An Amalgamation of Ontology Module in MultiTenant Cloud Architecture

Dimpy Jindal
Research Scholar
Amity University Rajasthan

Manju Kaushik
Research Guide
Jaipur Amity University Rajasthan

Barkha Bahl
Research Co-guide
Jaipur Trinity Institute of Professional Studies

ABSTRACT

“Cloud” is an amalgamation of servers, software and applications that can be accessed by individual or business organizations with an aim of accessing services at pay per usage policy. Customers or tenants get access to some portion of cloud to run their tasks and performs computation. As there are many challenges on cloud while accessing, storing and securing data like trade off in applications, higher costs incurred for low supply of resources and many more. It leads to the need of Multitenancy. Multitenancy is an approach of achieving flexibility, higher degree of scalability, clustering of services and reduced data accessing costs. It requires accessing of database by multiple clients at one go and it is obvious that it may lead to security risks in cloud environment.

The paper makes readers aware of concept of Multitenancy and its actual need in today’s computing era. It is followed by identification of security threats associated with multitenant environment in form of literature review. Lastly, a secured multitenant cloud environment using concept of ontology is being proposed in the following paper.

Keywords

Cloud computing, Multitenancy, ontology, hypervisors and segmentation

1. INTRODUCTION

Cloud computing can be defined as the amalgamation of servers which helps in accessing and management of data to be stored on local server by reducing workload over the Internet [1]. It is pay per service model i.e. customers or companies can access the cloud services by paying at certain period of time. The servers are arranged as per the user needs. Cloud computing is categorized into three cloud models [2].They are described in table 1. The phenomenon also includes deployment models like private, public, community and hybrid models [3]. Cloud computing depends on sharing of resources cohesively and economically without affecting network parameters. But, in practical view it is not feasible to achieve full utilization of resources due to various factors like deadlock, lock-in-period, network congestion and security issues. To overcome or mitigate this, concept of tenants in the context of cloud computing is being introduced [4]. The idea of Multitenancy or multiple tenants sharing resources is primary to cloud computing. It leads to the development of efficient and scalable network infrastructure. The concept of Multitenancy is mostly seen in Infrastructure as a service (IaaS) and Software as a service (SaaS). In case of IaaS, the infrastructure resources such as hardware, servers, and storage devices are shared by multiple tenants while in latter case, the data of multiple tenants is stored in same database so that it can be accessed directly within the application. The given paper is categorized into following sections. Section 2 provides information about Multitenancy and its need to certain extent. Section 3 presents brief literature review of studies conducted in the context of security challenges associated with multitenant cloud. Section 4 describes some possibilities of data storage in multitenant system. Various issues dealing with mentioned approaches are being described in this section. Section 5 presents a bird’s eye view of a secured ontology based multitenant architecture after addressing the issues that have been discussed in the previous section. Section 6 concludes the given paper followed by references.

