensitive data, viruses, worms, and theft of intellectual property are the most common types of attacks. In 2016, the FBI detected four thousand ransomware attacks every day. Additionally, victims and law enforcement have experienced 36 crypto-ransom attacks in the past four years. Hackers thus gain illegal access to user data in the cloud. Using various methods, they collect personal data for illegal purposes [6]. In addition, several breaches were reported in 2019 in various areas. With India's growing digital orientation, the country is also concerned about cyber security breaches by unauthorized users [9]. Social engineering attacks are the second most common type of cyber-attack and are often carried out via email, websites, downloads, phishing and identity theft.

Available research presents numerous threats that need to be addressed as soon as possible. It is generally accepted that cloud computing platforms require more security controls. Therefore, significant progress must be made in security systems to achieve a high level of security [10]. After some research, we found that security is a major concern in the cloud era, as new security issues emerge every day. Most existing research only examines threats to address security issues, although vulnerability plays an important role in addressing security issues.

LITERATURE REVIEW

Grobauer et al. (2010) [11] emphasize that while certain vulnerabilities are well-understood, their significance is amplified in cloud environments. The multi-tenant nature of cloud services means that vulnerabilities can impact multiple users simultaneously, leading to extensive data breaches and service disruptions. Additionally, the transition to cloud computing has introduced new vulnerabilities that were not present in traditional IT infrastructures.

Yan et al. (2015) [12] further elucidates the security challenges posed by Software-Defined Networking (SDN) in cloud computing, highlighting the potential for Distributed Denial of Service (DDoS) attacks. Such vulnerabilities can compromise service availability, an essential aspect of cloud computing, and underscore the need for robust security measures. The authors also point to the risks associated with malicious insiders, who can exploit their access within a single cloud environment, leading to severe data loss or corruption.

Fernandes et al. (2014) [13] discuss hypervisor vulnerabilities, which are particularly concerning as they expose systems to rogue guest virtual machines (VMs) and remote attackers. The hypervisor serves as the critical layer managing VMs; any vulnerabilities here can lead to significant breaches, including unauthorized access to sensitive data.

The architecture of cloud computing itself presents security vulnerabilities that can be exploited by hackers, as noted by Alzain et al. (2012) [14]. This exploitation can occur in both single- and multi-cloud environments, emphasizing the necessity of a multi-layered security approach to mitigate such risks.

Tabrizchi and Rafsanjani (2020) [15] highlight those issues related to data stored in cloud environments, such as untrustworthy management of authentication and authorization, are prevalent. These vulnerabilities can lead to unauthorized access and data breaches, reinforcing the need for enhanced identity management protocols.

The vulnerability of cloud computing systems to advanced persistent threats (APTs) is another significant concern discussed by Perez-Botero et al. (2013) [16]. APTs are sophisticated, targeted attacks that can remain undetected for extended periods. The ability of attackers to persistently exploit weak points in cloud systems necessitates the development of advanced detection and response strategies to thwart such attacks.

Cloud Construction

The deployment architecture and service delivery architecture include cloud computing standards. Deployment models: Private, public, hybrid, and community cloud deployment methods are the most common. This deployment strategy can cause various cloud security issues [17].

- *Private cloud:* This is an extension of cloud computing for exclusive use by a business or organization. This cloud can be attached to any organization or organization, group of individuals or group of individuals. This cloud is off limits to the public. Make sure that users using the private cloud are completely isolated from each other. A private cloud is owned and managed by one entity whose services are provided over a private network. Private organizations purchase hardware and software that can be stored inside or outside the organization's facilities and managed by the organization or a third party [18].
- *Public cloud:* This is an open environment. The service is available over the internet and is managed by a public cloud service provider. For example, services aimed at the masses, such as online photo storage, e-mail and social networks. In addition, the service may be provided through a public cloud. It gives you access to a shared computing environment over the internet and makes better use of resources because they are shared [19].
- *Hybrid cloud:* Hybrid Cloud Integration helps every user get access to the hybrid cloud. It combines private and public cloud resources. They pool their resources and provide customer

service. A hybrid cloud consists of multiple service providers and systems that work together to manage and protect data [20].

