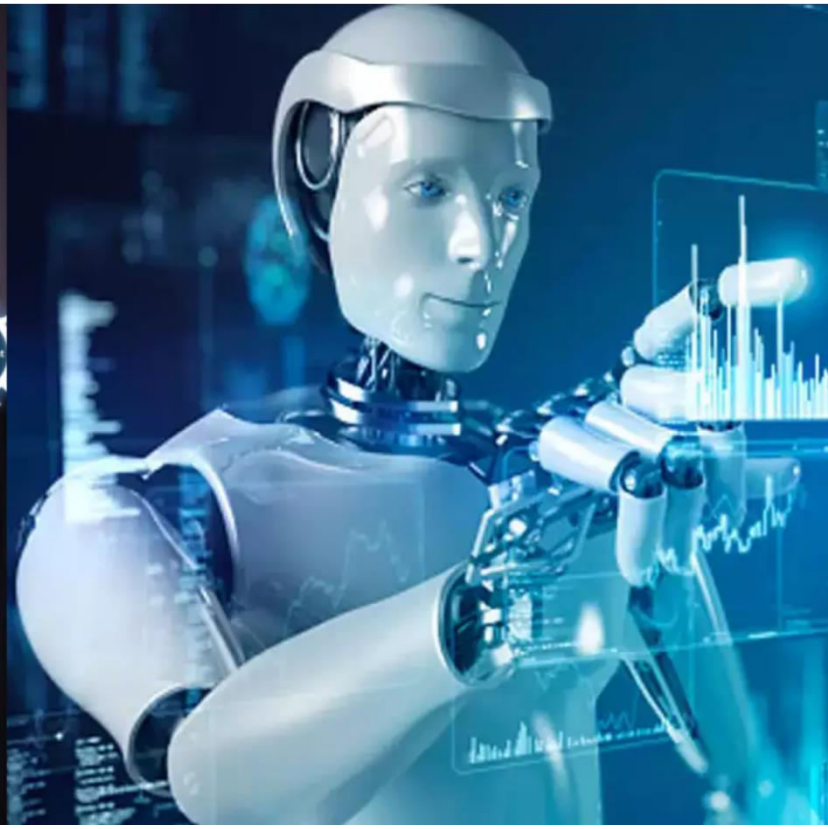
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404133|

Multi-Tenant Architectures with Efficient Resource Management in Cloud Applications

Mrs. M.Senthamarai Selvi, R.Priya

Assistant Professor, Department of Computer Science and Engineering, Mrk Institute of Technology, Nattarmangalam, Kattumannarkoil, Cuddalore District, Tamil Nadu, India

Student, Department of Computer Science and Engineering, Mrk Institute of Technology, Nattarmangalam, Kattumannarkoil, Cuddalore District, Tamil Nadu, India

ABSTRACT: Today's most modern research area of computing is cloud computing due to its ability to diminish the costs associated with virtualization, high availability, dynamic resource pools and increases the efficiency of computing. But still it contains some drawbacks such as privacy, security, etc. This paper is thoroughly focused on the security of data of multi tenant model obtains from the virtualization feature of cloud computing. We use AES-128 bit algorithm and cloud SQL to protect sensitive data before storing in the cloud. When the authorized customer arises for usage of data, then data firstly decrypted after that provides to the customer. Multi tenant infrastructure is supported by Google, which prefers pushing of contents in short iteration cycle. As the customer is distributed and their demands can arise anywhere, anytime so data can't store at particular site it must be available different sites also. For this faster accessing by different users from different places Google is the best one. To get high reliability and availability data is stored in encrypted before storing in database and updated every time after usage. It is very easy to use without requiring any software. This authenticate user can recover their encrypted and decrypted data, afford efficient and data storage security in the cloud.

KEYWORDS: Cloud Computing, Multi-tenancy, Multi-tenant architecture, security, Database storage, Partition.

