International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Enhanced Cloud Computing Security based on Single to Multi Cloud System

G. Mohideen Basha, S. Nirmala Sugirtha Rajini

PG Student, Department of Computer Applications, Dr. M. G. R. Educational and Research Institute, Chennai - 95
Email: *mohideenb476[at]gmail.com*

Abstract: ***Cloud computing has increased rapidly in many organizations and then it's utilized. Cloud computing provides safe data. Cloud computing provides many advantages in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi - clouds", or in other words, "inter clouds" or "cloud - of - clouds" has emerged recently. We propose the recent research related to single and multi - cloud security and address possible solutions. It is found that the research into the use of multi - cloud providers to maintain security has received less attention from the research community than the use of single clouds. This work aims to promote the use of multi - clouds due to their ability to reduce security risks that affect the cloud computing user. We proposed the AES algorithm can explore the cloud sharing to multiple clouds. This algorithm protects secure to personal information, financial records, and other confidential records. The system is highly effective in accuracy.***

Keywords: Cloud computing, cloud of clouds, multi - clouds

1. Introduction

Cloud computing is an IT approach that provides scalable and lightweight IT capabilities to customers using Internet technology. In terms of describing cloud computing, really isn't such a backwards term; however, it is an evolving concept that combines many existing technologies to provide a useful new IT management tool. Using web services in the cloud is called cloud services [1].

Virtualization defines an abstract approach to creating a computer that allows resources to be distributed in a cloud environment. Resource sharing is possible with a virtual machine via a file, commonly called an image, which can be generated by users or obtained from external sources [2].

llustrates general management of resources without any assumptions in a service - based cloud model. It should be noted that in real scenarios the levels of management may vary depending on the user's preferred settings. As described in virtualization versions 2.1.1 and HV 2.1.2, the management of the type, architecture, and therefore layers may change accordingly [3].

The user can then use the provided services through APIs over the Internet. A company can rent all the necessary IT resources to build a software ecosystem with a per - use subscription. Amazon EC2 (Elastic Compute Cloud) is an example of IaaS providers. In this environment, users have more flexibility to run multiple virtual machines simultaneously. In IaaS, a user can deploy a private or public image, which is a template for configuring a VM. Private images are defined by users, while public images are published by external sources such as a company or an open source organization [4].

In This article focuses on issues related to cloud computing data security when data is exchanged with other (third - party) clouds or an unknown cloud service provider. In addition, a single cloud provider is transformed into a multi - cloud system, and the information security issues of single and multi - cloud cloud services are studied. It analyzes next - generation multi - cloud solutions and current cloud services and explores their limitations [5].

2. Literature Survey

According to **Pramod Chandra P Bhatt**. et al., 2020 server refers to larger computers that support multiple users at the same time, usually using multiple multi - core processors, larger memories, and larger storage capacity. Historically, mainframe computers fit this description, and more recently, smaller computer servers have been combined to meet the needs of multiple users simultaneously [6].

According to **Azman Samsudin**. et al., 2021 cloud services are vulnerable to attack. Data manipulation is a serious threat to data integrity that can occur in cloud services, a relatively new offering under the cloud services. Data can be corrupted and malicious actors can exploit it to their advantage [7].

According to **Seema Nikam**. et al., 2022 cloud service has recently gained a lot of attention thanks to its cost - effective and high - quality services. Over the past decade, cloud services have inevitably entered the daily lives of businesses and individuals through products and services. Affordable capabilities encourage companies to outsource part of their business to accelerate services and multiply value [8].

According to **Mohamed Ezz**. et al., 2023 multi - factor authentication ensures that only genuine cloud users can access cloud applications, data, services and resources, making it more secure for businesses and less hassle for users. The number of authentication factors varies depending on the architecture of the security framework and the level of security required [9].

GO Ogunleye. et al., 2022 says that data stored in the cloud is said to be dangerous and can be hacked. It was difficult for users to trust their data in the cloud. Users want to know that their data can be accessed from anywhere and not accessed by unauthorized users. Another problem is user authentication through the cloud [10].

3. Proposed System

Our proposed project aims to advocate for the adoption of multi - cloud environments as a strategy to mitigate security risks inherent in cloud computing. We propose leveraging the AES algorithm to distribute data across multiple cloud platforms effectively. This proposed algorithm ensures the secure storage and transmission of sensitive information such as personal data, financial records, and confidential documents. Our proposed system is designed to deliver high levels of accuracy and efficiency in safeguarding data integrity and confidentiality across diverse cloud infrastructures.

Architecture Diagram:

4. Explanation

Single Cloud:
Begin with a representation of the initial single cloud architecture, where all services and data are hosted within a single cloud provider's infrastructure. Explain that while single cloud architectures offer simplicity, they also pose risks such as vendor lock - in, limited redundancy, and a single point of failure.

Multi - Cloud Architecture:
Transition to the enhanced multi - cloud architecture, where services and data are distributed across multiple cloud providers' infrastructures. Illustrate the presence of multiple cloud providers (e. g., AWS, Azure, Google Cloud) interconnected through secure network connections.

