Scientific Research Publishing

Journal of Software Engineering and Applications, 2024, 17, 763-769
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

Cloud Computing: Purpose and Future

Robb Shawe

Department of Cyber Leadership, Capitol Technology University, Laurel, MD, USA
Email: rshawe@captechu.edu

How to cite this paper: Shawe, R. (2024) Cloud Computing: Purpose and Future. *Journal of Software Engineering and Applications*, **17**, 763-769.
https://doi.org/10.4236/jsea.2024.1710041

Received: September 15, 2024
Accepted: October 13, 2024
Published: October 16, 2024

Copyright © 2024 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution-NonCommercial International License (CC BY-NC 4.0).
http://creativecommons.org/licenses/by-nc/4.0/

Open Access

Abstract

Cloud computing is the new norm within business entities as businesses try to keep up with technological advancements and user needs. The concept is defined as a computing environment allowing for remote outsourcing of storage and computing resources. A hybrid cloud environment is an excellent example of cloud computing. Specifically, the hybrid system provides organizations with increased scalability and control over their data and support for a remote workforce. However, hybrid cloud systems are expensive as organizations operate different infrastructures while introducing complexity to the organization's activities. Data security is critical among the most vital concerns that have resulted from the use of cloud computing, thus, affecting the rate of user adoption and acceptance. This article, borrowing from the hybrid cloud computing system, recommends combining traditional and modern data security systems. Traditional data security systems have proven effective in their respective roles, with the main challenge arising from their recognition of context and connectivity. Therefore, integrating traditional and modern designs is recommended to enhance effectiveness, context, connectivity, and efficiency.

Keywords

Cloud Computing, Hybrid Cloud, Private Cloud, Public Cloud, IaaS, PaaS, SaaS, On-Premises, Platform, Data Security Systems

1. Introduction

Cloud computing, a term that describes the operation and hosting of computer programs over the internet, is a crucial enabler of on-demand services at a minimal cost [1]. The historical development of cloud computing has been a transformative force in technology. It has redefined how data is stored, processed, and accessed, ushering in a new era of efficiency and flexibility for individuals and businesses. From its early conceptualization to the present day, cloud computing has reshaped the landscape of IT infrastructure and continues to drive the future

of digital innovation. The scalability, cost-effectiveness, and accessibility of cloud services have made them an indispensable tool in the modern era, fueling progress in various industries and unlocking new possibilities for collaboration and growth.

Before discussing issues on data security, the article introduces the concept of cloud computing, followed by an analysis of the applicability of an integrated cloud computing approach—hybrid computing. Hybrid computing is chosen due to its combination of public and private cloud environments, which helps to provide a holistic view of cloud computing as a system. The pros and cons of the hybrid computing system are highlighted, thus introducing the issue of data security. Finally, a literature review and procedural tests compare traditional and modern data security systems, which inform the article's discussion and recommendations.

2. Overview of Cloud Computing

Cloud computing is dependent on three critical layers—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [2]. Infrastructure as a Service—This component provides the physical resources, bandwidth, networks, and storage. Platform as a Service—This layer provides end-users with access to the media and operating systems required to establish and develop applications and includes venues such as databases.

Software as a Service—The SaaS layer provides access to software applications. There are three common types of cloud deployment: public, private, and hybrid. Public cloud computing refers to a computing environment that provides infrastructure and services accessible and shared by all customers through an Internet platform. Private cloud computing is a computing system hosted on an organization's premises and utilized only by one organization. Finally, a hybrid cloud environment refers to a computing system that combines private clouds with public clouds. Hybrid clouds are chosen for analysis and discussion in this article to integrate the core types.

2.1. Hybrid Cloud Computing

A hybrid cloud combines the use of private and public cloud infrastructure. This option is often used by organizations seeking to leverage public clouds to add to the available capacity within private clouds. Unlike private clouds operated on-premises and traditional public clouds used off-premises, a hybrid cloud combines both to allow an organization to run its workload physically and virtually. Hybrid cloud computing enables organizations to host critical and sensitive workloads on the private cloud. In contrast, the less critical resources are hosted through a third-party, public cloud service provider [3].

Support for a remote workforce is considered one of the main benefits of a hybrid cloud [4]. Hybrid clouds support desktop virtualization, allowing organizations to support distributed and remote employees with access to data that is not restricted to one location. Such action implies that organizations running on the

hybrid cloud platform can move their sensitive data to on-premises servers that ensure increased privacy while leaving other services and applications available on the public cloud for easy access by all authorized personnel.

A hybrid cloud is a cost-effective way for an organization to scale its operations to meet growth demands. The option to house critical data on private servers while deploying less sensitive data to public clouds provides cost benefits as the organization only pays for the cloud resources required for its operations [5]. Therefore, growth in business or demand can be separate from an infrastructure expansion. Instead, the organization can pay for the additional resources required and drop this once the market reduces.

A hybrid cloud environment provides an organization with greater scalability and data control. In addition, the cloud enables automation that allows an organization to adjust its cloud settings to respond to changes in demand automatically. As a result, this will enable organizations to scale their workloads and improve efficiency and performance.

