



A Review of Cloud Service Security with Various Access Control Methods

Shakti Dubey¹; Dr. P. K. Rai²

¹Research Scholar, APS University, Rewa, MP, India

²Department of Computer Application, APS University, Rewa, MP, India

¹Shakti_it@rediffmail.com; ²pkrapso@gmail.com

DOI: 10.47760/ijcsmc.2021.v10i03.005

Abstract— *Cloud computing is the use of computing resources like hardware and software that are delivered as a service over a network. It confides remote services with a user's data and software. It enables a user to do large amount of storage and large amount of computations. Due to which data security in cloud becomes an important issue. Data access control provides the security of data in the cloud. The large amount of data outsourced in cloud servers. The data access control becomes a challenging issue in cloud storage systems. Basic models includes DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC (Role based access control), task based access control (TBAC) and ABAC (Attribute Based Access Control) model. Risk based access control method is also used in multilevel organization. Security of data as well as services & privacy of users are important in cloud computing environment. Access Control methods provide an effective way to ensure that authorized user's access the data and the system. In this paper we have discussed various features of access control methods for cloud computing environment.*

Keywords— *Access control methods, MAC, DAC, ABAC, RBAC, Risk based access control*

I. INTRODUCTION

Cloud computing is an emerging technology whose growth is on a rise and is being widely adopted by various IT conglomerate companies such as Google, IBM, Salesforce.com. It combines many technologies such as utility computing, grid computing, virtualization, etc.. Cloud computing leverages the advantages of these technologies and provides many benefits that include low investment cost, large storage, faster computations, virtualization, etc. Users store and share their data and information on the cloud and are able to access it from anywhere, anytime on a pay-per-use basis. Since the cloud service provider uses the multi tenancy model [24], the outsourced data in it is accessible to multiple users. Thus, there is a high threat to the security of outsourced data in the cloud. Also, the cloud service providers and the data owners are most likely to be in different domains.

Therefore, there is a great need for providing security against these untrusted service providers. Each of these technologies has its own security mechanisms to ensure security and privacy of the user's data. However, security mechanism of one technology cannot be applied to cloud computing as a whole. Protecting the data from the malicious users in the cloud is of utmost importance. Data can be secured and protected by ensuring that only the authenticated and authorized users access it. One of the solutions for providing security and

privacy to the data is through the use of access control mechanisms. Access control is a fundamental aspect of information security that is directly tied to the primary characteristics such as confidentiality, integrity and availability.

Cloud computing service providers are expected to provide the following basic functionalities from the perspective of access control: (i) Control access to the service features of the cloud based on the specified policies and the level of service purchased by the customer. (ii) Control access to a consumer's data from other consumers in multi-tenant environments. (iii) Control access to both regular user functions and privileged administrative functions. (iv) Maintain accurate access control policy and up to date user profile information. In this paper we have compared various access control mechanisms and identity & access management mechanisms in cloud environment.

II. BASIC ELEMENTS OF ACCESS CONTROL

The purpose of access control is to restrict access by an accessing subject to an accessed object and to make information resources accessible within the legal scope [20]. There are basically three components in the access control model: subject, object and access control policy. The subject is an active entity that makes the access request and, therefore, is the initiator of the access action. The object is a passive entity that receives access to other entities and, therefore, is the recipient of the access action. Access control policy is the set of access rules of the subject to the object. Fig 1 shows, the main elements and the process of making authorization decisions through access control [12]. The access matrix model uses a matrix to describe the access control policy of a system [8]. Lampson first abstracted the problem of access control and proposed a formal representation that uses the subject, the object and an access control matrix [17]. In the model, the object is accessed by the subject and the system uses the notion of a reference monitor to control access based on the access matrix.