Table 1: Comparison among cloud models

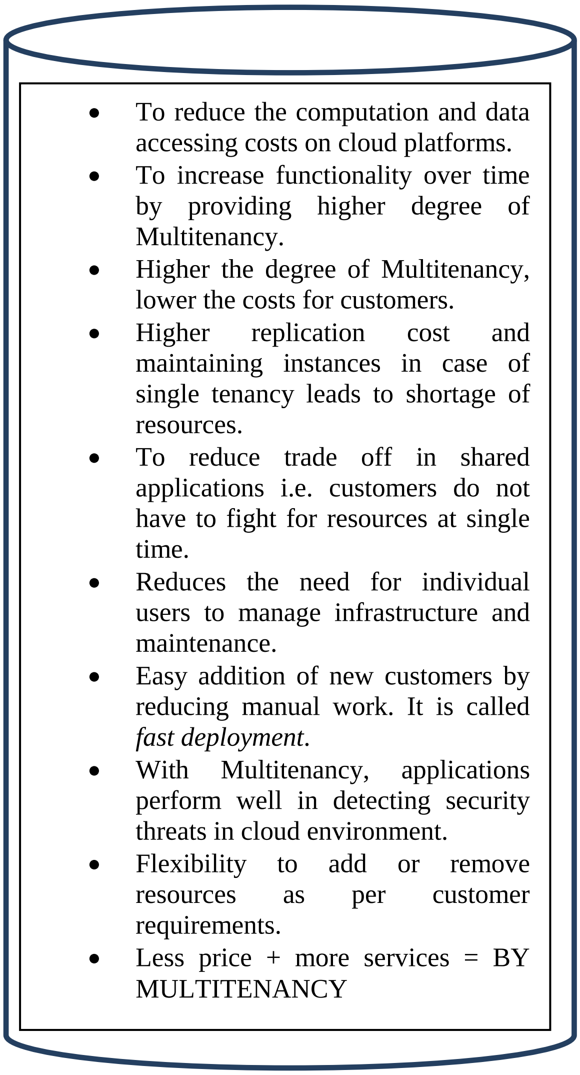
S.No.	Public Cloud	Private Cloud	Hybrid Cloud
1.	Simple and easy to use.	Monitoring is needed to control latest software updates	Most efficient (combination of both)
2.	Widely accessible.	limited accessible	Used to reduce work load.
3.	Less costly and reliable	More costly and less reliable	Most costly and most reliable.
4.	Suitable for handling large workload pressure	Not suitable for large workload pressure	Suitable for handling large workload pressure
5.	No space allocated for data center	Largest space allocated for data center.	Average space allocated for data center

2. INTRODUCTION TO MULTITENANCY

A tenant is defined as any application that requires secure virtual environment whether it is inside cloud or outside the cloud. Multitenancy is the fundamental attribute of both public and private clouds that can be understood as “An application that processes confidential data within private cloud is tantamount to a tenant that publishes catalog information in a public cloud [5]. It is applicable to all three layers of cloud viz. IaaS, PaaS and SaaS. It is commonly seen that virtualization is implemented at IaaS layer. IaaS includes features like service level agreements, identity management, fault tolerance and dynamic procurement in clouds. But, Multitenancy should not be limited to IaaS only; it should go beyond IaaS to other layers. Only then tenants can enjoy the full range of services in cloud from physical to user interface layer.

2.1. Why Multitenancy?

Various factors initiated the need of Multitenancy in the field of cloud computing as follows:



- To reduce the computation and data accessing costs on cloud platforms.
- To increase functionality over time by providing higher degree of Multitenancy.
- Higher the degree of Multitenancy, lower the costs for customers.
- Higher replication cost and maintaining instances in case of single tenancy leads to shortage of resources.
- To reduce trade off in shared applications i.e. customers do not have to fight for resources at single time.
- Reduces the need for individual users to manage infrastructure and maintenance.
- Easy addition of new customers by reducing manual work. It is called *fast deployment*.
- With Multitenancy, applications perform well in detecting security threats in cloud environment.
- Flexibility to add or remove resources as per customer requirements.
- Less price + more services = BY MULTITENANCY

Fig 1: Need of Multitenancy

2.2. Degree of Multitenancy

In Multitenancy, it is said that SaaS vendor offers single version of its software for all its customers. It implies that the degree of Multitenancy is based on how much SaaS layer is being shared across tenants. Higher the degree of multitenancy, lower the costs for customers**.** The highest degree signifies sharing of database,customization of logicsand workflow at different layers of cloud computing. Thus, all the layers of cloud offer multitenancy on basis of their degrees [6].

