ICIC Express Letters
Volume **15**, Number **1**, January **2021**

 ISSN 1881-803X
pp. 1–8

AUTHORIZING SAAS CLOUD SERVICES IN MULTI-TENANCY ENVIRONMENT

Tanveer Ahmad[1], Rajiv Pandey[1] and Suhel Ahmad Khan[2]

[1]Department of Computer Science
Amity University
Malhaur Railway Station Road, Gomti Nagar, Lucknow, Uttar Pradesh 226010, India
ahmadtanveer80@gmail.com

[2]Department of Computer Science
Indira Gandhi National Tribal University
Lal Pur, Amarkantak, Madhya Pradesh 484886, India

Received April 2020; accepted July 2020

Abstract. *An easy, scalable, on-demand, a dynamic access of application and services over the cloud are most influencing features of cloud computing. The valuable IT resources at the enterprise level are adopted by a variety of firms on an assortment of needs including cloud services 'Infrastructure as a Services' (IAAS), 'Platform as a Services' (PAAS), or 'Software as a Services' (SAAS). The sharing of the environment with other consumers is called multi-tenancy. The nature of the public cloud is multi-tenant. Performance evaluation, data latency, and authorization are significant issues related to the cloud provider at the time of supplying services to vendors. The main focus on study is to analyze the best practices over secure cloud environment in authorization perspective. A conceptual authorization model is being presented in this paper to help secure cloud services especially software as a service in a multi-tenant cloud environment.*
Keywords: Cloud computing, Authentication, Authorization, Access management system, Multi-tenancy, Cloud security

1. **Introduction.** The National Institute of Standard and Technology (NIST) describes cloud computing as a platform used for accessing computing resources like servers, physical storage, network, hosted applications and services which are shareable and configurable. The computing resources will be accessed over the network on demand. It can be rapidly provisioned and released with minimal management effort or services. In cloud there are two players: cloud providers and cloud consumers. Cloud providers arrange and manage the services. To save operational cost, cloud provider imitates multi-tenancy concept especially in Software as a Services (SAAS) computing model. Therefore, multi-tenancy environment must have highest concern of unauthorized access of cloud services by the other tenants.

Therefore, the researchers and cloud providers must pay attention to it as much as they could, if they fail in doing so then it will result in losing business and trust in adapting cloud models in their day to day IT operations. So authorization should always be through as our highest concerning area in case of multi-tenant environment. Authentication ensures the authenticity of the user and authorization ensures the permission boundary of the end user. Authorization is a tool to check the utilization limit of the user on the system inside the guardrail [1]. The used mechanism in concert with authorization is a component of an access policy. Access control is a security technique that can be used to formulate who are authorized to use cloud services in cloud computing model. The authorization

DOI: 10.24507/icicel.15.01.1

techniques presently exist in multi-tenant environments are governed by Policy Base Access Control system (PBAC), Role Base Access Control (RBAC); Attribute Base Access Control (ABAC); and user & password base mechanism. Few researchers like Priya et al. presented trust based authorization model while going through different access control models like RBAC, ABAC, DAC, ABE, MAC, their characteristics [2].

To save operational costs cloud provider imitates multi-tenancy concept, especially in the SAAS cloud computing model. Multi-tenant environment generally takes care of security. However, researchers found few lapses while securing services in the cloud from authorization perspective.

This article describes an authorization model which will secure SAAS services. The proposed model adapted the universal concept of access management system that comprises three components, namely Policy Enforcement Point (PEP), Policy Decision Point (PDP) and Policy Information bridge Point (PIP). This paper is categorized as follows. Section 2 describes about delivery model. Section 3 describes about related work on cloud related to authorization. The proposed authorization model is described in Section 4. Section 5 describes the authorization system architecture. Section 6 focuses on conclusion and future work.

2. **Cloud Computing Model.**

The whole cloud computing is divided into two categories, the first is the deployment model (Public cloud, Private cloud, Hybrid cloud) and the second is the services delivery model (IAAS, PAAS and SAAS). This section describes about the deployment model, introduction of the cloud provider and their services, example of the delivery model and talks on security concern associated with the delivery models.

