بسم الله الرحمن الرحيم
Omdurman Islamic University Journal(OIUJ)
مجلة جامعة أم درمان الاسلامية
https://journal.oiu.edu.sd/index.php/oiuj
https://doi.org/10.52981/oiuj
2024; 20(2):25-33
ISSN: 5361-1858

Review of Security Concerns and Solutions with Cloud Computing Deployment and Delivery Models

Khalid Mohammed Osman Saeed*[1] , Anwer Mustfa Mohammed Salih Hilal[2] , Manar Ahmed Mohammed Hamza[3] , Mohammed Mohammed Osman Mokhtar [4]

[1] *Faculty of Computer Science and Information Technology Omdurman Islamic University Sudan*
[2] *Faculty of Computer Science and Information Technology Omdurman Islamic University Sudan*
[3] *Faculty of Computer Science and Information Technology Omdurman Islamic University Sudan*
[4] *Faculty of Computer Science and Information Technology Omdurman Islamic University Sudan*

Corresponding Email address: khalidmohosman@gmail.com

To cite this article:

Review of Security Concerns and Solutions with Cloud Computing Deployment and Delivery Models , Khalid Mohammed Osman Saeed*[1] , Anwer Mustfa Mohammed Salih Hilal[2] , Manar Ahmed Mohammed Hamza[3] , Mohammed Mohammed Osman Mokhtar [4] Omdurman Islamic University Journal-Sudan

ISSN: 5361-1858

https://doi.org/10.52981/oiuj.v1i2.1726

Abstract

This paper focuses on the analysis of the security challenges faced by organizations when adopting cloud computing, as well as the potential solutions that can be employed across different cloud deployment models (public, private, hybrid) and delivery models (IaaS, PaaS, SaaS). The review examines common threats, such as data breaches, loss of control, and service disruptions, and explores various security measures, including encryption, multi-factor authentication, access control mechanisms, and compliance frameworks. Additionally, it highlights emerging trends and technologies, such as AI and block chain, that could enhance security in cloud environments.

The goal is to provide a comprehensive overview of how security can be effectively managed and mitigated to ensure the safe use of cloud services.

Keywords— Clouds; Cloud Computing Security; Security Issues; Security Solutions

1. Introduction

The increasing adoption of cloud computing has brought numerous benefits such as scalability and cost-efficiency, but it has also introduced significant security concerns. This review explores the security challenges associated with various cloud deployment models (public, private, hybrid) and delivery models (SaaS, PaaS, IaaS). It examines issues such as data privacy, compliance, and unauthorized access, and reviews current solutions aimed at mitigating these risks, including encryption, identity management, and advanced monitoring techniques [1].

The paper aims to provide insights into securing cloud environments while balancing flexibility and risk management. Additionally, cloud computing gives people and business access to shared tools and services like online storage through the internet. Because of this, cloud computing data centers are essential as the main suppliers of cloud computing infrastructure, including Google Cloud, Oracle Infrastructure Cloud, and others [2].

Data owners upload data to the data centers to save and may utilize later in order to benefit from cloud computing and storage capabilities provided by cloud computing infrastructure providers. On the other hand, data owners do not fully trust these online storage services. Additionally, data and services are virtually always created to be shared across dependable partners, whether they are people or businesses. Therefore, the confidentiality of data must be protected by cloud computing providers. However, before outsourcing to the cloud and vice versa, these critical data and apps must be kept and used in an encrypted manner. In addition, as was already mentioned, a lot of commercial and governmental organizations are moving their operations to the cloud, so cloud computing security is always being scrutinized. Louis Columbus [3] claims that 80% of all IT costs were spent on internet solutions, but on the other hand, 49% of tasks obstruct cloud operations due to security worries, and 73% of businesses are getting ready to switch to fully software by defined data centers. This paper briefly examines cloud computing security challenges due to the ongoing attacks on cloud computing providers and customers' privacy.

1. Introduction

The increasing adoption of cloud computing has brought numerous benefits such as scalability and cost-efficiency, but it has also introduced significant security concerns. This review explores the security challenges associated with various cloud deployment models (public, private, hybrid) and delivery models (SaaS, PaaS, IaaS). It examines issues such as data privacy, compliance, and unauthorized access, and reviews current solutions aimed at mitigating these risks, including encryption, identity management, and advanced monitoring techniques [1].

The paper aims to provide insights into securing cloud environments while balancing flexibility and risk management. Additionally, cloud computing gives people and business access to shared tools and services like online storage through the internet. Because of this, cloud computing data centers are essential as the main suppliers of cloud computing infrastructure, including Google Cloud, Oracle Infrastructure Cloud, and others [2].

