International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)

Compliance Frameworks for Multi-Tenant Cloud Architectures

Laxmana Kumar Bhavandla
Independent Researcher, USA

Article Info
Volume 6, Issue 2
Page Number : 591-598

Publication Issue :
March-April-2020

Article History
Accepted : 01 March 2020
Published : 20 March 2020

ABSTRACT

Optimizing the use of resources is made possible by multi-tenant cloud architecture for scalable, cost-effective solutions in any industry. It has however led to massive difficulties including isolation of data, control of access, regulation, and security vulnerabilities. The present report delves into the compliance framework specifically for the multi-tenant cloud systems that synthesize advanced mechanisms from the role-based access control mechanisms, cross-tenant authorization models, and architecturally significant requirements. This proposed framework would leverage ontological models and semantic web technologies to make sure that HIPAA standards were being met. Vulnerabilities within shared environments would be dealt with. Fine-grained trust relationships, policy enforcement mechanisms, and adaptive strategies to manage tenant-specific requirements are key components. The framework is illustrated using case studies on healthcare systems and collaborative cloud services to show scalability and efficacy. This report provides an all-inclusive approach in the design of robust, compliant multi-tenant cloud systems by integrating ASRs such as privacy, security, and scalability to accommodate evolving organizational and regulatory needs.

Keywords : Multi-Tenant Cloud Architecture, Resource Optimization, Cost-Effective Solutions, Data Isolation, Access Control, Regulatory Compliance, Security Vulnerabilities, Compliance Framework, Role-Based Access Control (RBAC).

I. INTRODUCTION

Multi-tenant architecture for a cloud environment is required to optimize resource sharing and scalable in current cloud-based services, but issues in isolation, access controls, and maintaining regulatory compliances such as HIPAA. This research paper deals with a compliance framework that bridges these gaps using advanced features of role-based access control (RBAC), models of cross-tenant authorization and architecturally significant requirements. By using semantic technologies and adaptive trust relationships, the architecture ensures data security, privacy, and scalability. The document provides strategies for building robust multi-tenant cloud systems aligned with evolving regulatory needs through a focus on real-world case studies.

Literature Review

Access Control for Multi-tenancy in Cloud-based Health Information Systems

According to Anwar and Imran, (2015) : Multi-tenancy within cloud-based healthcare information systems brings about various challenging issues about the privacy and security of Personal Health Information. Anwar and Imran proposed an ontological framework in 2015 for the enforcement of HIPAA compliant access control policies based on the objective of protecting PHI against illegal access within multi-tenant environments of cloud (Anwar, et al., 2015). This model is using Role-Based Access Control, which incorporates semantic web rule language with representations of policies as rules read by machines. The integration of healthcare workflows with multi-tenancy models provides an answer to key vulnerabilities, such as cross-tenant data breaches.

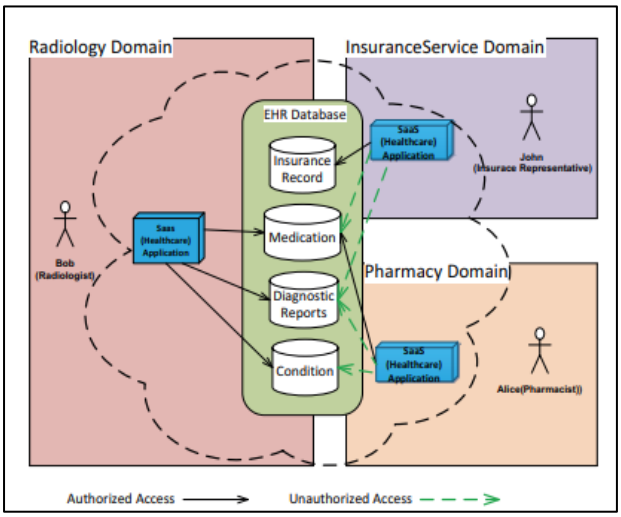

Figure 1: Multi Tenancy Use Case In healthcare organization

(Source : Self Created)

The implementation of this framework on OpenStack's Keystone module showcases the feasibility of enforcible access control policies that could enforce resource isolation and guarantee adherence to HIPAA administrative and technical safeguards. Keystone, by its identity service, makes role-based authorization possible, segregating tenant-specific resources to reduce risks associated with shared infrastructures.