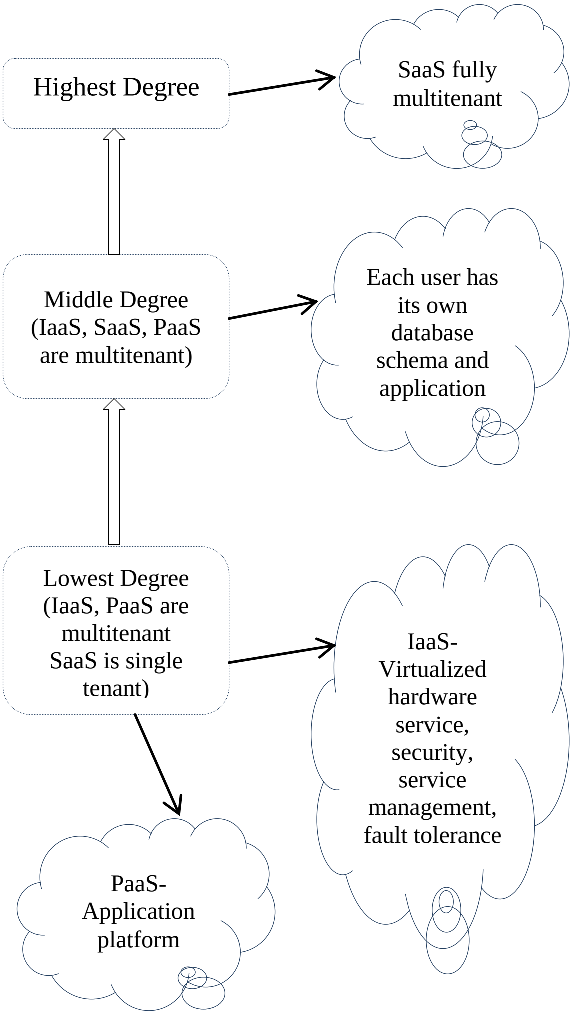

Highest Degree
SaaS fully multitenant
Middle Degree (IaaS, SaaS, PaaS are multitenant)
Each user has its own database schema and application
Lowest Degree (IaaS, PaaS are multitenant SaaS is single tenant)
IaaS- Virtualized hardware service, security, service management, fault tolerance
PaaS- Application platform

Fig 2: Levels of Multitenancy

3. LITERATURE REVIEW

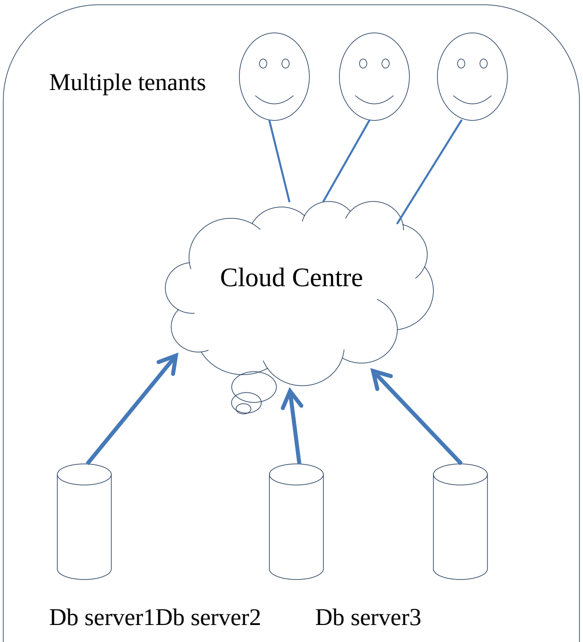
In multitenant cloud computing, management and monitoring of secured data may lead to issues. They include accessing same database by multiple customers that leads to breach of confidentiality and mixed data but still it is ruling in technology era due to its effective utilization of same physical resource at very low cost services. Singh et. Al [7] discussed security issues in cloud and tried to mitigate using RSA encryption and cryptographic algorithm. But it has not applied in SaaS layer of cloud. Issac et al. [8] introduced virtual machine segmentation and virtualization to ensure security in cloud environment. It does not specify about hypervisors. John et. Al [9] discussed security issues in context of healthcare multitenant cloud system. Fox et.al [10] stated that the fundamental security threat is usage of single and same hardware by multiple clients that causes challenges in terms of compliance, security and privacy. Malicious tenants may cause attacks for other tenants sharing resources on same hardware. Zha et.al [11] introduced new attack called Shrew attack which makes any malicious activity as unidentified in network. The tenants are not aware that they are sharing resources with malicious tenants. Walraven et.al [12] described multi tenancy support layer for multiple tenants but it is only for web applications and does not support hypervisors and segmentation. Few more studies are shown in form of table as given below.