Data owners upload data to the data centers to save and may utilize later in order to benefit from cloud computing and storage capabilities provided by cloud computing infrastructure providers. On the other hand, data owners do not fully trust these online storage services. Additionally, data and services are virtually always created to be shared across dependable partners, whether they are people or businesses. Therefore, the confidentiality of data must be protected by cloud computing providers. However, before outsourcing to the cloud and vice versa, these critical data and apps must be kept and used in an encrypted manner. In addition, as was already mentioned, a lot of commercial and governmental organizations are moving their operations to the cloud, so cloud computing security is always being scrutinized. Louis Columbus [3] claims that 80% of all IT costs were spent on internet solutions, but on the other hand, 49% of tasks obstruct cloud operations due to security worries, and 73% of businesses are getting ready to switch to fully software by defined data centers. This paper briefly examines cloud computing security challenges due to the ongoing attacks on cloud computing providers and customers' privacy.

2. Cloud Computing Architecture

Understanding the cloud computing terminology and architecture is crucial before the researchers' digs into cloud computing security challenges. Dr. Akila Ganesh and D. Jothipriya claim that cloud computing is a collection of resources that are provided on demand [4]. That is, it is a new way to deliver services which is provided by cloud computing and with the aid of these new technological possibilities, business is conducted.

Cloud computing, according to Rajani Sharma and Rajender Kumar Trivedi [5], is a collection of resources that may be scaled up or down as needed. These resources are available via the cloud with only a minimal amount of contact between data owners and the cloud service providers needed. Cloud computing enables data owners in a variety of ways by providing them with the data in many formats, the technology in various forms, and the service options they require at competitive pricing. Cloud computing is described as "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" by Alan Sill, Annie Sokol, and others [6].

From a researchers' vantage point, it is increasingly evident that cloud computing is a sophisticated technological solution with several possible security flaws [7].

2.Cloud Computing Benefits

A variety of advantages of cloud computing, according to Abhijit Dubey, Dilip Wagle [8], and Maricela-Georgiana Avram [9], include, the amount of resources used by both the smallest and largest companies is greatly reduced. Additionally, it offers a significant opportunity for emerging nations or resource-constrained nations to catch up with the information technology revolution.

As well, it is able to provide immediate access to hardware resources that can be shared and segregated from one another by a variety of users. However, the flexibility of the cloud enables operations to manage workloads, ensuring equitable resource distribution.

Without a doubt, whenever needs occur, computing resources are managed and controlled by software programs like operating systems. This indicates that based on current activities, the services offered may be scaled.

According to Sean Marston et al. [10], cloud computing also makes it possible to develop new kinds of apps and offers features like scaling and parallel processing that enable large enterprises to handle their big data with the utmost efficiency.

3. **Deployment and Delivery Models Security Issues**

In cloud computing, there are three different deployment models: private, public, and hybrid. There are also three different delivery models: infrastructure as a service (IaaS), platform as a service

(PaaS), and software as a service (SaaS). The following two sections will briefly discuss each of these models and the security concerns they raise from the perspective of researchers.

4.1 Cloud Deployment Models Security Issues

4.1.1 Private cloud model

In this strategy, internet-based subscription services are used to allocate resources to a certain company or consumer. Although scalable resources and virtual applications are available via the internet and are housed in cloud providers' data centers on demand, this poses a number of security concerns, including risk assessment, high implementation and management costs, the need for customers to have specialized skills, and vulnerability management.

4.1.2. Public cloud model

In this arrangement, online resources that are assigned to the general public run on distant servers. These materials could be accessible for free or through a subscription basis like pay per use. However, a public cloud might include virtual machines, storage options, and apps with scalability and sharing features.

According to the researcher [11], a large number of cloud users and the volume of transactions they generate force many cloud service providers to adhere to a shared responsibility model. In other words, while the cloud provider looks after the security of the entire cloud, the customer is responsible for looking after the security of his own data that will be transferred to the cloud. In other words, users and public cloud providers must consider inadequate infrastructure changes, data breaches, incorrect configuration, spoofing identities, and access management.

4.1.3. Hybrid cloud model

It is a technology that describes a variety of computing, storage, and service environments like Amazon Web Services (AWS) or Microsoft Azure. Typically, it combines a private cloud with one or more public cloud services from other companies, enabling the sharing of data and applications between them. It is a potent method since it gives organizations control over their own private information.

Hybrid cloud models are not an exception to the rule that every technology has its own security hazards, but in these semi-dynamic or frequently changing workloads and heterogeneous environments, security might be specifically constructed for vulnerabilities, threats, and risks that

are appraised. This necessitates additional administrative attention, which raises the expense of the security measures.

4.2. Cloud Delivery Models Security Issues

As previously indicated, the National Institute of Standards and Technology offered three cloud delivery models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These models have been adopted by the technology community and industry. Despite this, they nevertheless have security concerns.

4.2.1. Software as a Service (SaaS)

This delivery architecture offers the opportunity to employ one or more cloud-based servers and their running applications. These programs are accessible through a variety of device interfaces, including web browsers. The underlying cloud infrastructure does not need to be maintained, managed, or controlled by the service's user. [12]

Consumers are still in charge of protecting their own devices, but software as a service companies are required to keep the servers hosting their services and applications secure.