The strengths notwithstanding, the study outlines the challenges faced with the adaptation of the ontological models towards constantly evolving compliance requirements in dynamic cloud environments. An approach shows promise towards automatically enforcing compliance and thus achieving improved security, yet scalable to accommodate the diversity of health workflows and large-scale interactions involving tenants. Future work includes developing more adaptive and scalable ontological models and also taking the framework further to ensure compliance monitoring in real-time and enhanced security and trust with multi-tenant architectures in clouds.

Multi-tenancy authorization models for collaborative cloud services

According to Tang, Sandhu and Li, (2015) : The issue of collaborative access control complexity in multi-tenant cloud services is tackled by MTAS, the framework proposed by Tang et al. (2015), which enhances the traditional role-based access control mechanism to include fine-grained trust mechanisms that provide secure cross-tenant interaction (Tang, et al., 2015). MTAS introduces public roles, truster-centric, and relation-centric, thereby minimizing exposure to sensitive information while providing tenants with means to collaborate without jeopardizing data security.

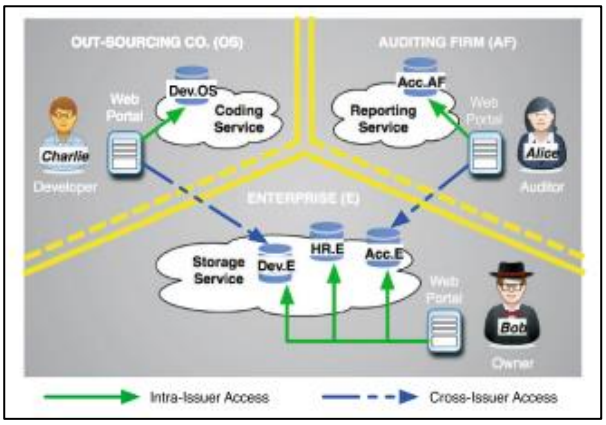

Figure 2 : Out Sourcing Case of Multi-tenant Accesses

(Source : Self Created)

The MTAS framework supports central management of policy but maintains flexibility for decentral interactions of tenants. By using trust relations, tenants may selectively provide access permissions, thus creating hierarchical role mappings and ensuring that a resource is shared in a secured and controlled manner. For example, the trustor may expose certain roles to the trustee while keeping access to other more sensitive assets. This alleviates semantic mismatches and promotes easier cross-tenant interaction.

Experimental evaluations of MTAS, for instance, with XACML showed that it is scalable and latency low because its average policy decision overhead was 12 milliseconds. Such results reveal the applicability of MTAS for real-world cloud deployments. Still, the study confesses that universal standards of cross-tenant authorization and decentralized authority can be tough to achieve. Two areas for future development in ensuring that the collaborative framework for multi-tenant systems is more robust are interoperability and scalability in a dynamically heterogeneous cloud environment.

Architecturally Significant Requirements Identification, Classification and Change Management for Multi-tenant Cloud-based Systems

According to Chauhan and Probst, (2017) : Authors note ASRs as one of the determining factors of design and operation for the multi-tenant cloud system, where some of the major ASRs include scalability, security, privacy, and interoperability (Chauhan, et al., 2017). each one vital in providing the necessary requirements in the aspect of system reliability and tenant satisfaction. Scalability will refer to the use of predictive resource allocations and autonomous provisioning that ensure handling of dynamic workloads in multi-tenant clouds while emphasizing the robust use of RBAC and encryption mechanisms.

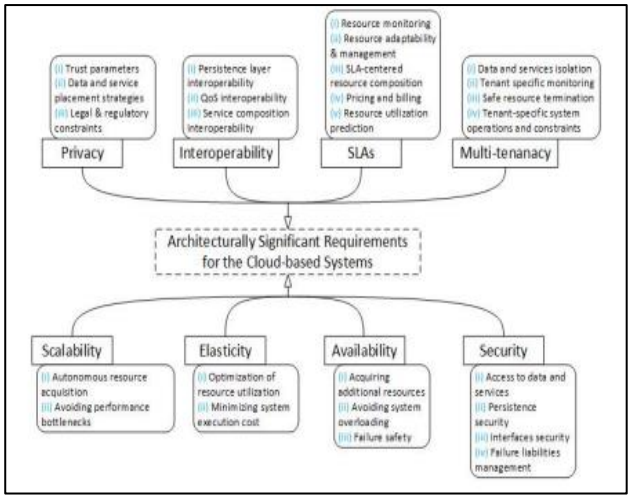

Figure 3 : Overview of Architectural Signnificant Requirement (ASRs)
(Source : Self Created)

Privacy requirements ensure that the legal and regulatory framework is tenant-specific, covering data localization and usage constraints. The requirements also address privacy-preserving protocols for the integration of protocols to reduce risks of data breaches and unauthorized access (Madi, et al., 2018).Interoperability allows tenants to work across the layers of clouds, IaaS, PaaS, and SaaS, without degrading system performance or security and with resources and services being accessible.