Table 2: A Precise Comparative Analysis of Few Research Papers (in ascending order by year

Reference No.	Year	Pros	Cons/Research gaps identified
[11]	2008	Identified new fingerprint attack called Shrew attack	--Its low payload and less time duration makes it unable to detect. --No multi tenancy introduced
[13]	2011	Introduced concept of multi tenancy in cloud	Failed to identify security issues and isolation management in multitenant environment
[12]	2012	Introduced multitenant variable layer	--This model is only suitable for web applications. --No use of hypervisors and segmentation techniques.
[14]	2018	Service level agreements are defined in multi cloud networks	They are not operational in SaaS layer which is considered as basic layer for multi tenancy.
[15]	2019	Removes problem of data de-duplication in cloud	Compression techniques failed in case of multiple users and leads to deadlock.
[16]	2019	Provides secured multitenant design cloud	Does not make use of hypervisors and segmentation
[17]	2019	Qualitative analysis of security challenges is being done	It does not mention multitenant techniques in cloud databases
[18]	2020	Shift transposition algorithm is used to perform shifting in multitenant cloud.	This algorithm counters with segmentation basic nature of creating cluster of customers into similar groups.
[19]	2020	Data encryption approach is used to enhance multi tenancy	It uses AES encryption standard which is very difficult to be compatible with hybrid cloud
[20]	2020	Proposed multitenant model on basis of linguistics	No clearly defined parameters
[21]	2021	Scheduling approaches are defined for multi tenancy	It does not integrate scheduling with security challenges.

4. DATA STORAGE IN MULTITENANCY

It is being described in figures below:

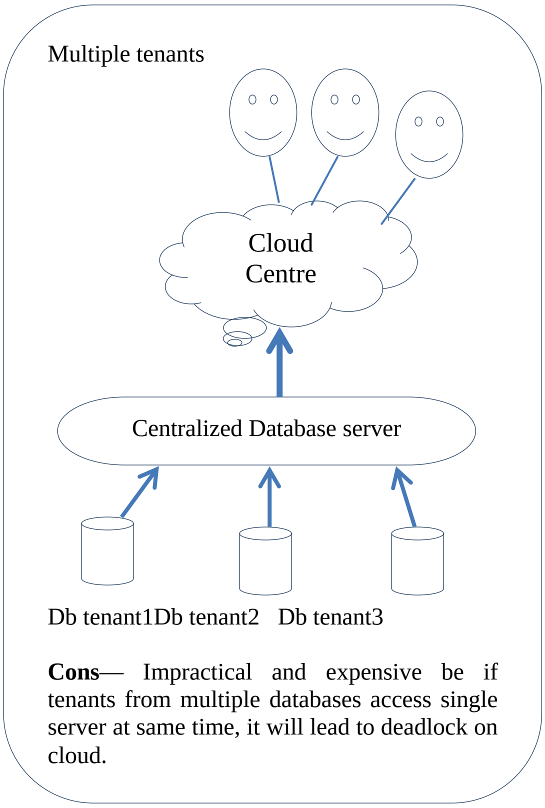


Pros- (a) each tenant has separate database server. (b) Tenant isolation is there, so less chances of threats

Cons—Expensive as it is difficult to maintain multiple servers (here 3 tenants means 3 servers)

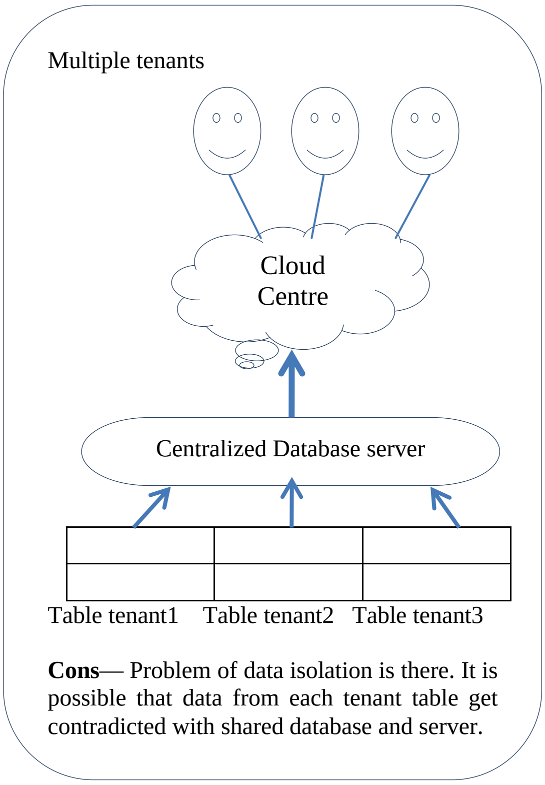
Fig 3: Tenants with Separate databases server