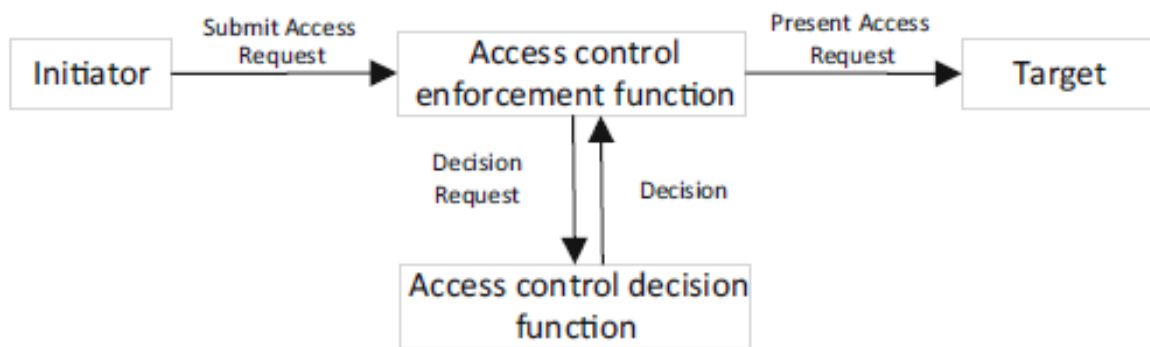


Fig. 1: Process of access control mechanism.[12]

Access control strategy is the main strategy of network security for the prevention and protection of objects with the goal of ensuring that network resources are not illegally used or accessed. There may be multiple access control policies in an access control system. When the subject, the object, and the authority of access control are subordinates to different access control strategies, it may lead to conflict of access control policies, which in turn leads to inconsistent system behavior and result in lower inefficiency and accuracy of the access control. There are definitely more security issues such as access control vulnerabilities.

We have done an in-depth requirement analysis to find the fundamental access control requirements for cloud computing [2]. They are given below –

- a) Dynamic performance and mobility features [15].
- b) Authentication [22].
- c) Trust [15].
- d) Scalability [4].
- e) Heterogeneity [16].
- f) Quality of service [11].
- g) Interoperability [23].
- h) Flexibility in attribute management [13].
- i) Virtualization and sharing of physical resources [18].
- j) Transfer customers' credentials across layers [18].
- k) Assign and ease of privileges [9].
- l) Delegation of capabilities [26].
- m) Auditing [11].

- n) Policy management (add, delete, change, import, and export)
- o) Flexibilities of configuration [9].
- p) Operational and situational awareness [5].

Identity and access management is one of the best practices to measure on cloud services. Presently, Identity and Access Management (IAM) provides effective security for cloud systems. IAM systems perform different operations for providing security in the cloud environment that include authentication, authorization, and provisioning of storage and verification. Taxonomy of cloud service security in various fields are given in Fig 2.

A typical organization's security framework provided by IBM represents that, the organization's security policy should be driven by one of the important security controls that is identity and access management [29]. Identity and access management should ensure that only valid users can have authorized access to the corporate data that can reside across applications. The users accessing the cloud can have various roles such as developer, administrator, IT manager, quality approver, and others, or they may be outside the enterprise such as partners, vendors, customers, and outsourced business or support staff. Beach [25] has presented a governance model which is based on Role-based Access Control (RBAC) policies, enabling dynamic modification of access rights associated with data objects based on activities and responsibilities ("roles") within a virtual enterprise, assigned to subjects within the system.