This framework analyzes how changes occur throughout the lifecycle of a system so as to address the variance of tenant requirements. It hence allows for the identification of trade-offs between conflicting ASRs like scalability and privacy, thus guaranteeing balanced architectural decisions. This implies architects can keep their systems well-adaptable to a change in the demands of environments that are multi-tenanted, hence sustaining growth coupled with adherence to a variety of stakeholder demands.

Framework Design Considerations

But what would be the case while building a compliance framework that focuses in relation to multi-tenancy architectures is, quite indeed, multiple issues pertaining to securing and scaling it to levels highly achievable and maintaining full compliance

within what is required as set through dictation by regulations in total.

Key Elements of a Compliance Framework

Administrative, technical, and physical means of an infrastructure would give multi-tenant cloud the needed compliance (Matthew, et al., 2016). Administration refers to policies to access and controls definition. Such practices in terms of monitoring role assignment protect data, at both at rest and while moving using technical approaches that apply such forms as encryption protocols secure APIs. Physically, means safeguards protecting such physical aspects that guard infrastructure from unwanted or unpermitted entry.

Addressing Multi-Tenancy Requirements

Multi-tenancy presents a challenge since resources are shared; thus, the framework needs to isolate tenant data from cross-tenant vulnerabilities. Good models for access management include Role-Based Access Control that is widely accepted and in use (Hossain, et al., 2015). The advanced versions that rely on ontologies or based on trust mechanisms will be capable of offering fine granularity in access and flexibility in a collaborative environment. For example, SWRL can be used to define rules and access control by validation that can be set with HIPAA compliance.

Regulatory Compliance

Global multi-tenant systems fall under several regulations, such as GDPR, HIPAA, and PCI-DSS. The compliance framework is therefore bound to comply with all those requirements in protecting sensitive information. For example, in HIPAA, health care data is required to have technical components for safeguarding, including encryption, role-based access control, and audit trails. The same will be the requirement for protection of data, consent, and notification in case of a breach as per GDPR.

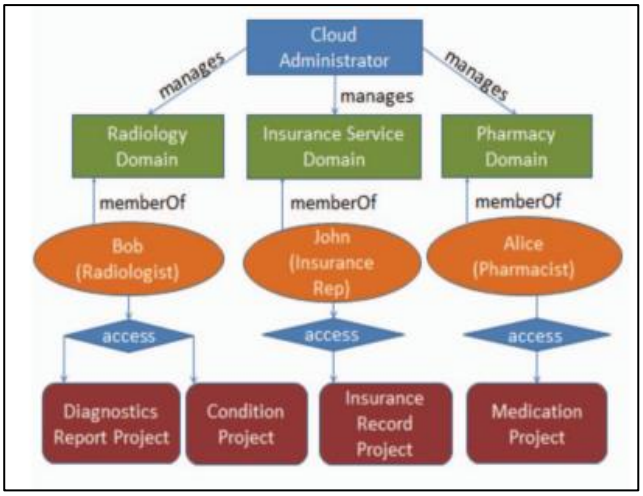

Figure 4 : Tenant And Resources Representation

(Source : Self Created)

Scalability and Adaptability

Scalability: It must ensure scalability in terms of dynamic tenant demand. The framework should be able to adapt to changing demands without losing its focus on security and compliance (Baldin, et al., 2018). In this direction, automation-or rather AI-powered monitoring-will enhance the scalability as it will do real-time anomaly detection and enforce policies accordingly. The same is the requirement for being able to integrate with more than one cloud environment while adapting the framework in a hybrid or multi-cloud environment.