I. INTRODUCTION

Cloud Computing is the modern computing technique which is based on Grid, Utility Computing, quickly adopted by organizations and businesses alike to help increase profit margins by decreasing overall IT costs as well as provide clients with faster implementation of services. Service are delivered to client as three major service models—SaaS, which includes Web services such as Yahoo Flickr, Google Docs, and Microsoft website designer. These Web services perform functions traditionally done with software installed on an individual computer. The second service module is platform as a service (PaaS). This model provides computing services as websites—such as mashups or the APIs of Google Maps—as well as file storage systems—such as Drop-box or box.net. The final service model is infrastructure as a service (IaaS). It includes business-to-business (B2B) services that are usually invisible to customers. The first service to reach the market was Amazon Elastic Compute Cloud (EC2)[1]. Currently the cloud computing industry has no standard business model, instead the companies are experimenting with four different ideas—private, community, public, and hybrid models.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404133|

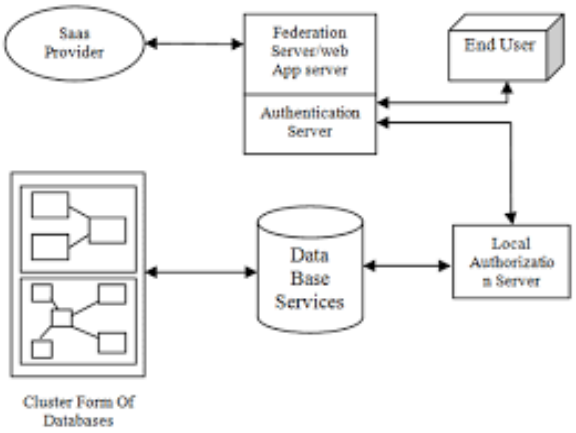


Fig 1: Secure Multi-Tenant Model for SaaS System

Various characteristics of cloud such as elasticity, metered service, on-demand service, broad network access will allow services to be shared among different users or same organization or between different organization which leads to an important cloud element multitenancy[2]. Multi-tenancy spans the layers at which services are provided. In IaaS, tenants share infrastructure resources like hardware, computation servers, and data storage devices. With SaaS, tenants are sourcing the same application (e.g., Salesforce.com), which The impact of multi-tenancy is visibility of residual data or trace of operations by other user or tenant. The majority of the cloud service providers offer multitenancy to capitalize on the associated economies of scale which also translates into savings for the end user. In fact the competitive nature of cloud computing is such that cloud service providers have to minimize the total cost of ownership of their IT infrastructure, thus introducing multitenancy is a popular way to reducing total cost of ownership.

The rapid adoption of cloud computing has led to the proliferation of multi-tenant environments, where multiple customers share the same underlying infrastructure to maximize resource utilization and reduce costs [1]. While this model offers significant advantages in terms of scalability and efficiency, it also introduces complex challenges in balancing robust security measures with optimal performance. As organizations increasingly rely on shared cloud resources, the need to maintain strong security protocols without compromising system responsiveness has become paramount [2]. This delicate balance between security and performance in multi-tenant cloud environments presents a critical area of study, with far-reaching implications for both cloud service providers and their clients. Our article explores the intricate interplay between various security implementations—such as data isolation, access control, network security, and threat detection—and their impact on key performance metrics in shared cloud infrastructures. By examining these trade-offs, we aim to provide insights and strategies for optimizing the security-performance nexus in multi-tenant cloud computing.

II. RELATED WORK

Various studies reveal security issues regarding multi-tenancy support, which is a prime focus of this paper. Multi-tenancy is the ability to efficiently deal with multiple administrative domains (tenants) that are using the same service which, in turn, has isolated resources belonging to particular tenants. In tenant based environment VM security , hypervisor security, platform security, Data storage security, user authentication, etc. to be considered seriously. The following are some of the threat vectors affecting the multi-tenant data center:

In Mulit-tenant applicatins unlike IaaS where multiple tenants share resources, SaaS tenants share a database. Users of Salesforce.com or SmugMug, for instance, pay to use an application that manages their customers and photos respectively. While the value is in the application interfaces that make it easy to manage complex tasks and large data sets, the data itself is stored in a database as rows in tables that the tenants of Salesforce.com and SmugMug databases share. The customer ID is what distinguishes one row from the next. In this area, security concerns run high that misconfigured application code or an error in an access control list may put tenant information at risk of theft and misuse. For controlling access to database data, there are quite a few tools and technologies available. The new

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404133|

applications implemented is used for authentication and authorization of the access request so that only certain rows or fields are modifiable based on security policies that ensure that access is warranted. Encryption of data in the database is also common to protect it at rest, so that if it is ever compromised or stolen it would be difficult todecipher the underlying data.