2.1. **Public cloud.**

Organizations owning cloud services provide IT infrastructure platform to general public and other organizations in exchange of monetary remuneration using public cloud [3]. Examples of public cloud providers are Amazon web services, Google app engine, Microsoft azure, etc. Due to provisioning, shared infrastructure, remote hosting, public cloud becomes a temptation for a company. Pay as you go model is also an eye-catching element of the public cloud. The town hall meeting that was conducted by president Obama in 2009 is one of the examples of public cloud. Most of the management task is unladed by public cloud from the client organization to the third-party cloud service vendor. There are multiple points identified in 2018 at which researchers need to concentrate on security aspects [4]. For example, 1) Not enterprise-ready – Among cloud services, 95 percent that are used in the market, lack security strength and enterprise-readiness. By using unsecured application knowingly or unknowingly, corporate sensitive data is getting exposed. 2) Data breach – New General Data Protection Regulation (GDPR) introduced in 2018 by the European Union. Organizations whose services are not complying with GDPR law, risk $4 million fine. Only 5% of enterprise cloud applications are GDPR-ready. Researchers/developer have to rewrite GDPR compliance services. 3) Weak authentication and identity management – Often organizations are oblivious towards the identity management which leads data breaches within organizations. The Anthem Inc. did not opt for multifactor authentication, which inturn breached the data that allowed hackers to retrieve medical and personal profile of eighty million customers. 4) DDoS – Researchers need to develop more strategy to mitigate DDoS attack risk.

2.2. **Private cloud.**

NIST remarks that if a cloud infrastructure is operated or managed by an organization, for it or a third-party functioning from within or outside the organization, then it is termed as private cloud [5]. In private cloud the tailored services are deployed at organization level so that data and accessibility are only for internal user. There is a high security firewall associated with infrastructure of private cloud because

no other organization will get access to the data without the permission of the service provider. The cloud infrastructure includes customers, vendors, business partners, intranet users, corporate offices and all other parties involved in the business. The table shown below depicts about private cloud provider and its services.

Table 1. Private cloud example

Cloud provider	Offered services
HPE	• Helien cloud suite software
VMWARE	• vRealize suite cloud management platform
Microsoft	• Hyper-V virtualization
	• Microsoft windows servers with many features of cloud
	• Microsoft Azure stack
AWS	• Virtual Private Cloud (VPC), cloud storage
Dell	• VPC, cloud management & security software, cloud computing services
Oracle	• Managed cloud services

Similar to above tables, CISCO, NetAPP, RedHat provides private cloud in a very cost-effective way. The existing system of the State Bank of India is based on private cloud on top of VMware with the name Maghadoot. Threat and security concern may be possible like inside the organization may be risk of compromise through a host attack vector explaining local applications such as browsers or document viewers. Security challenges on private cloud may be faced 1) at the time of scalability and consistency, 2) during patch management, 3) during in appropriate configuration, 4) un-patch of hypervisor, 5) keeping simple or default password, and 6) insecure API.

2.3. **Hybrid cloud.** The combination of private and public cloud is termed as hybrid cloud. This combination together behaves as single entity. Bonding between these entities is based on remarkable technologies that make portability of application and its data hassle free. Good part of hybrid cloud is that some hybrid deployment is required during spike in demand and this can be achieved by CLOUD BURST concept. A cloud burst generally happens when an application is deployed dynamically into the internal infrastructure of the firm. Cloud burst dynamic deployment also happens when the demand spike occurs [6]. Hybrid cloud data centers are available at both on premises and on public cloud and it manages the load by application delivery controller (Load balancer). Security of hybrid cloud can be compromised in the cases [7] like 1) lack of encryption, 2) inadequate security risk assessment, 3) poor compliance and weak security management, 4) failure to authenticate, 5) poor IP protection, 6) badly constructed cross platform tools and 7) malicious employee.

3. **Related Work.** The related work on multi-tenancy and authorization model has been described in this section. Kanade and Manza have surveyed the state-of-the-art multi-tenancy in cloud, and they explained the concept and architectural design of multi-tenancy. In multi-tenancy the tenants who are sharing the resources do not have right to modify the application configuration and data [8]. In this paper researchers provided a model by which application configuration can manage outside the application as per tenant tradeoff agreement, so that cloud services can be secure.

Chandra et al. focused on authorization to cloud security via identity management mechanism that provides directory services for application access management [9]. Chandra et al. used custom authorization considering different filters like exception, action and result. To apply the said filters they are trying to access applicationSettings, ADGroupConfig, PharmaBrossardAuthentication Attribute and ADGroupRetrieval. In addition

to above research we are focusing on the agreement policy between cloud consumer and providers in the multi-tenant environment.