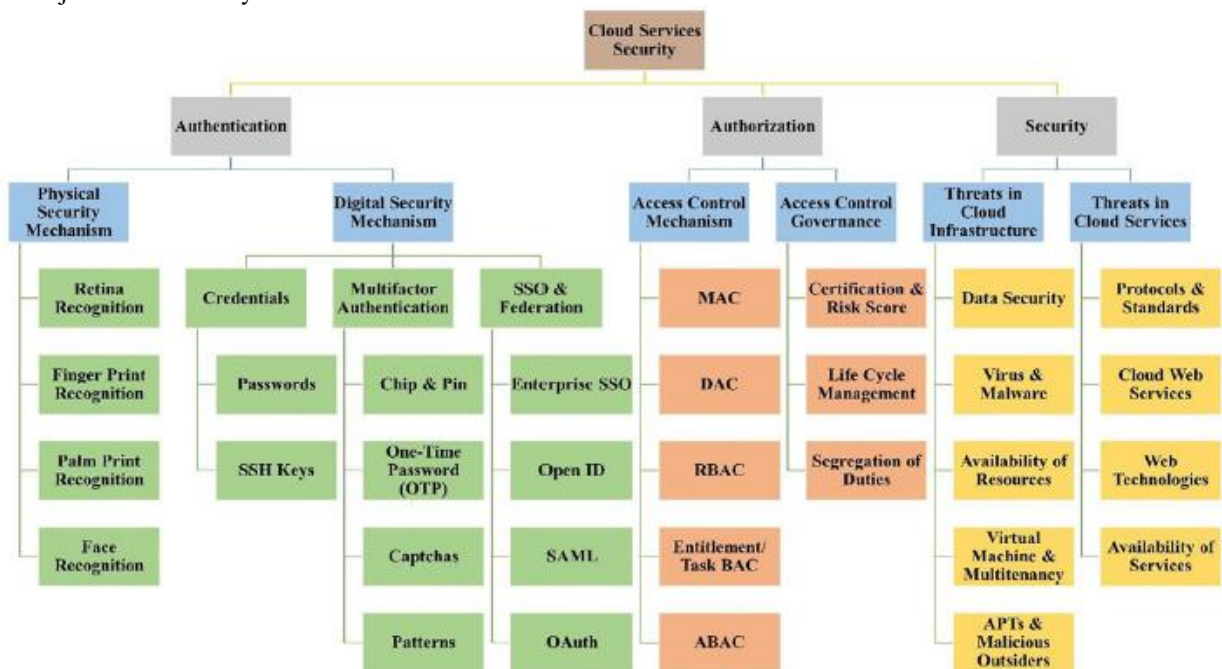


Figure 2: Taxonomy of cloud services security [21]

III. RELATED WORK IN THE FIELD OF ACCESS CONTROL METHODS

Cloud computing technology had developed extensively over the past decade. Most of the organizational computing and data storage had moved on to the cloud environment. Researchers are conducting extensive research to improve cloud computing environment. They are focusing on the virtualization, cloud security, networks, QOS. Cloud computing is a Utility model with high availability and reduced operational cost with higher flexibility and provides services on demand. [3]. Cloud consumers are not required to purchase any additional hardware and software. Cloud service provider (CSP) must ensure the security of the data and services hosted by customers/clients on the cloud. One such popular technique to restrict access to the stored data is through "access control". Access control techniques ensure confidentiality of the data by restricting access only to the authorized users [28].

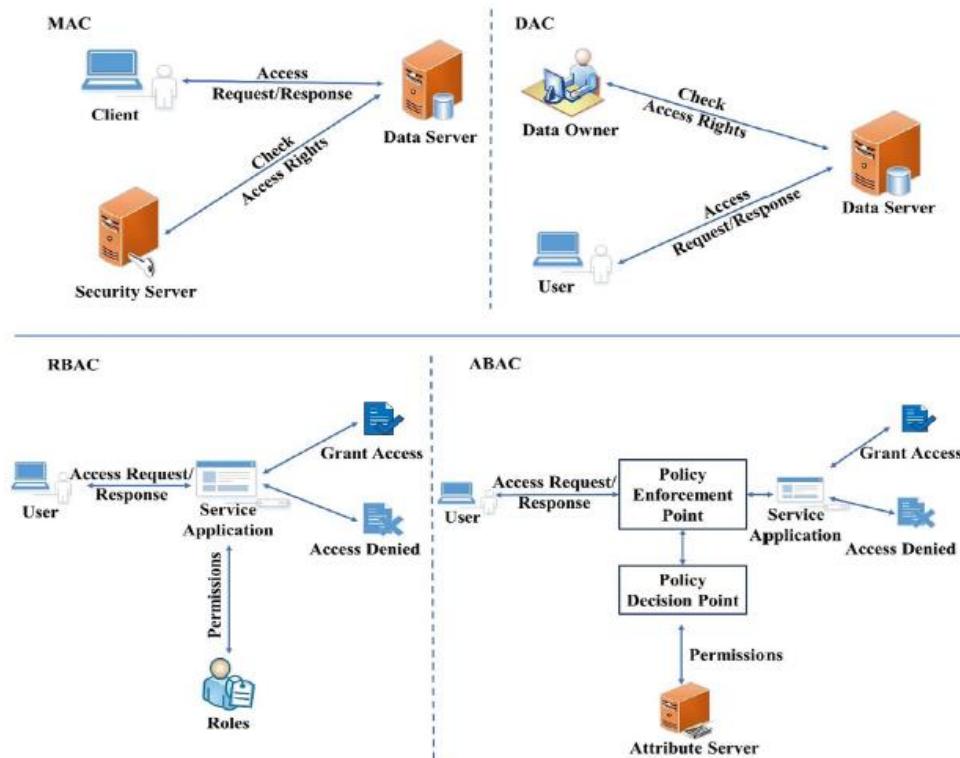


Figure 3: Functional view of main access control methods [21].

