Table 2. EF-RBAC against ordinary methods of access

S. No	Comparison Property	DAC	MAC	RBAC	TRBAC	ARBAC	EF-RBAC
1	Least privilege principle	N	N	Y	Y	N	Y
2	Delegation of duties	Y	N	N	N	N	Y
3	Separation of duties	N	N	Y	Y	N	Y
4	Auditing	Y	Y	Y	Y	Y	Y
5	Configurational flexibility	N	N	Y	Y	N	Y
6	Situational and Operational analysis	N	N	N	Y	Y	Y
7	Handling of heterogeneity	N	N	N	N	N	Y
8	Scalability	N	N	Y	Y	N	Y
9	Limiting the accesses	N	N	N	N	N	Y
10	Flexibility to request transaction from other user	N	N	N	N	N	Y

of the previous one. After that User 3 can view video from her own account.

- Thus, the user borrowing transaction, need not to login with another user's ID.
- Thus, the EF-RBAC scheme results in limited and predictable load for the server and also reducing rates of packages as per the user's requirements. This also helps to protect one's credentials, as for sharing a transaction users need not to share their login details.

6. Analysis, benefits & limitations of proposed scheme

6.1. Analysis

The EF-RBAC scheme is providing flexible, efficient and dynamic functionality like modification of permissions assigned for various tasks, updating of specific tasks for particular roles and also updating of roles specific to various users can be done as per the requirements of currently active tasks of the organization. Furthermore, by imposing a limit over the number of transactions specific to each user and role, this scheme is providing an upper bound for the server's load. Also, it is flexible enough by providing transaction requesting facility among users with the same role if one's limit exceeds.

If the organization has N number of users and T number of transactions, the worst case complexity of the algorithm for looping through all the N users for the execution of T tasks will be O(N*T). Thus, a server needs to handle a fixed number of tasks daily, unlike ordinary schemes with no limit over the server load. Also, table 2 is presenting the functionality analysis of EF-RBAC against ordinary methods of access control over various parameters.

6.2. Benefits

For the proposed scheme users are assigned with roles based on the least required privileges policy for an object. Every access is tracked and any practice of unauthorized access is also captured. In nutshell, we can say that this scheme is scalable, dynamic and support active and passive workflow in the system. Apart from these, the proposed mechanism can also provide the following benefits:

- *Protection against Distributed Denial of Service Attacks (DDoS):* With limited accesses scheme this will also provide protection against distributed denial of service (DDoS) attacks. As no attacker can barr the services with limited accesses.
- *Decreased threats on the server:* It will minimize the risk of information access by the intruders by limiting the accesses for users. Also, it reduces the chance of information misuse by even authentic users, as only required information is available to them under the least privilege policy.
- *Reduces the cost of organization:* As the model is scalable enough, the cost of management, operations, and maintenance also varies according to services availed with time.
- *Improved server response time & operational efficiency:* It reduces server workload by limiting the per day accesses as per users/roles, unlike ordinary access control methods. This leads to higher operational potency and better response time for the servers.
- *Separation of duties and auditing*: This model reduces conflicts by separating each permission for tasks, tasks specific to roles and roles for each user. The auditing process gets simplified by this approach.
- *Delegation of tasks:* This policy leads to easy auditing and visibility of tasks for administration. Thus if any user is overloaded with tasks, then the administration has the choice to delegate his/her duties to different users.
- *Improved security as it follows the least privilege principle:* As data is a valuable asset nowadays, this scheme is surely enhancing the security from suspicious attempts from internal and external users. So it is decreasing the risk of data leakage and breaches by intruders.
- *Limited network usage if organization have numerous employees:* No matter the number of employees an organization hires, the network usage will always be limited. The network cost and server cost will always be measurable with the proposed scheme.

- *Compliance enhancing:* As most of the costs are countable, it gives the ability to easily verify all the policies and activation compliances.

well as reducing the server's overhead. A case study for the Netflix Cloud server is also discussed followed by the benefits and limitations of the proposed EF-RBAC scheme. For further improvement, some good authentication mechanisms can also be applied within this