Key Components:
Load balancers and traffic managers for distributing incoming requests across multiple cloud environments. Virtual private networks (VPNs) or dedicated connections for establishing secure communication between the organization's on - premises infrastructure and the multi - cloud environment. Identity and access management (IAM) solutions for centrally managing user access and permissions across multiple cloud platforms.

Security Enhancements:
Reduced risk of vendor lock - in, enabling organizations to leverage best - of - breed solutions from multiple cloud providers. Improved resilience against cyber threats and potential service outages through geographic redundancy and diversified infrastructure. Enhanced data protection and compliance adherence by implementing consistent security policies and controls across multiple cloud environments.

Scalability and performance: Discuss how the multi - cloud architecture enables scalability and enhances performance by allowing organizations to leverage the resources and capabilities of multiple cloud providers based on workload requirements and geographic proximity to end – users

5. Result and Discussion

Enhanced security posture through distributed authentication and reduced dependence on a single provider. improved resilience against potential security breaches or service disruptions. greater flexibility and scalability to meet evolving business needs and regulatory requirements.

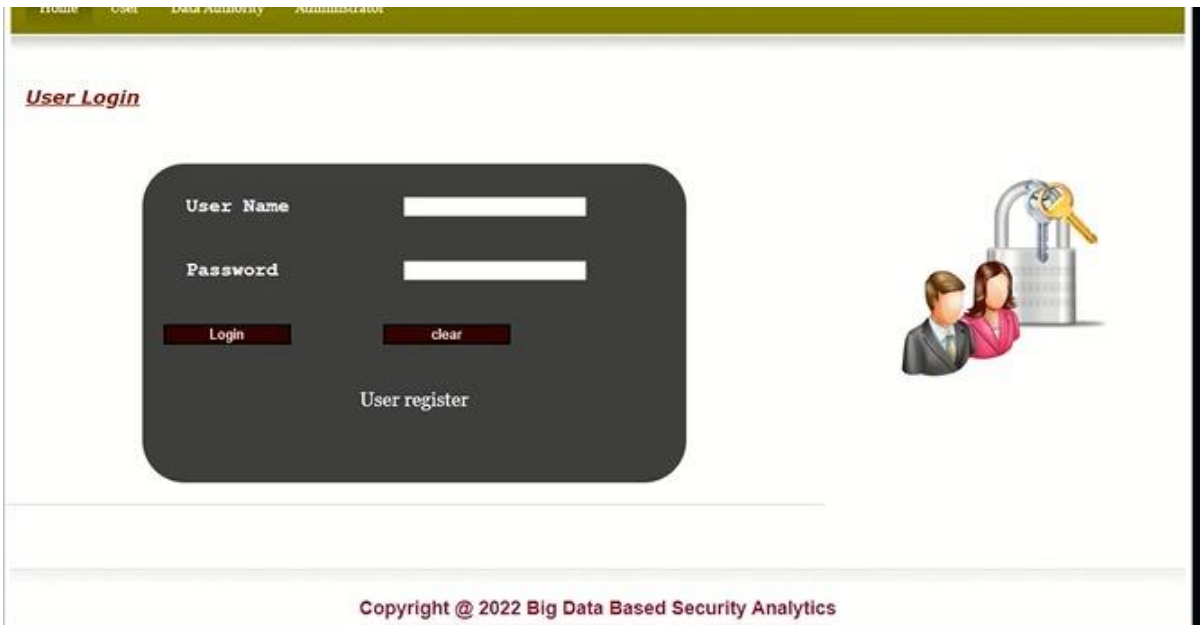

Figure 1: User Login

User Login:
The process involves entering a user name and password on the login page to gain access for big data based security analytic. Implement robust logging and monitoring mechanisms to track user login activities and identify any suspicious or unauthorized access attempts.