4.2.2. Platform as a Service (PaaS)

According to John Rittinghouse and James Ransome [13], platforms act as service providers by giving customers access to tools like supported applications that they have created or purchased. The hosting environment and applications that are used by customers of this service are under their control, but not the cloud infrastructure [14], which includes the network, storage, servers, operating systems, etc.

Because platforms as service providers assist customers with such essential resources as networks, storage, servers, and operating systems, the platform as service provider is frequently held responsible for security. And lastly, providers are more at risk than customers.

4.2.3. Infrastructure as a Service (IaaS)

In contrast to the two cloud delivery models mentioned above, this one gives users minimal control over a number of networking elements, processes, and storage options, as well as operating systems and apps. [12]

However, in this case and according to the researchers', the consumer and the infrastructure acting as a service provider share equally in the obligation for security.

5. Countermeasures & Controls

Because cloud computing security risks and vulnerabilities are so widely discussed, they are thoroughly documented. Based on their assessments, each cloud service provider and cloud user must devise countermeasures and security procedures to reduce and eliminate the dangers they encountered. The best practices for controls and countermeasures, however, include some of the following.

5.1. Encryption

It is crucial and essential that the data in a cloud be encrypted because it may go via many different networks, servers, and geographical locations.

5.2. Malicious Code Checking

It is important for cloud service providers to have adequate security controls and countermeasures to reduce risks from malicious software traveling with the encrypted data because encrypted data cannot be read by intrusion detection systems and firewalls.

5.3. Personality Validation

To stop threats like session hijacking and intrusions, cloud service providers must take enough security precautions to monitor cloud users' behavior and activities.

5.4. Continuity Plans

Denial of service attacks occasionally occur, preventing authorized cloud users from using the services they are authorized to utilize. As a result, cloud service providers need a continuity strategy. This guarantees that cloud users and their belongings are safe and can operate promptly in the event of a security compromise.

6. Conclusion

The newest technology that has become widely used recently is cloud computing. Although the cloud has several drawbacks such as large file storage, complex architecture, and a wide range of applications, many businesses are adopting and using it despite the fact that there is a constant security risk of data breaches.

Understanding how to reduce security sabotage is important. However, in order to effectively combat security issues, security needs to be built into the cloud computing infrastructure at every level by using best practices and cutting-edge technologies.

The security industry is aware that security engineering offers the best methods and techniques for creating systems and services that are made specifically for security, according to recent papers on cloud security challenges. Additionally, businesses looking for an economic competitive edge might benefit greatly from cloud service providers.

Sensitive data can be lost or discovered by using an attack like SQL injection, which is the main concern about systems where data is shared and exchanged. As a result, each organization needs to have solid security measures in place to safeguard its data, infrastructure, services, and even its employees.

[1] Dinesh Kumar Saini, Krishan Kumar, Punit Gupta, Security Issues in IoT and Cloud Computing Service Models with Suggested Solutions, Security and Communication Networks (Wiley), April 2022.

[2] Flexera, State of Cloud Report, https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020, (visited on 1/October 2020).

[3] Louis Columbus, State of Cloud Adoption and Security, https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/#d0c3ae818483, (visited on 25/May 2020).

[4] D. Jothipriya, Dr. Akila Ganesh, Literature Review: Cloud Computing–Security Issues, Technologies and Challenges, Engineering and Scientific International Journal, Volume 3, Issue 2, 2016.

[5] Rajani Sharma and Rajender Kumar Trivedi, Literature review: Cloud Computing-Security Issues, Solution and Technologies, International Journal of Engineering Research, Volume 3, Issue 4, p. 221-225, 2014.

[6] Alan Sill, Annie Sokol, (et al.), NIST editors Michael Hogan and Annie Sokol, NIST Cloud Computing Standards Roadmap, National Institute of Standards and Technology, NIST Special Publication 500-291, Version 2, 2013.

7] Akhil Kumar, Akhil Kumar Reddy Vesireddy, Sharan Manohar Shetty, Cloud computing security issues in delivery service models and solutions, Security and Communication Networks (Wiley), December 2023.

[8] Abhijit Dubey. Dilip Wagle, Delivering software as a service, The McKinsey Quarterly, p. 1–12, 2007.

[9] Maricela-Georgiana Avram, Advantages and challenges of adopting cloud computing from an enterprise perspective, ScienceDirect, Volume l2, p. 529-534, 2014.

[10] Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, Anand Ghalsasi, Cloud computing The business perspective, Elsevier, 2010.

[11] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan, A survey on security issues and solutions at different layers of Cloud computing, The Journal of Supercomputing, Volume 63, Issue 2, p. 56l-592, 2012.

[12] Peter Mell, Tim Grance, The NIST definition of cloud computing, National Institute of Standards and Technology, NIST Special Publication 800-145, 2011.

[13] John Rittinghouse, James Ransome, Cloud Computing: Implementation Management and Security, CRC Press, 1st Edition, 2009.

[14] Vaikunta Pai T., P. S. Aithal, A Review on Security Issues and Challenges in Cloud Computing Model of Resource Management, International Journal of Engineering Research and Modern Education (IJERME), Volume 2, Issue 1, p. 65-70, 2017.