Hybrid cloud environments foster innovation and agility. The automation from a hybrid cloud environment allows an organization to respond to market changes with speed and increased accuracy. In addition, optimizing performance and the lack of restricted access to private infrastructure make it possible to meet the ever-changing business demands and expansion requirements.

Finally, hybrid cloud environments support business continuity. In the event of disasters within the organization, hybrid cloud environments help to ensure minimal interruption or downtime, thus enabling operations to continue. In addition, hybrid systems allow for the backup of critical data as the vital data within its private servers can be replicated within the cloud network, implying that a problem within the private network will not cause significant damage that may cripple the organization's operations.

The hybrid cloud model has several advantages, some of which may not benefit other organizations and could be considered limitations. Additionally, a hybrid cloud platform requires the organization to maintain both on-cloud and on-premises infrastructure. Maintaining computing infrastructure on the premises is expensive, and the bigger the infrastructure needed, the higher the costs [6]. The hybrid cloud strategy also requires the choice of technologies and solutions to consider the organization's various environments.

Operating a hybrid cloud environment requires an organization to maintain and keep track of multiple platforms and vendors. In addition, prompt coordination and management will be necessary to ensure that the two computing environments work harmoniously for the organization's benefit.

Finally, cloud computing environments are generally sophisticated. However, combining two such environments makes the situation even more complex, making it harder to understand the organization's cloud environment. Therefore, the combination of two domains introduces the risk of missing out on critical opportunities and issues within the system that could result in trouble for the organization.

2.2. Data Security in Cloud Computing

The most critical gateway to cloud computing services is the identity authentication process. Knowledge of this has increased the susceptibility of such gates to hackers who use different techniques, including denial of service attacks, to close the gates permanently. As a result, data security has become one of the most significant barriers to adopting cloud computing by organizations [7]. The situation worsens with cloud environments that represent scattered data across different storage devices and machines.

3. Materials and Methods

A literature review of existing works on traditional and modern data security was used, along with an experimental comparison of the two approaches. The pros and cons of traditional and contemporary data security systems were collated for the literature review to determine the most cited benefits and limitations. A retailer computing system was used for the experiment, two different data security systems were hypothetically applied, and the results were compared for accuracy and efficiency.

A modern security tool was integrated with the traditional security tool to establish data security and protection changes. In this case, the integration was carried out for a small retail outlet using conventional security tools. For this specific example, an employee of the maintenance company associated with the outlet tries to log into the outlet system to authenticate sensitive payment data. The system will be working to certify sensitive payment data on one end. In contrast, on the other end, the endpoint protection tool would detect unusual malware on the computers concerning the user identity. The data loss prevention software will see that encrypted files are erroneously sent to an external account since the account is not on the company's internal network.

4. Results

The first system fails to flag down the authentication activity when the operation is conducted on the system with only traditional security systems. Instead, it is considered an incorrect login. With the correct credentials, the individual will eventually access the system. The endpoint would respond with a system cleansing to erase any malware on the computer. As a result, data loss prevention events would eventually become shortsighted, and further action would only be taken.

All security systems on the company's infrastructure are integrated when the new application is installed. However, the execution of the same operation provides different results, with the systems generating an alert for investigation. The new application connects all three occurrences due to user identification data. First, it indicates an unusual attempt to access a computer, usually associated with a single identification log. Second, this will connect with the extraordinary data loss protection activity, creating an alert visible to the system analyst. Finally, as a result, this action prompts the deactivation of the user trying to gain access and

produces an immediate investigation to determine the purpose of the attempt.

5. Discussion

The hybrid cloud strategy offers affordability, flexibility, improved access, enhanced security, and customizable solutions. However, the safety of every system is susceptible to attacks from hackers, and the situation is heightened within a hybrid system as it involves numerous infrastructures.

The data loss protection system will compare modern and traditional data security systems. The data loss prevention system refers to tools and processes tasked with defining, discovering, and monitoring an organization's sensitive data to protect and prevent it from leaving the local environment.

The traditional data loss protection system provides passive monitoring, recording all system activities. Specifically, data administrators can access the numerous logs of all network activities. The administrators are then tasked with monitoring activities, investigating unusual incidents, and troubleshooting detectable issues within the network.

The main advantage of the traditional system is its use of a firewall to restrict external access [8]. The system effectively scans the system for external attacks and prevents insider threats. Visibility is also ensured when using a traditional design to monitor the type of data shared with external parties while preventing the copying or sending of sensitive data unless there is authorization.

The main limitation of the system is that it requires manual classification and identification of data [9]. An organization using such a system has to take inventory of all data and indicate who has access to classified data. Additionally, the system requires the organization to distinguish and audit the privilege levels of individuals within the organization concerning their access to information. Finally, this system can only work if the organization has developed a comprehensive data loss protection policy, which clarifies how to integrate the system into the organization's cybersecurity system.

A modern data loss prevention system would provide active monitoring, which could be deployed to the organization's server to monitor and control all activities within its strategy and endpoints. In addition, the new cyber data loss prevention system would effectively identify all sensitive information within servers, including details concerning credit cards and credentials, thus, enhancing the ability to detect potential data breaches.