Access control means the selective restriction of access to data, service or resource. Accessing a resource means consuming, updating, or using. Authorization is the privilege given to access a resource. For traditional systems, various access control models are proposed. List of basic models includes DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC (Role based access control), task based access control (TBAC) and ABAC (Attribute Based Access Control) model. These basic models are not sufficient for the dynamic cloud environment [28][14]. Functional view of MAC, DAC, RBAC, ABAC model is shown in Fig 3.

Summary of various access control mechanism, security aspects and their issues are shown in Table 1:

TABLE I
SUMMARY OF VARIOUS ACCESS CONTROL MECHANISM

Mechanism	Security aspects	Issues
MAC	Application owns the individual access permissions	Unauthorized access, over classification of data, difficult to implement,
DAC	Access rights to an application is owned and controlled by another application	Trojan horse susceptibility, Flawed software, Information flaws, Malicious attacks
RBAC	Access rights and privileges to multiple applications are bundled as an organizational role	Administrative issues, data abstraction issues, Real-time issues
ABAC	Access rights and privileges to an application determined based on Subject, Object, Policy and Environmental Attributes	Delegation issues, administration issues, auditability and scalability issues

Customer/client loses ownership on cloud-stored data. Encryption based access control models are proposed for cloud computing environment. These access control models restrict unauthorized access by the third party and even by cloud service provider.

In Attribute-Based Encryption (ABE) model user is allowed to access the data using user attributes [1]. The private key and secret key are generated using user attributes. Private keys are shared with consumers satisfying data owner defined access policy. Data owner defines access policy based on user attributes. User having the private key only can decrypt the cipher text. The major disadvantage with ABE is that the data owner has to use the public key of all the users to encrypt the data for storage on the cloud.

To overcome the said problem various access control models are proposed based on ABE. We will be discussing few of them. In Key policy Attribute-based Encryption (KP-ABE) access control model cipher text is

associated with a set of user attributes and the private key is associated with access structure [1]. The user can decrypt the cipher text only when the associated attribute set satisfies the access structure.

In Ciphertext-Policy Attribute-Based Encryption (CP-ABE) model cipher text is associated with access structure and the private key is associated with a set of user attributes [19]. A user can decrypt the cipher text only when the user attributes satisfies the access structure associated with the ciphertext. In risk based access control, they will deal with risk parameters [7].

Lakshmi et al [16] implements risk based access control. They have taken into consideration several parameters that assess the individual's risk. Access is provided to the user only if his/her risk value is lesser than the threshold risk. Therefore, any possibility of insider threat such as buffer overflow and session hijacking attack is tackled before it occurs. According to them their model allows a maximum risk of 70% which means that even at the worst case scenario, 30% of the data is still secure. There is a huge potential for future enhancement.

In this research work, they have considered risk parameters and calculated two types of risk i.e. Current risk value and Threshold risk value. The effectiveness of module has been demonstrated through example which clearly blocks the inside attackers. The module considers risk level with respect to various parameters and calculates the required computations using simple equations. Also, the risk parameters can be adopted as per the organizational requirements. This proposed module is static in nature. The dynamic and adaptive risk based access control modules require slight modification and enhancement of the static risk based access control since it is the foundation for working of the two.

Usually, researcher uses eight parameters to calculate the final risk value - Year of Experience, Designation, Defect Level, Referral Index, Location Index, Time Index, Appraisal Factor & Probationary Period[7]. Wided Ben Daoud et al proposes the use of risk and role based dynamic access control for preventing intrusions targeting the cloud computing, where the main enhancement of the proposed procedure is that access decision is mainly based on the resources available in the cloud services providers. This model allows the discard of non-authorized users based on a computed and updated risk metric, which allows preventing intrusions targeting the cloud network. The basic idea behind this model is to enhance the security of the access control procedure in cloud system. By implementing RBAC combined with the concept of risk and trust[27]. Table 2 shows contrast results of common access control methods on various factors [6].