In next case, there is single server with multiple tenants and multiple databases. It is depicted in figure 4.



Cons— Impractical and expensive be if tenants from multiple databases access single server at same time, it will lead to deadlock on cloud.

Fig 4: Multiple tenants with multiple databases but single server


Multiple tenants
Cloud Centre
Centralized Database server
Table tenant1 Table tenant2 Table tenant3

Cons— Problem of data isolation is there. It is possible that data from each tenant table get contradicted with shared database and server.

Fig 5: Separate tables per tenant with central database server

5. PROPOSED SECURED ONTOLOGY BASED MULTI TENANT CLOUD ARCHITECTURE

It is proposed with an intention of securing data along with providing relevant results to tenants.

- The architecture uses concept of hypervisors, virtualization, segmentation and ontology.
- Virtualization involves virtual machines (VM) which are databases, file servers, applications and web services constituting a physical network and perform effective consumer communication over cloud network.
- Virtualization includes optimized software called Hypervisors. They perform management and mapping of traffic from virtual machine to specific portion of cloud so that users can access data through data center.
- But in IaaS layer, the VM's are placed just relative to one another that can increase the risk of unauthorized connections, multiple login attempts and malware attacks.
- So, the proposed model uses hypervisors in SaaS layer also. It is isolated from IaaS so that management is done at IaaS and application of services is done at SaaS.
- Now, it is also possible that tenants may retrieve irrelevant data after accessing cloud data center. This irrelevancy is mitigated by creation of automatic web ontologies [22].
- The database related to specific tenant domain is mapped into ontologies.
- Now, when the user requests for specific resources, the relevant results are presented from ontological databases.
- It is an attempt to maintain security, confidentiality and authenticity of data. It's detailed algorithm and working scenario is the subsequent task of this paper.

6. CONCLUSION & FUTURE SCOPE

The paper revolves around the concept of multitenancy and its need in cloud environment to make it authenticated, secured and free from irrelevancy. It begins from basic cloud deployment models followed by basic definitions of multitenancy. Several studies are being reviewed in context of security issues or risks that are encountered in multitenant cloud environment.A comparative analysis is being shown in ascending order of years. It is followed by existing data accessing approaches with the use of multi tenants either with single database server or separate tenant databases or having separate tables associated with each tenant. Lastly, a concept of automatic creation of ontologies from databases is introduced in proposed architecture. Ontologies are the characteristics of classes, properties and instances of given domain. It maintains hierarchical relationship among concepts used in datasets and removes sense of ambiguity among relations. It leads to relevant results to the tenants.

As future work, the working of proposed architecture and algorithm behind it is discussed in next paper. It is followed by experimental results and comprehensive analysis of the proposed ontology model. The given paper presents only layout of cloud model.