- *Community cloud:* It refers to a distributed system created by combining multiple cloud services to meet the unique needs of an industry, community, or business sector. In a community cloud, infrastructure is shared between groups with similar interests or responsibilities. This cloud can be managed by a company or a third party [21].

Types of Services

Based on the services provided by the cloud, the cloud is divided into three types of services. This is a summary of each type of service.

Software-as-a-Service (SaaS)

This is an example of software distribution where vendors or service providers host customers via a network or the internet [22, 23]. As the underlying technologies that enable web services and mature enterprise services (SOA) and new development methods, such as Ajax, emerge, SaaS is becoming increasingly popular. SaaS is like ASP (application service provider) and on-demand software delivery methods. IDC defines two types of SaaS delivery. In the software as a service model, the provider gives the customer access to a network of single applications designed exclusively for SaaS.

Advantages of the SaaS Model

- Simple management
- Automatic update and patch management
- All users have the same understanding of the newsletter
- Easy collaboration
- Global access

Platform as a Service (PaaS)

PaaS is a method of renting hardware, operating systems, storage and network bandwidth over the internet [23, 24]. The instance deployment service allows the instance to rent enterprise-class hosting to connect to the system and run existing applications, or to build and test new applications. SaaS is a branch of PaaS. It represents a simpler distributed model where an operating system application is sent to its peers on the internet [25].

Advantages of PaaS:

- Through PaaS, shared computing functions can be updated and replaced.
- Services are available from many sources, including international divisions.
- Startup and payment costs can be reduced by using infrastructure provided by a single procurement team, rather than maintaining multiple equipment installations that often overlap or are on hold due to incompatible issues.
- In general, costs can also be reduced by combining breeding activities.

Infrastructure as a Service (IaaS)

The customer gets access to the workload, storage, web and various applications they want to use, as well as the software they want to use in the cloud [22]. Cloud provides hosting devices such as router, storage, and system administrators managed by peer transfer agents instead of consumers [23]. The equipment that supports the project, including the warehouse, equipment, waiting staff and network equipment, the service project must be the owner of the equipment and is responsible for protection, cutting and maintenance. Generally, the buyer pays the workers.

IaaS has the following features and products:

- Benefits and reporting model.
- Task automation.

- Dynamic scaling.
- Thin client workstation.

Security Aspects

The most important aspect to consider when using cloud computing is security. Users will store a lot of confidential and secure information on their computers. When using cloud computing, this information is sent from their devices to the cloud. Therefore, the cloud needs to take security measures to protect sensitive data. Confidentiality, accessibility, and privacy are security issues in cloud [26].

The following are security-related issues:

Privacy Protection

Threats to user information include internal threats, external threats and information leaks. First, internal threats to user data are caused by cloud service providers' illegal or unfair access to user data. This is a serious security problem. This threat may come from malicious users of cloud service providers, malicious users of cloud service providers, or third parties who could help malicious or unwelcome users of cloud service providers [27]. Second, the external attack threat applies to public cloud services; these threats include remote software or hardware attacks on cloud applications and cloud users, as well as the management of relationships between cloud service providers and users to obtain personal data and sensitive personal data. Third, data leakage is a risk, and cloud computing can cause data risk due to human error, hardware damage, inaccessibility to security, etc. [28].

Integrity Threats

It includes internal and external threats to user data and information flows. First, internal risks to user data arise from illegal or inappropriate cloud services that provide employees with access to customer data. This is an important security issue. This threat may come from malicious users of cloud service providers, malicious users of cloud service clients, or hostile third parties supporting malicious cloud service providers or cloud service clients [29]. Second, the power of foreign attacks affecting public cloud services. This risk includes remote software or hardware attacks on cloud applications and cloud users, as well as social pressure on cloud service providers and users to access private and sensitive data. Third, messages are likely to leave the cloud due to human error, technical failure, or secure access failure [27].