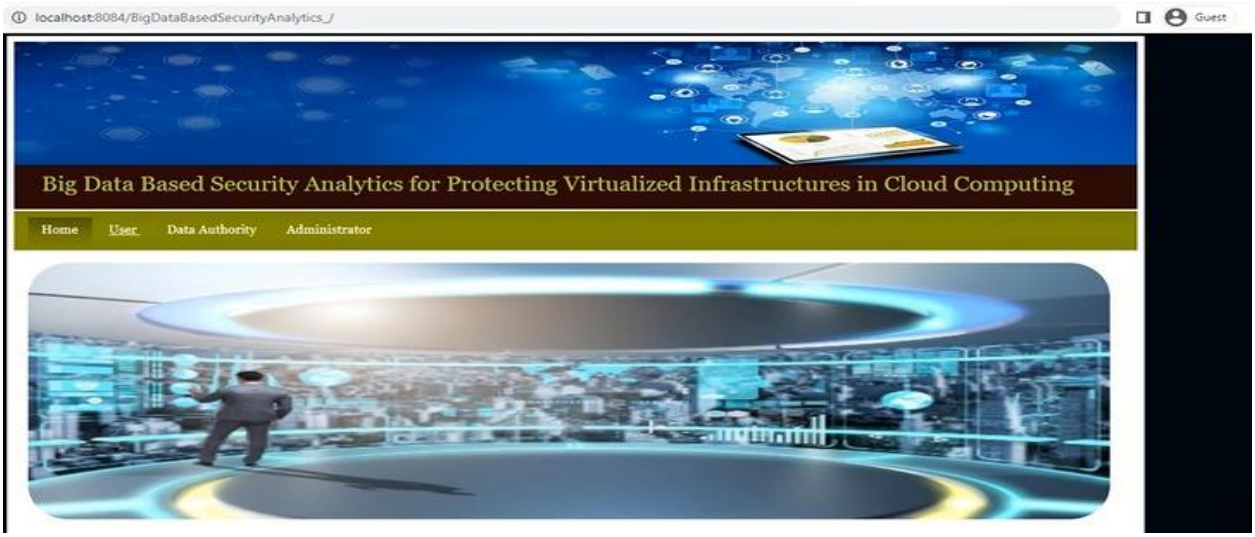

Figure 2: Home page for Big data analytics

Home page for Big data analytics:
After logging in, users are directed to the home page of the big data - based data analytics platform. This page serves as a central hub where users can access various analytics tools, dashboards, reports, and other features for analyzing large datasets.

.

Figure 3: User Register

User Registration:
Before accessing the platform, users need to register by providing necessary information such as name, email address, and creating a password. Registration allows users to create an account and access the platform's functionalities.

Figure 4: Finalize File

Finalize File:
This step involves users completing the process of uploading or preparing a file for analysis within the data analytics platform. Users may need to specify parameters, select analysis methods, or configure settings before finalizing the file for processing.

6. Conclusion

Provide a conclusive statement summarizing the article impact and significance in advancing cloud computing security. Emphasize the importance of continuous monitoring, adaptation, and innovation to maintain a secure and resilient multi - cloud environment in the ever - evolving landscape of cybersecurity threats. Recap the primary objectives of the system including enhancing security, resilience, and flexibility by transitioning from a single to a multi - cloud environment. Highlight the accomplishments and outcomes of the project, such as the successful implementation of multi - cloud architecture, integration of advanced security measures, and improvements in system reliability and performance. Discuss the specific security enhancements achieved through the adoption of a multi - cloud approach, such as reduced risk of vendor lock - in, improved data redundancy and availability, and enhanced protection against cyber threats and service outages. Outline the benefits gained from transitioning to a multi - cloud system, including increased resilience, scalability, and compliance adherence, as well as greater flexibility in resource allocation and workload. Offer insights into future directions and potential areas for further improvement or expansion. This may involve exploring additional security measures, optimizing resource utilization, or leveraging emerging technologies to enhance cloud computing security further.

References

[1] Enokido T, Aikebaier A, Takizawa M (2019) A model for reducing power consumption in peer - to - peer systems. IEEE Syst J 4 (2): 221–229

[2] [24] H. Tabrizchi and M. K. Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” J. Supercomput., vol.76, no.12, pp.9493–9532, 2020.

[3] A. Rashid and A. Chaturvedi, “Virtualization and its role in cloud computing environment,” International Journal of Computer Sciences and Engineering, vol.7, no.4, pp.1131–1136, 2019

[4] A. H. Shaikh and B. Meshram, “Security issues in cloud computing, ” in Intelligent Computing and Networking. Springer, 2020, pp.63–77.

[5] Puneeth Kumar BS, Ramesh Naidu P, Sridhara SB (2023) Internet of Things and cognitive radio networks: applications, challenges and future. In: Yadav S, Chaudhary K, Gahlot A, Arya Y, Dahiya A, Garg N (eds) Recent advances in metrology. Lecture Notes in Electrical Engineering, vol 906. Springer, Singapore.

[6] Cloud computing with security Naresh Kumar Sehgal, Pramod Chandra P Bhatt, John M Acken Concepts and practices. Second edition. Switzerland: Springer, 2020.

[7] An integrated architecture for maintaining security in cloud computing based on blockchain Ruba Awadallah, Azman Samsudin, Je Sen Teh, Mishal Almazrooie IEEE Access 9, 69513 - 69526, 2021.

[8] Cloud computing security: A survey of service - based models Fatemeh Khoda Parast, Chandni Sindhav, Seema Nikam, Hadiseh Izadi Yekta, Kenneth B Kent, Saqib Hakak Computers & Security 114, 102580, 2022.

[9] Strengthening Cloud Security: An Innovative Multi - Factor Multi - Layer Authentication Framework for Cloud User Authentication Ayman Mohamed Mostafa, Mohamed Ezz, Murtada K Elbashir, Meshrif Alruily, Eslam Hamouda, Mohamed Alsarhani, Wael SaidApplied Sciences 13 (19), 10871, 2023.

[10] Elliptic Curve Cryptography Performance Evaluation for Securing Multi - Factor Systems in a Cloud Computing Environment GO Ogunleye, SE Akinsanya Iraqi Journal of Science, 3212 - 3224, 2022.