According to Armbrust and Fox (2010) and Feng et al (2011), the fundamental security issue with multitenancy is clients using Cloud Computing by employing single and the same computer hardware to share and process information. This presents a number of challenges in terms of compliance, security, and privacy (Bernardo and Hoang, 2010). The lack of user network isolation, In this technique, as the data stored by cloud applications used by tenants is on a same database but in a different partitions. So to ensure security for data of each tenant, in this paper we are proposing Data Partition Encryption Technique(DPET) in which each record in partition before stored is encrypted two times first by tenant's public key and by Cloud Service Provider (CSP), and decrypted only by tenant. Since the record 'R' to be stored at CSP is encrypted by tenant, 'R' cannot be revealed by CSP also. In this way the proposed DPET technique is secure by not revealing the record to other Tenants residing or using shared database.

The fundamental security issue with multitenancy is the very premise in which multitenancy is based upon; that is, multiple tenants sharing the same computer hardware. Indeed, using a multitenancy approach for the development of public cloud infrastructure presents a number of challenges in terms of compliance, security and privacy . One of the main challenges of using this form of multiple services is ensuring data isolation. Data management is critical as several users will be using the same system but all require privacy and confidently . Indeed multitenancy and lack of network isolation among tenants make the public cloud vulnerable to attacks [3] .

III. METHODS

A. Multi-Tenancy In Cloud Computing

Multi-tenancy is a fundamental architectural principle in cloud computing where a single instance of software serves multiple customers or "tenants." Each tenant's data and configuration settings are isolated and remain invisible to other tenants, despite sharing the same computational resources. This model enables cloud service providers to achieve economies of scale, offering cost-effective solutions by distributing infrastructure costs across multiple clients [3].
In multi-tenant environments, resources such as computing power, storage, and networking are dynamically allocated and deallocated based on tenant demands. This elasticity allows for efficient resource utilization but also introduces complexities in managing security and performance across shared infrastructure.

Security in multi-tenant cloud environments encompasses a wide range of considerations, from data isolation and access control to network security and compliance. The shared nature of these environments introduces unique challenges, as a security breach in one tenant's environment could potentially impact others.

Key security considerations include:

1. Data isolation: Ensuring that each tenant's data remains segregated and inaccessible to others.
2. Access control: Implementing robust authentication and authorization mechanisms.
3. Network security: Protecting against both external threats and potential lateral movements within the shared infrastructure.
4. Compliance: Meeting various regulatory requirements while serving multiple tenants with potentially different compliance needs.

Performance Metrics In Cloud Systems

Performance in cloud computing is typically measured across several dimensions, each critical to ensuring service quality and user satisfaction. Common performance metrics include:

1. Latency: The time taken for a request to receive a response.
2. Throughput: The amount of data processed in a given time period.
3. Resource utilization: The efficiency of CPU, memory, storage, and network usage.
4. Scalability: The system's ability to handle increased load without significant performance degradation.
5. Availability: The percentage of time the system is operational and accessible.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404133|

These metrics are often governed by Service Level Agreements (SLAs) between cloud providers and their tenants, setting expectations for system performance.