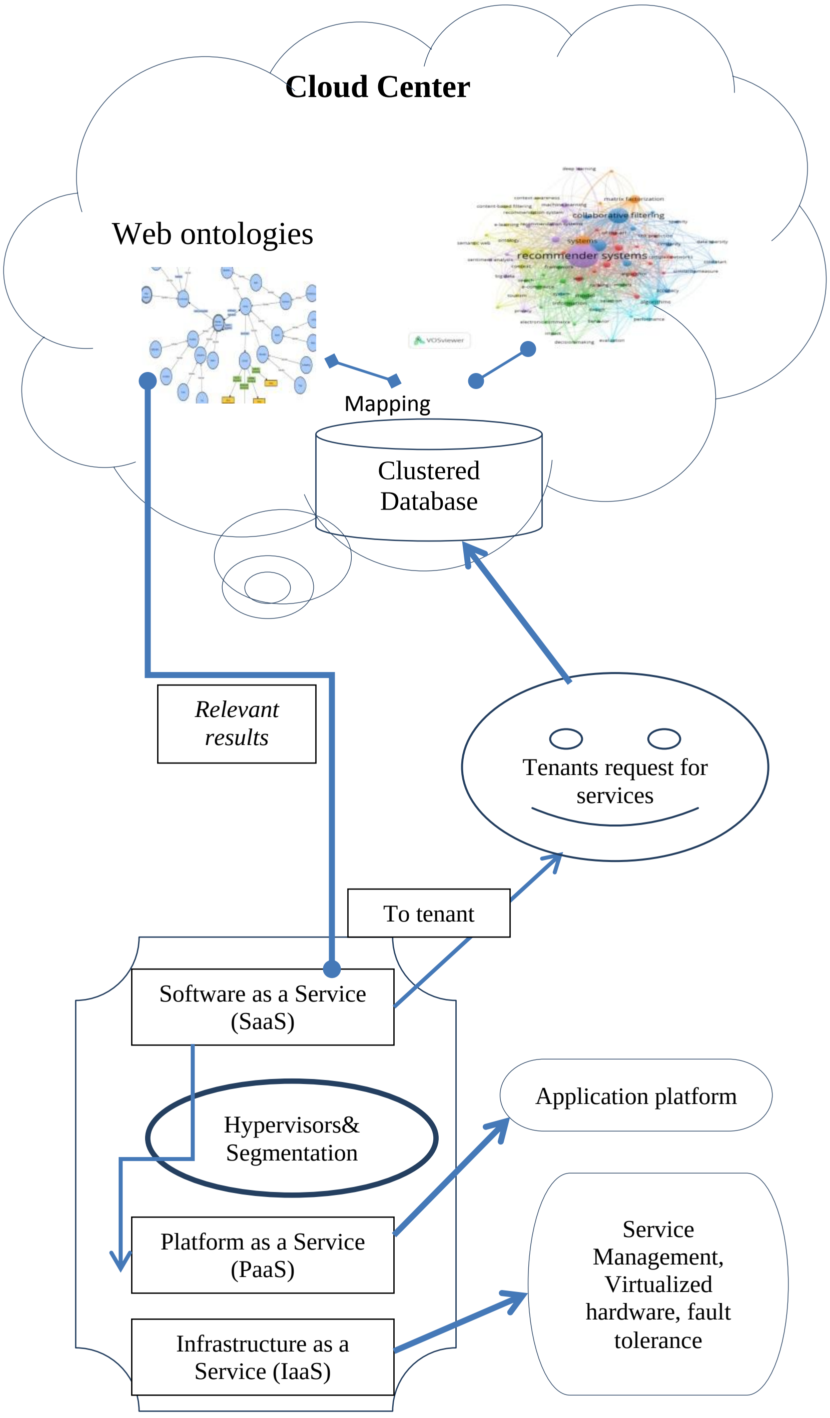

Cloud Center
Web ontologies
Mapping
Clustered Database
Relevant results
Tenants request for services
To tenant
Software as a Service (SaaS)
Hypervisors& Segmentation
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Application platform
Service Management, Virtualized hardware, fault tolerance

Fig 6: Proposed Ontological MultiTenant Cloud Architecture

7. REFERENCES

[1] V Krishna Reddy, Dr. L.S Reddy, “ Security Architecture of Cloud computing”, International Journal of Engineering Science and Technology (IJEST), Vol3 No.9, Sept 2011

[2] Abraham E., Ajakaiye, “The trend and challenges of cloud computing: a literature review”, International Letters of Social and Humanistic Sciences (ILSHS), Vol 5. Pp 13-20, 2014

[3] Gartner, Bart Dhoedt and Piet Demeester, 2012, “Cloud-Based Desktop Services for Thin Clients”, IEEE Computer Society, Nov/December 2012, pp 60-67