TABLE 2
COMPARISON OF COMMON ACCESS CONTROL METHODS [6]

Factor	MAC	DAC	RBAC	TBAC	ABAC
Security	Y	N	N	N	N
Confidentiality	Y	Y	N	N	N
Flexibility	N	Y	Y	Y	Y
Minimum privilege	Y	N	Y	Y	Y
Duty separation	Y	N	Y	Y	Y
Description	Y	Y	Y	Y	Y
Granularity	Y	Y	N	Y	Y
Constraint	Y	N	Y	N	Y
Dynamic	N	Y	N	Y	Y
Compatible	N	Y	Y	N	Y
Expansibility	N	Y	N	Y	Y
Management	Y	N	Y	N	N

IV. CONCLUSIONS

Cloud computing is an emerging technology that is currently the most reliable system to store and secure information. Even though cloud based system has numerous benefits, it has some issues associated with security of the stored data. In this paper, we have analyzed different articles that examine the access control mechanisms used in cloud computing according to the NIST standards and compared and classified processes of these articles.

Access control for intrusion prevention is a basic condition of any information system. It is already becoming a hot topic in the field of services security. Thus, there are several models, methods, and technologies capabilities deployed to offer adequate access control systems. Furthermore, although MAC and DAC are the most trustworthy models amongst the systems that were examined, they were not preferred on their own because of the flexibility of MAC and the low security of DAC relative to MAC. The research in the literature shows that the most used model is RBAC.

REFERENCES

- [1]. A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A Berkeley view of cloud computing," Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, vol. 28, no. 13, p. 2009, 2009.
- [2]. Almutairi A, Sarfraz M, Basalamah S. "A distributed access control architecture for cloud computing." *Softw IEEE* 2012;29(2):36e44. Retrieved from, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber%406095492.
- [3]. Aluvalu RajaniKanth and Lakshmi Muddana. "A Survey on Access Control Models in Cloud Computing." *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1*. Springer International Publishing, 2015.
- [4]. Choudhury AJ, Kumar P, Sain M, Lim H, Jae-Lee H., "A strong user authentication framework for cloud computing." In: 2011 IEEE Asia-Pacific Services Computing Conference. IEEE; 2011 pp. 110e5. <http://dx.doi.org/10.1109/APSCC.2011.14>.
- [5]. Crago S, Dunn K, Eads P, Hochstein L, Kang D-I, Kang M, et al., "Heterogeneous cloud computing." In: 2011 IEEE International Conference on Cluster Computing. IEEE; 2011. pp. 378e85. <http://dx.doi.org/10.1109/CLUSTER.2011.49>.
- [6]. Fangbo Cai, Nafei Zhu, Jingsha He, Pengyu Mu, Wenxin Li, Yi Yu, "Survey of access control models and technologies for cloud computing" Springer 2018 <https://doi.org/10.1007/s10586-018-1850-7>
- [7]. Ferraiolo DF, Barkley JF, Kuhn, "A role-based access control model and reference implementation within a corporate intranet." *ACM Trans Inf Syst Secur* 1999;2(1):34e64. <http://dx.doi.org/10.1145/300830.300834>.
- [8]. Goyal, V., Pandey, O., Sahai, A. and Waters, B., 2006, October. "Attribute-based encryption for fine-grained access control of encrypted data". In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89-98). Acm.
- [9]. Han, D.J., Gao, J., Zhai, H.L., et al., "Research progress of access control model." *Comput. Sci.* 37(11), 29–33 (2010)
- [10]. Hasebe K, Mabuchi M, Matsushita A., "Capability-based delegation model in RBAC." In: *Proceeding of the 15th ACM symposium on Access control models and technologies e SACMAT '10*. New York, New York, USA: ACM Press; 2010. pp. 109e18. <http://dx.doi.org/10.1145/1809842.1809861>.
- [11]. Hu VC, Kuhn DR, Ferraiolo DF., "The computational complexity of enforceability validation for generic access control rules." In: *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing e Vol 1 (SUTC'06)* vol. 1. IEEE; 2006. pp. 260e7. <http://dx.doi.org/10.1109/SUTC.2006.1636184>.
- [12]. I. Indu a, P.M. Rubesh Anand, Vidhyacharan Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges" *Engineering Science and Technology, an International Journal* 21 (2018) 574–588 elsevier
- [13]. Jin X, Krishnan R, Sandhu R., "A unified attribute-based access control model covering DAC, MAC and RBAC." In: *DBSec'12 Proceedings of the 26th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy*, vol. 7371; 2012. pp. 41e55. Retrieved from, <http://www.springerlink.com/index/V7Q168247006164H.pdf>; 2012.
- [14]. Karthick, A. V., E. Ramaraj, and R. Ganapathy Subramanian. "An efficient multi queue job scheduling for cloud computing." *Computing and Communication Technologies (WCCCT), 2014 World Congress on*. IEEE, 2014.
- [15]. Keromytis AD, Smith JM., "Requirements for scalable access control and security management architectures." *ACM Trans Internet Technol* 2007;7(2):22. <http://dx.doi.org/10.1145/1239971.1239972>.
- [16]. Lakshmi Hi, Namitha S, Seemanthini, Satheesh Gopalan, Dr.Sanjay H N, Chandrashekar K, Atul bhaskar "Risk Based Access Control In Cloud Computing", 2015 IEEE
- [17]. Lampson, B.W., "A scheduling philosophy for multiprocessor systems." *Commun. ACM* 11(5), 347–360 (1968)
- [18]. N. N. Diep, L. X. Hung, Y. Zhung, S. Lee, Y.-Lee, H. Lee, "Enforcing access control using risk assessment", in *Proc. 4th European Conference on Universal Multiservice Networks (ECUMN '07)*, Washington DC., IEEE Computer Society, 2007, pp. 419-424.
- [19]. Oh S, Park S., "Task role-based access control model." *Inf Syst* 2003;28(2002):533e62. Retrieved from, <http://www.sciencedirect.com/science/article/pii/S0306437902000297>.
- [20]. Patil V, Mei A, Mancini L., "Addressing interoperability issues in access control models." In: *ASIACCS '07 Proceedings of the 2nd ACM symposium on Information, computer and communications security*, vol. 389e391; 2007. Retrieved from, <http://dl.acm.org/citation.cfm?id%401229337>; 2007.