Availability Risks

Includes the impact of change management, lack of service availability, physical disruption of resources and ineffective recovery processes. The first is the result of change management, including the results of user testing for other users and the results of changes to the infrastructure. Changes in hardware and software within the cloud system can disrupt the availability of cloud services [24]. The second is service unavailability, including network bandwidth, DNS services, and computer usage and resource unavailability. This is an external risk that affects all cloud types. The third is the physical disruption of IT services for service providers, cloud clients and WAN service providers. In highly secure environments or remote systems, devices can be easily compromised by insiders or external attackers. The fourth is the lack of a good disaster recovery plan, which affects the time needed to return to normal and work [27, 28].

Vulnerabilities and Problems

Vulnerabilities and problems address the security weaknesses and challenges [30] that can expose systems to risks and potential failures as shown in Table 1.

Counter Measures of Security Vulnerabilities

Cryptography

Cryptography is the process of converting unreadable data into a readable bubble, after which the data can be easily understood and retrieved by the client. This process is important to protect the privacy

of user data. “Crypto” means “encryption” and “Graphy” means “writing”. Encryption or cryptography provides both data security and user authentication. The information provided by the sender to the receiver is in a human-readable form, called “plain text”. However, when the data is converted into a cryptographic bubble by cryptography, the subject of the data becomes a bubble-text password [31]. Encryption converts plaintext to ciphertext, and encryption converts plaintext to plaintext. Cryptography includes encryption algorithms and asymmetric encryption algorithms. Symmetric and asymmetric security systems protect our data. Both have unique encryption methods. In both symmetric and asymmetric encryption, both the sender and receiver have their own encryption keys. Cryptography is used not only for security but also for user identification.

Table 1. Problems of vulnerability remediation.

Vulnerabilities	**Problems**
Data Losses and Breaches	● Faith concern along with the cloud supplier. ● In experiment strategy, quality, and lacking information safeguard techniques. ● Lack of understanding.
Insecure Interfaces and APIs	● Inability to evaluate circumstances are linked with APIs operated. ● Complications of the APIs.
Malicious Insiders	● Suppliers are concealing their company’s standards through the workers. ● Delay of the mixture to expand the experiences happens. ● Insufficiency of the cloud supplier to detect the workers.
Account, Service, and Traffic Hijacking	● The speedy development of cloud computing unlocks the latest crack. ● The latest techniques of automated recognition administration are not sufficient since compound clouds.
Shared-Technology Vulnerabilities	● Progress divided into pieces is not undertaken. ● Manipulations with telecommunications. ● Survey is connecting the assembly to undertaking and assignment which is divided into sections.
Misuse of Cloud Services	● Cloud contributors have a narrow capacity to observe because of their isolated constitution. ● Shareholders are diverse in their curiosity.

Authentication and Authorization

There are four steps to access control: authentication, authentication, authorization, and assignment. Users are identified when security systems are used and supported. To protect against criminals, some security systems generate random identification numbers

Authorization Systems Are Managed in Three Ways

Authorization for authorized users, authorization for team members, authorization across different systems, and requests that are systems that record processes. System logs record successful and failed login attempts.

Virtual Private Networks (VPNs) and Firewalls

Additionally, VPNs and firewalls are closely related when it comes to protecting cloud platforms. A VPN helps users create secure tunnels to access cloud services and protect data from malicious networks. Firewalls set policies with multiple filtering criteria for network traffic. If the packet has only passed the filtering rules, it is allowed to pass through the cloud network, otherwise it is prohibited; VPS with IP is a strong system for security [32]. A firewall is critical to network security because it inspects every incoming packet and sits between the internal network and the outside world. A combination of firewall and VPN allows access to the correct server. Antivirus (AV) is the last important protection for end users.

Anticipated Actions and Close Monitoring

Other key recommendations for attacks like Ransomware include preventative measures and being aware of access opportunities. All strategies to ensure system security must go through four steps: predict, limit, detect, and verify.

Homomorphic Encryption

The use of homomorphic algorithms in cloud data transmission may introduce security and privacy issues during encryption. Homomorphic encryption is a new technology that can program arbitrary computations such as addition or multiplication in ciphertext without encryption. On the other hand, extensive processing requirements can lead to additional costs such as increased reaction time and energy consumption.