Okamoto highlighted the drawback of advanced intrusion detection techniques means denial of the services, and presented an immunity enhancing module [10] to secure cloud services from cyber attack. On the top of immunity enhancing module researcher presented authorization model can be implemented to protect shared resources in multi-tenant environment.

Zhang et al. presented session on key based authorization model which is shared between the users of cloud services for elastic applications in cloud computing [11]. Zhang et al.'s mechanism also supported secure migration of weblets between device and cloud. One of their design goals is to give minimum security considerations to users and application developers. This paper has taken the session management concept and the configuration presented by Zhang et al.

AWS Amazon web services cloud providers present multi-tenancy through AWS Lambda, and AWS Lambda uses lambda authorizers. Bearer token authentication such as SAML or Oath authentication is used by Lambda authorizers. It receives caller's identity in token called token authorizers. Request authorizers receive the caller identity as a JSON which contains stage variables, headers, context variables and query string [12].

Azure Microsoft presents authorization system based on Azure AD, and Azure Active Directory (Azure AD) is Microsoft's cloud based identity and Access Management Service (ACS), which helps your cloud consumer sign in and access resources [13]. The ACS solves time consuming problems, such as: redirect unauthenticated requests, validate it, parsing incoming token, auth check implementation, tokens transformation based on claims types and values. Author presented an authorization model which provides authorization for the resources who do not belong to AD.

Zou et al. presented a fine-grained multi-tenant permission management framework [14]. This framework is addressing security issues on Software Defined Network (SDN) controller. To further enhance the security of cloud services API in multi-tenant environment, we propose an authorization model of permission based on Policy Database.

4. **Proposed Authorization Model.**

This section explains an authorization model that will control unauthorized access of resources belonging to different tenant residing in multi-tenant cloud environment. Multi-tenancy is the co residency of different tenants in the same logical and/or physical medium. In the cloud paradigm, the database, storage, memory, computing, physical access, logical access and other resources are shared among multiple tenants. Privacy of tenants is getting breached through resource sharing. Tenant data should maintain levels of isolation to ensure multi-tenancy with security. The access control systems presently existing are Attribute Base Access Control (ABAC), Policy Base Access Control system (PBAC) and Role Base Access Control (RBAC) user and password based [15]. No doubt RBAC, ABAC, PBAC and user/password authorization models are working successfully under individual system but, in case of multi-tenancy above said model is lacking to complete the authorization demand.

The proposed model explains the sharing of resources and how it can be protected by unauthorized access in multi-tenant environment. Let us assume a cloud provider (C1) which hosting environment contains software services related to retail sector. In this model service SwT1 is a tenant and that provides Employee Management System (EMS), similarly SwT2 provides Supply Management System (SMS), SwT3 provides Customer Management System (CMS) and SwT4 provides Shareholder Management System (ShrMS). Table 2 depicts the resources from respective services.

Till now, the setup of cloud environment for multi-tenant environment in SAAS paradigm has been explained above. The following section will explain about the tradeoff between retail sector management treated as cloud consumer, cloud provider (C1) and

TABLE 2. Resource table

Tenants	Services	Resources	Acronym of resources
SwT1	EMS	Pay slip info, Personal info, Assignment related info	T1R1, T1R2, T1R3, etc.
SwT2	SMS	Stock related info, Import/Export info, Supply related info, Transaction related info	T2R1, T2R2, T2R3, T2R4
SwT3	CMS	Customer profile, Purchase related info	T3R1, T3R2
SwT4	ShrMS	Business reports	T4R1

how our proposed model will secure shared resources of different tenants hosted on cloud C1 from unauthorized access. Once business deal is finalized the cloud consumer (Retail management) will be provided as an interface to make selection of associated resource as per business deal. The chosen information will be saved to a database called as POLICYINFODB. Figure 1 and Table 3 together depict the user interface and database of the proposed system. There are two components shown in Figure 1: one is high-level hosting environment and the other is the admin page for cloud consumer. Cloud consumer can easily manage the shared resource like T1R1, T3R3, and T4R1 for their tenant at application level.