- [21].R. Sandhu, P. Samarati, "Access control: principles and practice", IEEE Communications Magazine, vol. 32(9), 1994, pp. 40-48.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
- [22].RajaniKanth Aluvalu, Lakshmi Muddana, "A Survey on Access Control Models in Cloud Computing", Springer International Publishing Switzerland 2015 S.C. Satapathy et al. (eds.), Emerging ICT for Bridging the Future – Vol. 1, Advances in Intelligent Systems and Computing 337, DOI: 10.1007/978-3-319-13728-5_73 pp. 653
- [23].Shen, H.B., Hong, F., "Review of access control model." Appl. Res. Comput. 22(6), 9–11 (2005)
- [24].Sun, P.J., "Security and privacy protection in cloud computing: Discussions and challenges", Journal of Network and Computer Applications (2020), doi: <https://doi.org/10.1016/j.jnca.2020.102642>.
- [25].Thomas Beach, Omer Rana, Yacine Rezgui, Manish Parashar, "Governance Model for Cloud Computing in Building Information Management", IEEE TRANSACTIONS ON SERVICES COMPUTING, 2013
- [26].Wang W, Han J, Song M, Wang X., "The design of a trust and role based access control model in cloud computing." In: 2011 6th International Conference on Pervasive Computing and Applications. IEEE; 2011. pp. 330e4. <http://dx.doi.org/10.1109/ICPCA.2011.6106526>.
- [27].Wided Ben Daoud, Amel Meddeb-Makhlouf, Faouzi Zarai, " A Model of Role-Risk Based Intrusion Prevention for Cloud Environment", IEEE 2018
- [28].Younis A. Younis, Kashif Kifayat, Madjid Merabti, "An access control model for cloud computing," Journal of Information Security and Applications (2014) Elsevier, <http://dx.doi.org/10.1016/j.jisa.2014.04.003>
- [29].<https://www.ibm.com/cloud/architecture/architectures/securityArchitecture/security-policy-governance-risk-compliance/>