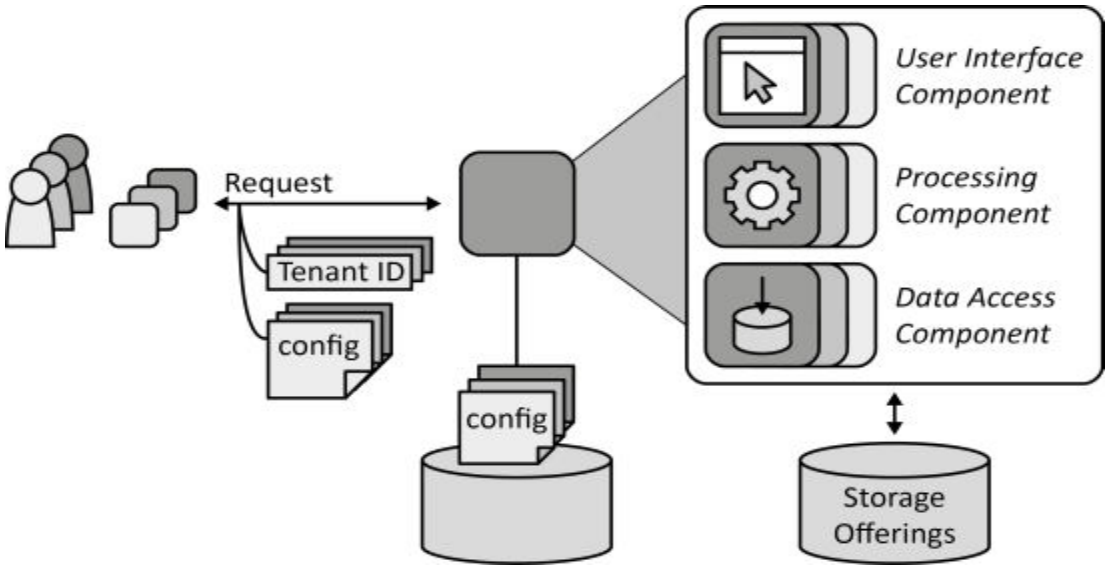


Fig 2: Tenant-isolated Component | Cloud Computing Patterns

The security-performance trade-off paradigm in multi-tenant cloud environments refers to the often inverse relationship between implementing robust security measures and maintaining high system performance. This paradigm posits that enhancing security often comes at the cost of reduced performance, and vice versa [4].

For instance, implementing strong encryption for data at rest and in transit enhances security but can increase latency and reduce throughput. Similarly, rigorous access control mechanisms might improve security but could lead to longer response times for user authentication and authorization.

Understanding and managing this trade-off is crucial for cloud service providers and tenants alike. It requires a nuanced approach that considers the specific needs of each application, the sensitivity of the data involved, and the performance expectations of end-users.

The challenge lies in finding an optimal balance that provides adequate security without significantly compromising performance, or high performance without exposing the system to unacceptable security risks. This balance often involves a combination of technological solutions, architectural designs, and policy frameworks tailored to the specific requirements of the multi-tenant environment.

IV. EXPERIMENTAL RESULTS

To understand this system better, we describe the scenario of a customer joining a Cloud provider. The process starts when a customer needs to utilize a public IaaS Cloud as its infrastructure. Firstly, the customer will register either online or by visiting the Cloud provider. Then, the provider will verify the information provided by the customer; official documents could be used for this purpose. If the customer passes the verification process, the provider will approve the process to the next stage. After the verification and approval processes, the customer's data will be stored in the control Database where all resource allocation restrictions will be specified by the CSP.

In most scenarios, storage resources will be tightly coupled to computational resources. A multi-tenant application running on the cloud could for example consist of multiple Virtual Machine (VM) instances. Initially, a single datacenter or even a single VM could be used to execute the application, but as the number of tenants and therefore the load on the VM increases over time, multiple geographically distributed instances could be provisioned. This might

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404133|

however require the migration of existing VMs to a different location, resulting in the migration of some blob storage, the provisioned virtual disks. Fig. 2 illustrates this concept. In this example, computational resources are represented by hardware (HW in the figure), these are the physical servers hosting the VMs, and storage resources are represented by disks (HDD), storing the virtual disk images. A tenant user located in the US is redirected to a provisioned VM in the North Central US Data Center, whereas for the European tenant user resources are provisioned in the West Europe Data Center. The tenant data should be stored close to the selected application server, preferably in the same data center, to minimize network latencies.