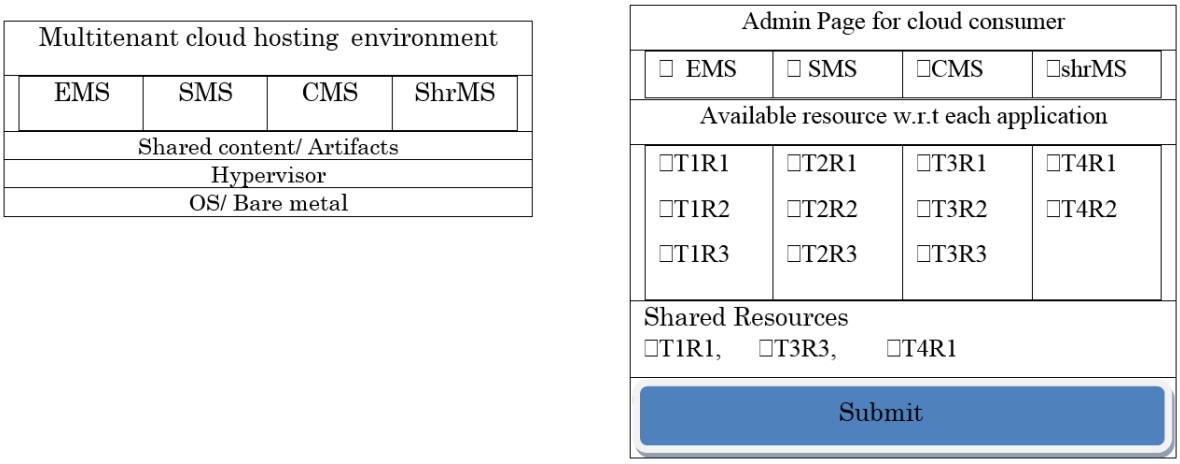

FIGURE 1. Cloud consumer admin page

Any resource selection request must be validated and authorized at two levels tenant's admin and cloud provider admin. Validated and authorized information will be stored in POLICYINFODB. Tabular view of policy POLICYINFODB is given below.

TABLE 3. POLICYINFODB

End user	Tenant	Services	Recourse	Permission
U1T1	SwT1	EMS	T1R1	Allow
U1T3	SwT3	CMS	T3R3	Deny
U2T4	SwT4	ShrMS	T4R1	Allow

Case study: Author's proposed model is based on the case study of retail sector BigBazar. There are multiple stakeholders in BigBazar like billing person, inventory managers, and delivery boys. To manage stake holders, it needs multiple software services. To buy this software BigBazar reached to cloud providers who have offered services in multi-tenant base.

5. **System Architecture.** The system architecture of this model consists of hardware and software architectures.

5.1. **Hardware architecture.** The hardware architecture of the proposed model contains guest operating system layer, hypervisor layer and then multiple VMS which contains all the different types of applications.

5.2. **Software architecture.** Software architecture is based on the universal concept of access management system. Universal concept is based on three components: Policy Information bridge Point (PIP), Policy Decision Point (PDP), Policy Enforcement Point (PEP) [16]. In addition to PIP, PEP and PDP, there are other components which play a major role for authorizing a request. The workflow of end user resource request has been explained in Figure 2 and Figure 3.

