Security and Performance of Public Clouds vs Private Clouds.

Sarthak Siddhant Bharadwaj
sarthak7@colostate.edu
CS Dept, Colorado State University

***Abstract*— Customers can access a pool of shared computer resources on a pay-per-use or on-demand basis with a cloud computing business providing several advantages for individuals and businesses in terms of capital investment and operating cost savings. The use of cloud computing is however constrained by a number of issues, notwithstanding these benefits. Security is an important consideration.This paper will compare various types of clouds, how secure they are and ways to make cloud more secure for the end users.[2]**

I. INTRODUCTION

Cloud computing broadly describes off-premise,on demand computing where the end-user is provided applications, computing resources, and services (including operating systems and infrastructure) by clouds services provider via the Internet.

Cloud computing is divided into two geographical categories[3]: Private Clouds provide exclusive architecture for a single client, with options for both on- and off-premises deployment; Public Clouds make use of vendor facilities that house shared equipment. Private clouds, however more costly, offer dedicated resources that are not shared by other companies.With a hybrid cloud, less important apps are hosted in public clouds while more important ones are hosted in private, secure clouds. This method, which makes advantage of "cloud bursting," uses internal infrastructure to optimize routine operations while accessing the cloud for heavy workloads.

A. *Proposed measures for security*

Cloud security can be achieved in several forms, protection against the Network attacks, Software attacks, Intrusion Detection, Access control, Analysis of abnormal behavior, Analysis of Virus, Analysis of Malware, Analysis of Trojans and so on.[1]

Password security :vital for cloud services. Users must use unique, strong passwords, avoiding reuse across platforms. Cloud providers should unlink usernames and passwords to bolster resilience against potential breaches.[5]

Access Recovery :For cloud access recovery, users should utilize confidential details, not information vulnerable to social engineering from social media profiles.

Multifactor authentication :Multi-factor authentication enhances cloud security by requiring two or more verification factors, such as knowledge (e.g., an additional password), possession (e.g., RSA key or USB key), or biometric features. This adds an extra layer beyond traditional username and password access.[1]

Login Monitor: Users and cloud providers should monitor recent devices accessing cloud services to detect suspicious logins. Timely password changes are recommended for unknown devices or locations. Cloud providers must enhance login statistics, detailing connected devices for all customers.

II. PROPOSED WORK

Identifying security vulnerabilities and conducting a comprehensive comparison of public and private clouds using various metrics is part of my plan. I intend to assess the speed and accuracy of both cloud types based on different criteria. While absolute performance values may be influenced by the uncontrollable nature of physical resources in public clouds, the comparative analysis remains valuable for users selecting a suitable cloud service for specific applications. The lower performance of public clouds is due to shared physical resources among multiple clients, leading to variations in processor load, memory access time, and I/O traffic capacity.[4]

III. CONCLUSIONS AND FUTURE WORK

I've proposed security enhancements based on my initial investigation into cloud security. In future projects, I plan to assess and compare the performance, speed, pricing, and security features of public and private clouds. This analysis aims to determine the optimal choice for customers, considering both business and personal use.

REFERENCES

[1] J. Surbiryala and C. Rong, "Cloud Computing: History and Overview," 2019 IEEE Cloud Summit, Washington, DC, USA, 2019, pp. 1-7, doi: 10.1109/CloudSummit47114.2019.00007.

[2] V. Vassilev et al., "Network Security Analytics on the Cloud: Public vs. Private Case," 2023 13th International Conference on Cloud Computing, Data Science Engineering (Confluence), Noida, India, 2023, pp. 151-156, doi: 10.1109/Confluence56041.2023.10048889.

[3] Solanke Vikas, Kulkarni Gurudatt, Maske Vishnu, Kumbharkar Prashant on "Private Vs Public Cloud" , Solanke Vikas et al, International Journal of Computer Science Communication Networks,Vol 3(2), 79-8379 ISSN:2249-5789

[4] C. Mancaş, "Performance analysis in private and public Cloud infrastructures," 2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet), Galati, Romania, 2019, pp. 1-6, doi: 10.1109/ROEDUNET.2019.8909453.

[5] I. Gordin, A. Graur and A. Potorac, "Two-factor authentication framework for private cloud," 2019 23rd International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania, 2019, pp. 255-259, doi: 10.1109/ICSTCC.2019.8885460.