[4] CC Kalyan, Lokesh, “Security Techniques for multi tenancy applications in cloud”, IJCSMC, Vol2 Issue 8, 2013, pp 248-251

[5] Mangesh, RoshnaRavindran, “Resolving Multi tenancy issues using cloud automation”, International Journal of Scientific research and Engineering trends (IJSRET), Vol 6, Issue 3, 2020, ISSN 2395-566X

[6] KaushalJani, Bimal Kumar, “Degree of Multi tenancy and its database for cloud computing”, International journal of engineering development and research (IJEDR), 2013, pp 168-171

[7] Manjinder Singh, “Multi tenancy security in cloud computing”, IJESRT, March

[8] IssacOdun, Sanjay Misra, “Cloud multi tenancy issues and developments”, Dec 2017, pp 68-73

[9] John Victor, Monisha Singh, “Security analysis in multi-tenant cloud computing using healthcare system”, IJMET, March 2018

[10] Muhammad Fahad Khan, Fox, “An Approach Towards Customized MultiTenancy”, I.J.Modern Education and Computer Science, 2012, 9, 39-44 Published Online September 2012 in MECS

[11] J. Zha, J. Wang, R. Han, and M. Song, “Research on load balance of service capability interaction management,” in *Proc. 3rd IEEE Int. Conf.Broadband Netw. Multimedia Technol.*, Oct. 2008, pp. 212–217

[12] S. Walraven, E. Truyen, W. Joosen, A middleware layer for flexible and cost-ef-ficient multi-tenant applications, 12th ACM/IFIP/USENIX International Middle-ware Conference, Lisbon, Portugal, December 12.-16., 2012, pp. 370-389

[13] P. A. Bernstein, I. Cseri, N. Dani, N. Ellis, A. Kalhan, G. Kakivaya, D. B. Lomet, R. Manner, L. Novik, and T. Talius. Adapting Microsoft SQL Server for Cloud Computing. In ICDE, pages 1255–1263, 2011

[14] G. Li, J. Wu, J. Li, Z. Zhou and L. Guo, "SLA-Aware Fine-Grained QoS Provisioning for Multi-Tenant Software-Defined Networks," in IEEE Access, vol. 6, pp. 159-170, 2018

[15] Dirk Meister, Andre Brinkmann, Tim S, “File Recipe Compression in data de-duplication Systems” in 11th USENIX Conference on File and Storage Technologies (FAST ’2019)

[16] G B, Pallavi and Jayarekha, Dr P, Secure Multi-tenant Design for Cloud Computing Environment (2019). Proceedings of the Second International Conference on Emerging Trends in Science & Technologies For Engineering Systems (ICETSE-2019

[17] Singh A.: ‘Security concerns and countermeasures in cloud computing: qualitative analysis’, Int. J. Inf. Technol., 2019, 11, pp. 683–690

[18] PK., Pradhan, S.K.: ‘Multi-level authentication-based secure aware data transaction on cloud using cyclic shift transposition algorithm’. Advances in Intelligent Computing and Communication, Singapore, 2020, pp. 384–393

[19] Pawan Kumar, Ashutosh Bhatt, “Enhancing multi tenancy security in the cloud computing using hybrid ECC based data encryption approach”, IET Commun., 2020, Vol. 14 Iss. 18, pp. 3212-3222, ISSN 1751-8628

[20] MN Faruk, G Lakshmi, “Multi tenant endorsements using linguistic model for cloud computing”, Int. J. Advanced Networking and Applications Volume: 11 Issue: 06 Pages: 4486-4493 (2020) ISSN: 0975-0290

[21] Ru, J, Yang, Y, Grundy, J, Keung, J &Hao, L 2021, 'A systematic review of scheduling approaches on multi-tenancy cloud platforms', *Information and Software Technology*, vol. 132, 106478. https://doi.org/10.1016/j.infsof.2020.106478.

[22] U. Yadav, Gagandeep Singh, N. Duhan, V.Jain, “Ontology Engineering and Development Aspects: A Survey”, IJEME, MECS Hong Kong, 2016, 3, 9-19.