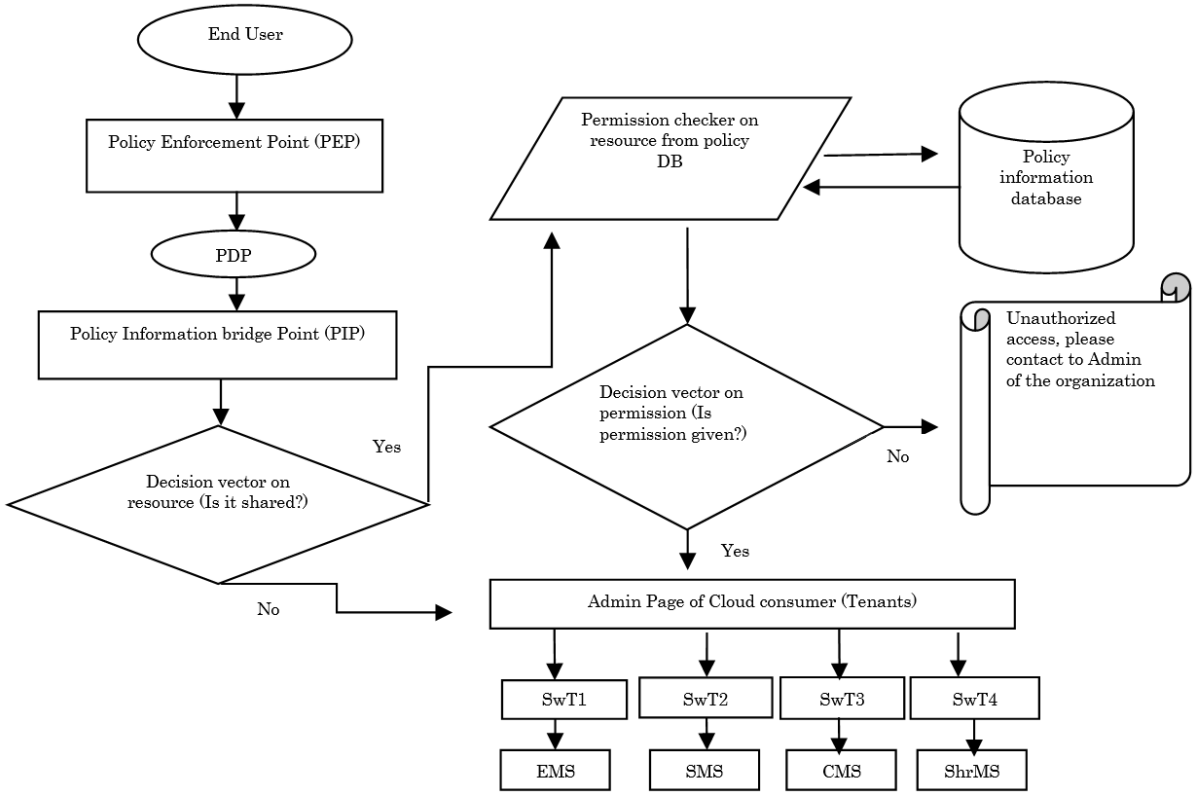

FIGURE 2. Resource request workflow part 1

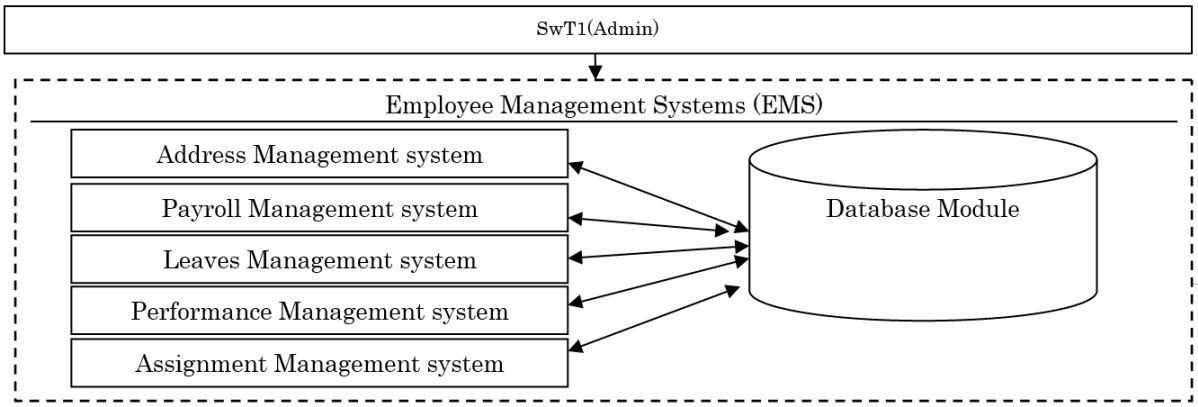

FIGURE 3. Resource request workflow part 2

5.3. **End user.** In proposed model the end user could be a cloud consumer (e.g., U1T1 from Table 3) of the cloud services (e.g., SwT1 from Table 2) or it could be the end user of the organization which acts as a cloud consumer. For example, retail store supervisor is the end user.

5.4. **Policy Enforcement Point (PEP).** The policy enforcement acts as door keeper. In short, the PEP will collect organizational profile of the end users and passes it to PDP for further action.

5.5. **Policy Decision Point (PDP).** In this model the PDP is the central location to collect legitimate request and analyzed. At this point decision is taken which resources are authorized to be used.

5.6. **Policy Information bridge Point (PIP).** In this model the PIP will act as bridge. At PIP, policy related information will be collected from different sources and store into policy DB.

5.7. **Decision vector on resource.** Depending on the resources type shared or non-shared, request is getting diverted to the decision vector or to the admin page for further processing.

5.8. **Permission checker on resource.** In this model, the permission checker checks about the permission status for a specific end user of requested resource present in policy DB.

5.9. **Policy information database.** In this model, policy information database acts as a source of policy information and the permission information on each of the resources. The pictorial representation of policy information DB is shown in Table 3: POLICYINFODB.