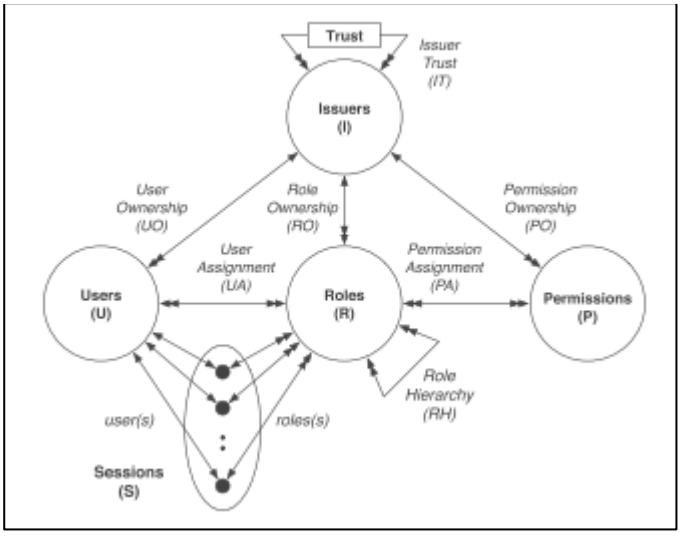

Figure 5: Abstract Model Of the MTAS System

(Source : Self Created)

Integration of Emerging Technologies

The inclusion of technologies like blockchain, machine learning, and advanced analytics can help strengthen the compliance (Ngo, et al., 2016). With blockchain, the access logs shall be made to ensure transparency and integrity due to the capabilities of the detection of threats with machine learning models that analyze user behavior. This increases the security of any organizational setting while simplifying how to manage compliance through action information.

Implementation Challenges and Mitigation

It will introduce multi-tenant cloud architecture-specific challenges: ensuring compliance with security standards, efficiency, and adherence to regulation. Data isolation, access control, monitoring for compliance, scalability, and tenant customization are such challenges.

Data Isolation

Shared infrastructure with multi-tenancy always introduces risks of unauthorized data access and breaches between tenants. Segregation of data is ensured if strong mechanisms are in place: fine-grained access-control policies, role-based access control, etc. Data segregation without compromising performance as well as scalability is highly challenging.

Mitigation:

Some other complex RBAC models, even those extended by ontological or trust-based approaches, will enforce access policies. Also, using containerization and VPN for logical isolation of data increases the protection given to such information.

Dynamic Access Control Management

In multi-tenant scenarios, tenants have often different access requirements that change over time, and hence managing access control policies in such cases is complex, thus implying a higher probability of misconfigurations or privilege escalations.

Mitigation:

Automating updates of policies by using Semantic Web Rule Language and other technologies, for example, will make sure that all standards like GDPR and HIPAA are followed. Centralized access control management tools integrated with monitoring systems will enforce and audit dynamically changing access policies.

Scalability Issues

As the number of tenants and workloads increases, the framework must scale without losing performance. It is a big challenge to ensure scalability while keeping the compliance in place.

Mitigation:

Integration of AI-driven monitoring and anomaly detection can be able to help manage scalability since it automates compliance checks and identifies problems in real-time.

Compliance Monitoring and Reporting

Continuous monitoring and compliance report violation reports must be carried out meeting regulatory requirements like HIPAA or PCI-DSS, which will be in-efficient and full of mistakes, if one is done by manual method.

Mitigation:

The use of automated compliance tools that are integrated with both audit logs and reporting systems will make it easier to process. Blockchain technology will give immutable records of compliance activities for more transparency (Maenhaut, et al., 2015). The organizations would ensure that the multi-tenant cloud architectures are both secure, scalable, and meet the necessary regulatory compliance through the handling of these mitigations about the highlighted issues.

Case Studies and Examples

Through different case studies in various domains, the research has explored several applications and practical solutions on the part of compliance frameworks in the multi-tenant cloud architecture.

Healthcare Cloud: HIPAA Compliance

Anwar and Imran (2015) did a study where a cloud healthcare system was developed incorporating OpenStack to abide HIPAA rules. The system applied to this study used RBAC with the ontology

enhancement to establish safe and compliant access to PHI while allowing various departments in their health care to be on the same database as different tenants. Implementation ensured cross-tenant data breaches protection through access control policies in place by using Semantic Web Rule Language and verified by OWL-DL reasoner.