Hash Function

Security is a very important issue in the cloud. There are many encryption methods available to help users protect their cloud data. Data hash functions also ensure data security and data privacy. Hash functions are currently attracting the attention and interest of the scientific community. Hash functions and encryption paths are also related. It consists of all encryption and security systems used to provide authentication services. A hash function is a function that transforms an input into an output of a specified length. Hash functions are used to improve performance and reduce bandwidth. Any small change in the data is better than a big change in the hash code. By using the hash function, we can verify that the received data is valid and has not been modified or tampered with by an attacker. Hash functions are different from encryption; There are many types of hashing algorithms such as SHA, MD5, digital images, etc. We can continue to explore double hashing strategies. When we combine the most secure hash algorithm for network security with the most secure hash algorithm for data security, users can send their data to the cloud as shown in Table 2.

Table 2. Threats and counter steps in cloud computing.

Threats	**Events**	**Counter Step**
Stealing Services or Accounts	When an attacker obtains the customer's information with a quick distribution like a citizen who collected simple credentials at that time, they can use this method because they publish a malicious project to do it in 'by releasing confidential information, reducing information, including the wrong dates for some contracts.	Specification including approach direction information energetic qualifications.
Information search	Every time a part of the machine malfunctions to deliver important information, every time it is announced as an information search if the boxer does not return the information that started it then information is lifeless	System strength acceptance needs to exist modernization in the company of dismantling the plan of action.
Data Leakage	Some services are associated with this type of data. Configuration, transmission and security can lead to data leakage to hackers or attackers.	Digital Signatures Encryption, Homomorphic encryption
Denial of Service	Clients who misbehave by intentionally stuffing their devices with brackets, don't understand what is required, and are separate from what the client thinks is impenetrable, is a big deal.	Restricted counting materials have to put forward
Clients Information Drafts	SQL Enhancer, Tutorial Enhancer, Untrusted correct examples and mixed tables are encountered in the main method, while improving service access information to serve threats.	Network approach scanning

CONCLUSION

Security is an important part of cloud computing. The cloud is surrounded by a variety of vulnerabilities, threats and attacks that can have a minor or sometimes severe impact on the cloud. Of course, any answer is possible. Attackers can choose to compromise cloud systems through various vulnerabilities. Hence, it is essential to thoroughly evaluate all aspects of security. Criminals modify and manipulate data when customers upload their data to cloud systems. Due to some special reasons, attackers may try to introduce malicious services into the cloud system, which may damage the data of other customers or even the cloud system itself. In this way, attackers can try to compromise or disable cloud services. The main customer is blocked from the service requested in the cloud system, and the owner cannot pay additional fees to the cloud service provider for other requests because of the attack.