5.10. **Decision vector on permission.** In this model, depending on the permission, vector diverts the authorization request to cloud consumer admin page or to the error message screen.

5.11. **Error information page.** In proposed authorization model the error information page is used to depict the message about unauthorized access of the resource by the requestor.

5.12. **Cloud consumer admin page.** Cloud consumer admin page is getting use for configuring the resource and its permission for individual employee of the organization.

5.13. **Cloud services.** Cloud services are the software hosted by multiple vendors on the cloud. This software together creates multi-tenant environment. Researcher has taken SwT1 and EMS as an example for explanation. SwT1 is the Tenant 1 who has developed Employee Management System (EMS) and hosted this to cloud hosting environment. Employee management system comprises components mentioned in Figure 3.

6. **Conclusion.** This paper focuses on the best practices for securing cloud services in multi-tenant environment and presented an authorization model. A case study of retail sector is being presented and the cloud architecture for multi-tenant environment in SAAS paradigm is founded first in place. The proposed model establishes an agreement between tenants, cloud providers and authorization policy is managed through policy database. In future, researchers are planning to modify the proposed model in the following three aspects: 1) apply model to other sector like manufacturing, 2) find out more solution towards performance and optimization and 3) conduct more in-depth research on allocation of cloud resources in isolation way for multi-tenant environment.

REFERENCES

[1] S. A. Khan and R. A. Khan, Authorization estimation model: An object oriented design complexity perspective, *International Journal of Security and Its Applications*, vol.8, no.5, pp.213-226, 2014.

[2] G. Priya, B. R. Kavitha, G. Ramya, P. Kumaresan and F. A. Mon, An access control models in cloud computing, *International Journal of Pure and Applied Mathematics*, vol.116, no.24, pp.539-548, 2017.

[3] R. L. Krutz and R. D. Vines, *Cloud Security – A Comprehensive Guide to Secure Cloud Computing*, Wiley Publishing, 2010.

[4] *Web-Reference*, https://www.comparethecloud.net/articles/8-public-cloud-security-threats-to-enterprises-in-2017/, Accessed on 30/09/2018.

[5] *Web-Reference*, https://www.datamation.com/cloud-computing/private-cloud-providers.html, Accessed on 30/09/2018.

[6] N. Xue, H. Haugerud and A. Yazidi, On automated cloud bursting and hybrid cloud setups using Apache Mesos, *The 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, DOI: 10.1109/CloudTech.2017.8284707, 2017.

[7] J. K. Wang and X. Jia, Data security and authentication in hybrid cloud computing model, *IEEE Global High Tech Congress on Electronics (GHTCE)*, DOI: 10.1109/GHTCE.2012.6490136, 2012.

[8] S. Kanade and R. Manza, A comprehensive study on multi tenancy in SAAS applications, *International Journal of Computer Applications*, vol.181, no.44, pp.25-27, 2019.

[9] J. V. Chandra, N. Challa and S. K. Pasupuletti, Authentication and authorization mechanism for cloud security, *International Journal of Engineering and Advanced Technology (IJEAT)*, vol.8, no.6, pp.2072-2078, 2019.

[10] T. Okamoto, An immunity-enhancing security module for cloud servers, *International Journal of Innovative Computing, Information and Control*, vol.16, no.1, pp.137-151, 2020.

[11] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham and S. Jeong, Securing elastic applications on mobile devices for cloud computing, *Proc. of the 1st ACM Cloud Computing Security Workshop (CCSW 2009)*, Chicago, IL, USA, 2009.

[12] *Web-Reference*, https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambda-authorizer.html, Accessed on 09/12/2019.

[13] *Web-Reference*, https://azure.microsoft.com/en-us/, Azure active directory (Azure AD) and API management system (APIM), Accessed on 15/09/2018.

[14] D. Zou, Y. Lu, B. Yuan, H. Chen and H. Jin, A fine-grained multi-tenant permission management framework for SDN and NFV, *IEEE Access*, vol.6, pp.25562-25572, DOI: 10.1109/ACCESS.2018.2828132, 2018.

[15] J. Luo and M. Kang, Risk based mobile access control (RiBMAC) policy framework, *Military Communications Conference (MILCOM 2011)*, Baltimore, MD, pp.1448-1453, 2011.

[16] J. Cao, P. Bellavista, F. Dressler and O. Akan, *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications*, DOI: 10.1007/978-3-642-27317-9, 2012.