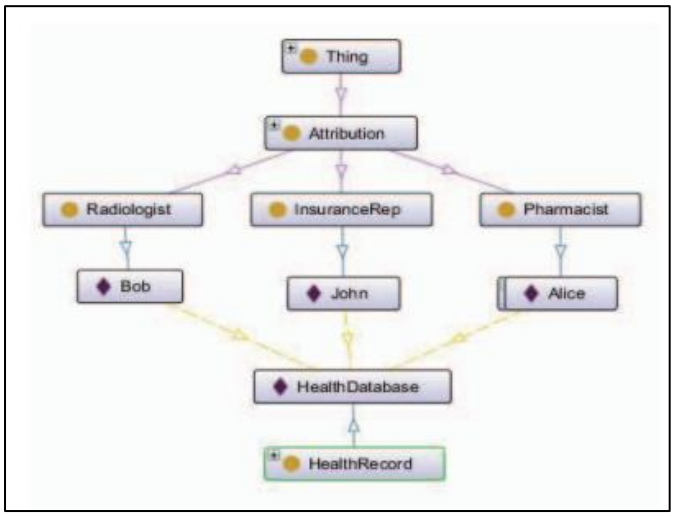

Figure 6 : An Ontological Representation

(Source : Self Created)

This example presents the use of a well-crafted compliance framework in achieving certain regulatory compliance requirements in a multi-tenant environment.

Multi-Tenant Collaborative Cloud Services

Tang et al. in 2015 demonstrated an MTAS that supports cross-tenant collaborations. In fact, extending RBAC with trust-based models would support a system that allows for safe sharing of resources between tenants while also providing fine-grained control over permissions. It was tested on a prototype private cloud, and it received very low latency for policy decisions, averaging at 12ms (Madi, et al., 2016). This case study reveals how adaptive trust mechanisms might enable secure collaborations within multi-tenant cloud environments and therefore balance flexibility with compliance.

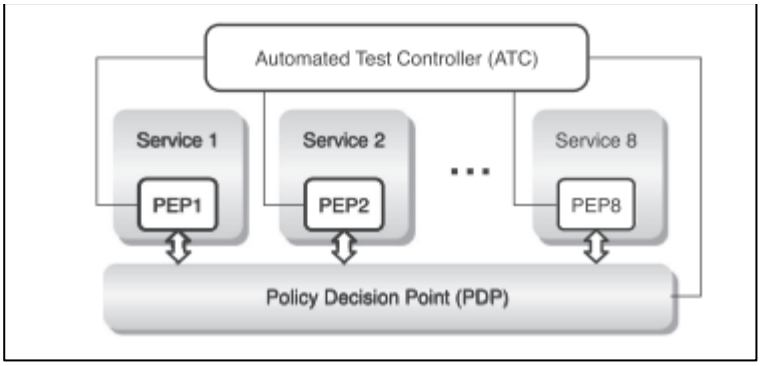

Figure 7: MTAS Testbed Architecture

(Source : Self Created)

Architecturally Significant Requirements Management

Chauhan and Probst (2017) outlined an approach to the management of Architecturally Significant Requirements in multi-tenant clouds using a framework. For the case study focused on achieving tenant-specific scalability, security, and privacy (Ioannidis, 2018). it demonstrates the need to have tenant-specific customization yet also reap the benefits of shared infrastructure; introduction of trade-off points into the architecture managed change with tenant-specific changes concerning system performance and adherence to regulations.

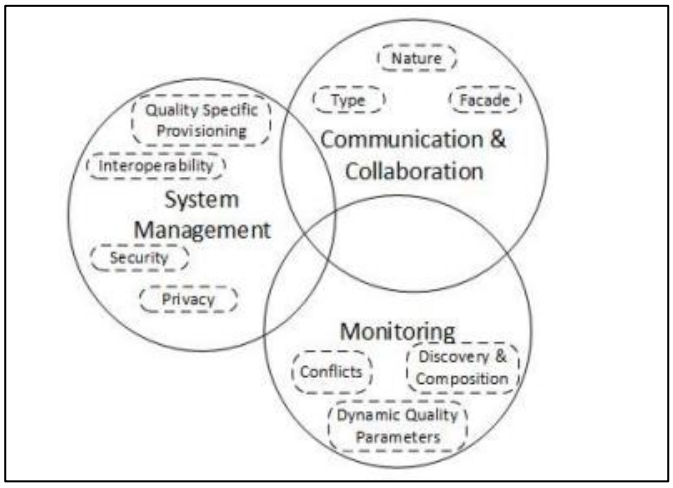

Figure 8: Key Classification For Cloud Based Systems

(Source : Self Created)

Future Directions

Future in the compliance framework of multi-tenant cloud architectures is to integrate technologies advanced and to resolve novel issues arising in

scalability, security, and regulatory compliance. Of prime innovation areas are as follows:

Advanced Role-Based Access Control (RBAC)

In comparison, enriched RBAC models which could use ontologies and include mechanisms based on trust might ensure the creation of dynamic access controls which are granular as well. It might leverage future frameworks where access predictions based on evolving algorithms will lead to the policy automatic revision.