REFERENCES

1. Ma X. Security concerns in cloud computing. In2012 Fourth International Conference on Computational and Information Sciences 2012 Aug 17 (pp. 1069–1072). IEEE.
2. Bharti J, Singh S. A Review on Security Vulnerabilities in Cloud Computing. In: International Conference on Data, Engineering and Applications; 2022 Dec 23; pp. 229–47. Singapore: Springer Nature.
3. Grover J, Sharma M. Cloud computing and its security issues-A review. In: 2012 Fourth International Conference on Computational and Information Sciences; 2012 Aug 17; pp. 1069–72. IEEE.
4. Cafaro M, Aloisio G. Grids, clouds, and virtualization. London: Springer; 2011.
5. Rittinghouse JW, Ransome JF. Cloud computing: implementation, management, and security. CRC press; 2017 Mar 27.
6. Bernsmed K, Jaatun MG, Meland PH, Undheim A. Thunder in the clouds: Security challenges and solutions for federated clouds. In: 4th IEEE International Conference on Cloud Computing Technology and Science; 2012 Dec;p.113–20. IEEE.
7. Dar AR, Ravindran D. A comprehensive study on cloud computing paradigm. Int J Adv Res Sci Eng. 2018;7(4):235–42.
8. Singh N, Jangra A. Challenges and prosperity research in cloud computing. Int J Comput Trends Technol. 2017;49(4):200–5.
9. Saad M, Khormali A, Mohaisen A. End-to-end analysis of in-browser cryptojacking. arXiv preprint arXiv:1809.02152. 2018 Sep.
10. Chou TS. Security threats on cloud computing vulnerabilities. Int J Comput Sci Inf Technol. 2013 Jun 1;5(3):79.
11. Grobauer B, Walloschek T, Stocker E. Understanding cloud computing vulnerabilities. IEEE Secur priv. 2010 Jun 17;9(2):50–7.
12. Yan Q, Yu FR, Gong Q, Li J. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE Commun Surv Tutor. 2015 Oct 5;18(1):602–22.
13. Fernandes DA, Soares LF, Gomes JV, Freire MM, Inácio PR. Security issues in cloud environments: a survey. Int J Inf Secur.. 2014 Apr;13:113–70.
14. AlZain MA, Pardede E, Soh B, Thom JA. Cloud computing security: From single to multi-clouds. In: 2012 45th Hawaii International Conference on System Sciences; 2012 Jan 4; pp. 5490–5499. IEEE.
15. Tabrizchi H, Kuchaki Rafsanjani M. A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput. 2020 Dec;76(12):9493–532.
16. Perez-Botero D, Szefer J, Lee RB. Characterizing hypervisor vulnerabilities in cloud computing servers. In: Proceedings of the 2013 International Workshop on Security in Cloud Computing; 2013 May 8; pp. 3–10.
17. Alhaidary M, Rahman SM, Zakariah M, Hossain MS, Alamri A, Haque MS, Gupta BB. Vulnerability analysis for the authentication protocols in trusted computing platforms and a proposed enhancement of the offpad protocol. IEEE Access. 2018 Jan;6:6071–81.
18. Yesilyurt M, Yalman Y. New approach for ensuring cloud computing security: using data hiding methods. Sādhanā. 2016 Nov;41(11):1289–98.
19. Khalil IM, Khreishah A, Azeem M. Cloud computing security: A survey. Comput. 2014 Feb ;3(1):1–35.
20. Potey MM, Dhote CA, Sharma DH. Cloud computing-understanding risk, threats, vulnerability and controls: a survey. Int J Comput Appl. 2013 Jan 1;67(3).
21. Barakat OL, Hashim SJ, Raja Abdullah RS, Ramli AR, Hashim F, Samsudin K, Ab Rahman M. Malware analysis performance enhancement using cloud computing J Comput Virol Hacking Tech. 2014 Feb;10:1–10.
22. Takabi H, Joshi JB, Ahn GJ. Security and privacy challenges in cloud computing environments. IEEE Secur Priv. 2010 Dec;8(6):24–31.

23. Chakraborty R, Ramireddy S, Raghu TS, Rao HR. The information assurance practices of cloud computing vendors. IT Prof. 2010 Mar;12(4):29–37.
24. Musa FA, Sani SM. Security threats and countermeasures in cloud computing. Int Res J Electron Comput Eng. 2016 Dec 15;2(4):22–7.
25. Singh S, Jeong YS, Park JH. A survey on cloud computing security: Issues, threats, and solutions. J Netw Comput Appl. 2016 Nov 1;75:200–22.
26. Catteddu D. Cloud Computing: benefits, risks and recommendations for information security. Web Application Security: Iberic Web Application Security Conference, IBWAS 2009, Madrid, Spain, December 10–11, 2009. Berlin: Springer; 2010.p17.
27. Sen J. Security and privacy issues in cloud computing. In: Architectures and protocols for secure information technology infrastructures; 2014. p. 1–45. IGI Global. Available from: https://www.igi-global.com/gateway/chapter/78864.
28. Krishnan R. Security and Privacy in Cloud Computing. 2017. Available from: https://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=1932&context=masters_theses
29. Jamil D, Zaki H. Security issues in cloud computing and countermeasures. Int J Eng Sci Technol. 2011 Apr;3(4):2672–6.
30. Zhang Q, Cheng L, Boutaba R. Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl. 2010 May;1:7–18.
31. Ashraf M, Kamel F. Vendor lock-in in the transition to a cloud computing platform. Degree project in Communication Systems, Second Level; Stockholm, Sweden; 2015. p.1–42.
32. Paquette S, Jaeger PT, Wilson SC. Identifying the security risks associated with governmental use of cloud computing. Gov Inf Q. 2010 Jul;27(3):245–53.