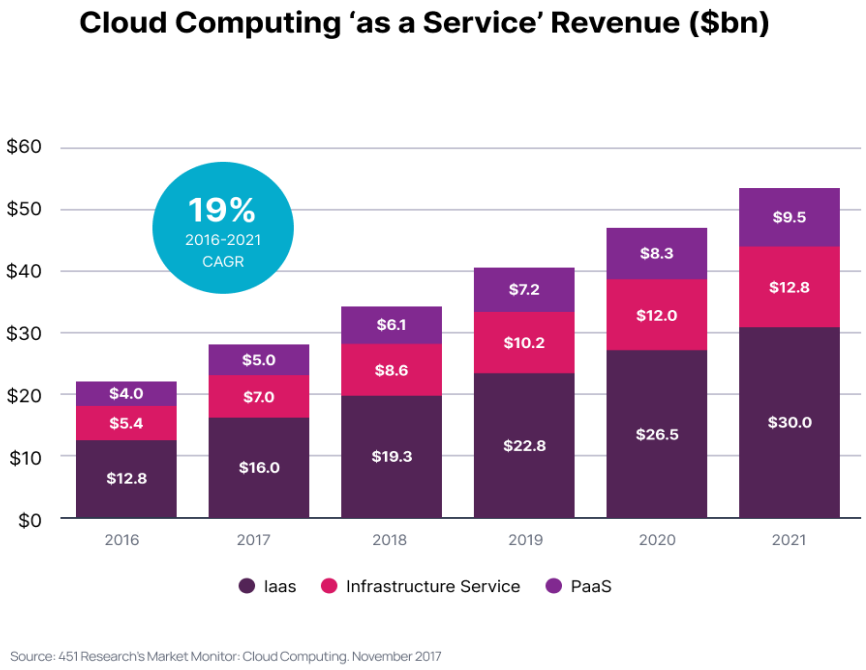


Fig 3: Multi-Tenant Architecture: Designing SaaS Application | Brocoders blog about software

The remainder of this article is structured as follows. In the next section, we discuss related work within the field. Next, in Section 3 we provide a general overview of the TDS system and discuss the major design decisions. In Section 4 we introduce several static and dynamic bin packing algorithms for the (re)allocation of tenant storage. In Section 5 we define the relevant evaluation metrics and present the most significant evaluation results and discuss these in Section 6. Finally, in Section 7 we state our conclusions and discuss avenues for future research.

V. CONCLUSION

This comprehensive examination of security and performance trade-offs in multi-tenant cloud environments underscores the complex and dynamic nature of modern cloud computing. Throughout our analysis, we have demonstrated that achieving an optimal balance between robust security measures and high performance is not a trivial task, but rather a continuous process of evaluation, optimization, and innovation. The case studies presented illustrate that tailored approaches, considering the specific needs and constraints of each system, are crucial for success. As cloud technologies continue to evolve, the integration of AI and automation in managing these trade-offs shows great promise, potentially leading to more adaptive and efficient solutions. However, significant challenges remain, particularly in areas such as scalability, privacy-preserving computation, and cross-layer optimization. Future research directions, including quantum-resistant cryptography and edge computing security, offer exciting opportunities for advancing the field. Ultimately, the ongoing pursuit of harmonizing security and performance in multi-tenant cloud environments will play a pivotal role in shaping the future of cloud computing, enabling more secure, efficient, and reliable services for a wide range of applications and industries.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404133|

REFERENCES

1. J. A. García-Espín, J. Ferrer Riera, S. Figuerola, and E. López, "A multi-tenancy model based on resource capabilities and Ownership for infrastructure management," in 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2012, pp. 1-8. Link: https://ieeexplore.ieee.org/document/6427535
2. M. Armbrust et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, 2010. Link: https://dl.acm.org/doi/10.1145/1721654.1721672
3. Geekflare, "Understanding Single Tenant vs. Multi-Tenant in Cloud Computing," Geekflare, 2023. Link: https://geekflare.com/single-tenant-vs-multi-tenant/
4. Shankertech Blog, "Single vs Multi Tenant: Key Differences and Best Use Cases," Shankertech Blog, 2024. Link:https://blog.shankertech.com/single-vs-multi-tenant-key-differences-and-best-use-cases/
5. Permify, "What is Multi-Tenant Architecture?", Permify Documentation, 2024. Link: https://permify.co/post/multitenant-architecture/
6. StarAgile, "Multi-Tenant Architecture in Cloud Computing," StarAgile Technical Blog, 2024. Link: https://staragile.com/blog/multi-tenant-architecture
7. Ceri, S., Pernici, B., & Wiederhold, G., "Distributed database design methodologies," in Proceedings of the IEEE, vol. 75, no. 5, pp. 532-543, 1987. Link: https://ieeexplore.ieee.org/abstract/document/1458038/authors#authors
8. Anupama, C., & Lakshmi, C., "A Comprehensive Review on Data Partitioning and Sampling Techniques for Processing Big Data," in 2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), pp. 1-8, 2022. Link: https://ieeexplore.ieee.org/abstract/document/10047766
9. TechRepublic, "Implement security management with these six steps," TechRepublic Security Guidelines, 2024. Link: https://www.techrepublic.com/article/implement-security-management-with-these-six-steps/
10. MDN Web Docs, "Practical security implementation guides," Mozilla Developer Network, 2024. Link: https://developer.mozilla.org/en-US/docs/Web/Security/Practical_implementation_guides
11. P. Estrach, "Scalability in Cloud Computing: A Deep Dive," MEGA Technical Publications, 2023. https://www.mega.com/blog/what-is-scalability-in-cloud-computing

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details