The main advantage of the modern system is machine learning algorithms that enable it to recognize any new data in sensitive systems [10]. Consequently, a modern design allows for the continuous improvement of systems, thus enhancing their capacity to identify any data that requires protection. Furthermore, the ability of the system to revamp and learn continuously is achieved through using new infrastructure that enhances its integration abilities.

Traditional security technologies are good at what they were explicitly built to accomplish but have the overall challenge of being susceptible to data breaches. Such deficiency is due to disconnected systems needing more contextual information to

protect the entire system. Instead, traditional security technologies are disconnected and operate in siloes, securing the dots between users, devices, and data. Additionally, traditional securities work without context and easily miss out on critical alerts that, when combined, indicate the need to prioritize investigations on potential threats to a system.

Integrating a new system into an old system is the solution to fixing this problem, thus, providing such systems with the interconnectivity that enables the development of context.

Therefore, this article proposes a blend of the traditional and new clouds to protect against attacks on data. Several applications have been developed to achieve visibility within an organization's cloud platforms. A data lake with time-stamped data can be created for all cloud networks—this comprises packets of data on present and previous network traffic. Combining the traditional and the new clouds would allow it to store this data for long periods. Such data lakes can identify attacks, thoroughly analyze cloud networks, and investigate potential anomalies. New and traditional application solutions enable the organization to view the entire network holistically. Consequently, this helps reduce blind spots that hackers can utilize, effectively locking them out of the network.

Cloud networks have been identified as dynamic, thus requiring continuous monitoring. Proper monitoring involves tapping data packets moving through the physical and virtual networks, combining traditional and new technologies in security monitoring. For example, conventional fixtures in a network system can intercept traffic or copy information when it leaves or enters a physical network switch. On the other hand, a virtual tap can block and copy data within the hypervisor layer for software-based networks.

A network packet broker (NPB) is recommended as the best modern monitoring tool for securing data on cloud networks. An NPB would monitor all organizational traffic, thus enhancing total visibility across all administrative functions and networks. A physical NPB can be deployed within the corporate premises, while a software-based NPB is deployed within its cloud services.

A hybrid cloud environment provides better security prospects for an organization's data than public and private cloud environments. However, hybrid systems' data security requires varied protocols for all interconnected networks. While data in private clouds is primarily secure, the public cloud requires the organization to establish the best platform and partnerships to integrate all data requirements successfully.

Future research on cloud computing holds great potential for advancements in technology and innovation. Security, scalability, and data management will continue to be critical for researchers and industry professionals. Integrating artificial intelligence and machine learning in cloud systems presents an exciting avenue for exploration and development. Addressing environmental sustainability and energy efficiency will also be crucial areas of study. The evolving landscape of cloud computing offers rich opportunities for future research and development.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Mell, P. and Grance, T. (2009) The National Institute of Standards and Technology Definition of Cloud Computing. National Institute of Standards & Technology.

[2] Rountree, D. and Castrillo, I. (2014) The Basics of Cloud Computing, Syngress. https://doi.org/10.1016/C2012-0-02521-5

[3] Laszewski, T. and Nauduri, P. (2012) Migrating to the Cloud. Syngress. https://doi.org/10.1016/C2010-0-67145-8

[4] Pallis, G. (2010) Cloud Computing: The New Frontier of Internet Computing. *IEEE Internet Computing*, **14**, 70-73. https://doi.org/10.1109/mic.2010.113

[5] Wei, Y. and Blake, M.B. (2010) Service-Oriented Computing and Cloud Computing: Challenges and Opportunities. *IEEE Internet Computing*, **14**, 72-75. https://doi.org/10.1109/mic.2010.147

[6] Rajan, S. and Jairath, A. (2011) Cloud Computing: The Fifth Generation of Computing. 2011 *International Conference on Communication Systems and Network Technologies*, Katra, 3-5 June 2011, 665-667. https://doi.org/10.1109/csnt.2011.143

[7] Latif, R., Abbas, H., Assar, S. and Ali, Q. (2014) Cloud Computing Risk Assessment: A Systematic Literature Review. In: Park, J., Stojmenovic, I., Choi, M. and Xhafa, F., Eds., *Future Information Technology*, Springer, 285-295. https://doi.org/10.1007/978-3-642-40861-8_42

[8] Sagiroglu, S. and Sinanc, D. (2013) Big Data: A Review. 2013 *International Conference on Collaboration Technologies and Systems* (*CTS*), San Diego, 20-24 May 2013, 42-47. https://doi.org/10.1109/cts.2013.6567202

[9] Chen, D. and Zhao, H. (2012) Data Security and Privacy Protection Issues in Cloud Computing. 2012 *International Conference on Computer Science and Electronics Engineering*, Hangzhou, 23-25 March 2012, 647-651. https://doi.org/10.1109/iccsee.2012.193

[10] Takabi, H., Joshi, J.B.D. and Ahn, G. (2010) Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy Magazine*, **8**, 24-31. https://doi.org/10.1109/msp.2010.186