Blockchain for Transparent Compliance

Blockchain technology provides immutable, transparent audit logs for tracing the access of data and also the compliance activities. Thus, this could potentially bring in more trust, increase simplicity in regulatory reporting for such industries as healthcare and finance.

Multi-Tenant Collaboration Models

Frameworks need to evolve to allow secure cross-tenant collaboration. Techniques such as MTAS with finer grain trust models can be used to make seamless sharing of resources feasible while ensuring compliance and security.

Tenant-Specific Customization and Scalability

Future architectures must balance tenant-specific needs with shared infrastructure. Architectures based on trade-offs and variability management can optimize scalability along with addressing diverse tenant requirements (Demchenko, et al., 2017). This will make an adaptive, scalable, and robust compliance framework that leads to achieving security as well as regulatory compliance in even more complicated multi-tenant cloud systems.

Conclusion

Ensuring data security, compliance, and operational efficiency through frameworks for multi-tenant cloud architectures is a pressing matter. The studies examined represent effective approaches to include a HIPAA-compliant ontology-based RBAC model, trust-based multi-tenancy authorization systems, and Architecturally Significant Requirements management frameworks. Advanced technologies including AI, blockchain, and automation are also implemented for the resolution of important issues in relation to data isolation, dynamic access control, and scalability. Future frameworks need to stress adaptive designs, transparent mechanisms of compliance, and customization based on tenant-specific requirements in order to meet emerging demands. Multi-tenant cloud systems, by applying these strategies, can enhance security, scalability, and compliance in complex, dynamic environments.

II. REFERENCES

[1]. Anwar, M. and Imran, A., 2015, November. Access control for multi-tenancy in cloud-based health information systems. In 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (pp. 104-110). IEEE.

[2]. Baldin, I., Ruth, P., Wang, C. and Chase, J.S., 2018, October. The future of multi-clouds: A survey of essential architectural elements. In 2018 international scientific and technical conference modern computer network technologies (MoNeTeC) (pp. 1-13). IEEE.

[3]. Chauhan, M.A. and Probst, C.W., 2017. Architecturally significant requirements identification, classification and change management for multi-tenant cloud-based systems. Requirements Engineering for Service and Cloud Computing, pp.181-205.

[4]. Demchenko, Y., Turkmen, F., Slawik, M. and De Laat, C., 2017, May. Defining intercloud security framework and architecture components for multi-cloud data intensive applications. In 2017 17th IEEE/ACM international symposium on cluster, cloud and grid computing (CCGRID) (pp. 945-952). IEEE.

[5]. Hossain, A. and Shirazi, F., 2015. Cloud Computing: A Multi-tenant Case Study. In Human-Computer Interaction: Users and Contexts: 17th International Conference, HCI

International 2015, Los Angeles, CA, USA, August 2-7, 2015, Proceedings, Part III 17 (pp. 178-189). Springer International Publishing.

[6]. Ioannidis, G., 2018. Adding flexibility to multi-tenant networks (No. 8243). EPFL.

[7]. Madi, T., 2018. Security Auditing and Multi-Tenancy Threat Evaluation in Public Cloud Infrastructures (Doctoral dissertation, Concordia University).

[8]. Madi, T., Majumdar, S., Wang, Y., Jarraya, Y., Pourzandi, M. and Wang, L., 2016, March. Auditing security compliance of the virtualized infrastructure in the cloud: Application to OpenStack. In Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy (pp. 195-206).

[9]. Maenhaut, P.J., Moens, H., Ongenae, V. and De Turck, F., 2015, May. Design and evaluation of a hierarchical multi-tenant data management framework for cloud applications. In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM) (pp. 1208-1213). IEEE.

[10]. Matthew, O.O., 2016. Establishing a standard scientific guideline for the evaluation and adoption of multi-tenant database.

[11]. Ngo, C., Demchenko, Y. and de Laat, C., 2016. Multi-tenant attribute-based access control for cloud infrastructure services. Journal of information security and applications, 27, pp.65-84.

[12]. Tang, B., Sandhu, R. and Li, Q., 2015. Multi-tenancy authorization models for collaborative cloud services. Concurrency and Computation: Practice and Experience, 27(11), pp.2851-2868.