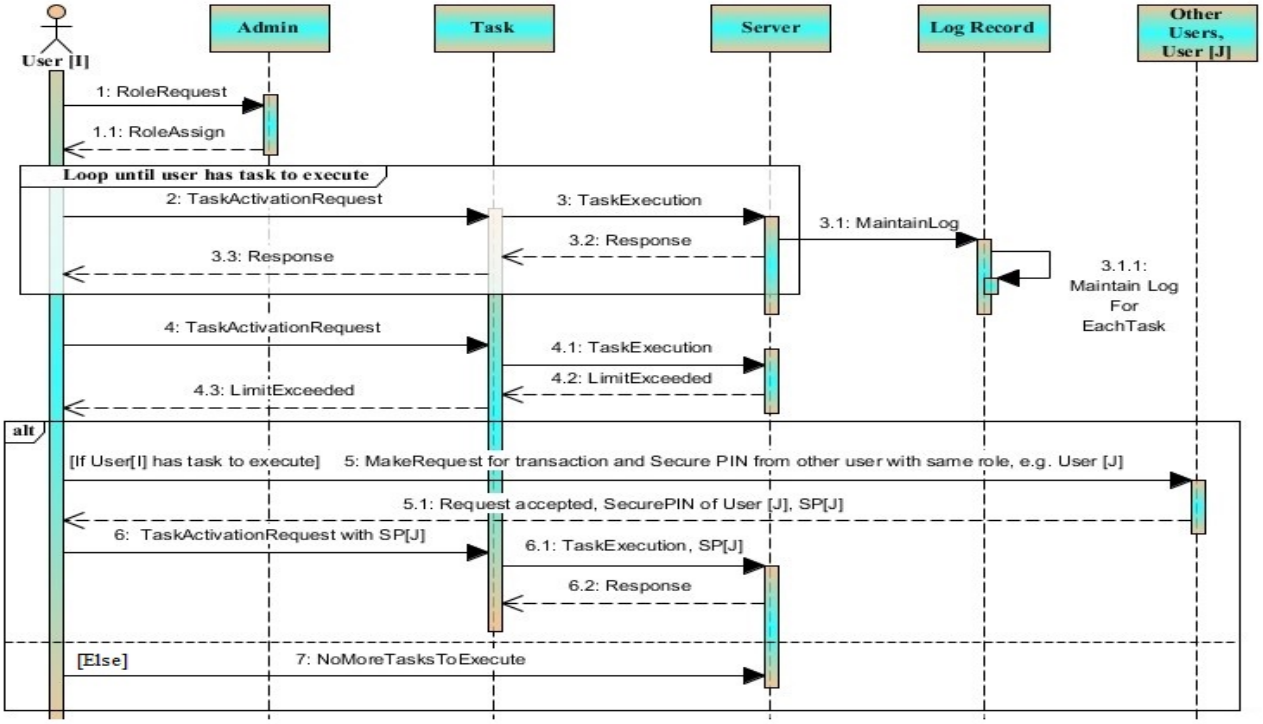

Figure 4. Sequence of events for EF-RBAC Algorithm's

6.3. Limitations of the proposed scheme

Sometimes if the roles of users are changing dynamically, it may create confusion regarding which user is associated with which privileges. Roles are assigned on the basis of the Least privilege principle, but still, if roles are changed frequently then some confusion may arise.

7. Conclusion and future scope

There are several access control mechanisms available but for the open cloud computing environment, but only a few access control schemes are applicable. The best and most applicable approach for such environments seems to be Role-based access control (RBAC). The scalability, measurability and flexibility properties of this model make it most useful amongst users. This work has implemented an efficient and flexible RBAC mechanism with some variations over ordinary RBAC. The implementation is done with the CloudSim (version 3.0) simulator and the steps are discussed in the form of an algorithm in paper. The proposed scheme is implemented for real applications can conspicuously give hopeful results as it is limiting the intruder's accesses, providing protection against DDoS attacks, improving security as model.

References

[1] Wang, W., Han, J., Song, M. and Wang, X. (2011). The Design of a Trust and Role Based Access Control Model in Cloud Computing. *In proceedings of the 6th International Conference on Pervasive Computing and Applications, IEEE*, ICPCA-2011, pp. 330-334.

[2] Harnal, S. and Chauhan, R.K. (2019). Hybrid Cryptography based E2EE for Integrity & Confidentiality in Multimedia Cloud Computing. *International Journal of Innovative Technology and Exploring Engineering (IJITEE), Scopus*, 8(10), pp. 918-924.

[3] Sandhu, R.S., Coyne, E.J., Feinsteink, H.L. and Youman C.E. (1996). Role-Based Access Control Models. *IEEE Computer*, 29(2), pp. 38-47.

[4] Younis, A., Kashif, K. and Merabti, M. (2014). An access control model for cloud computing. *Journal of information security and applications, Science Direct*, Elsevier Science Inc., 19(1), pp. 45-60.

[5] Rouse, M. (2018). Role-based access control (RBAC). *The Essential Guide [Internet]*. https://searchsecurity.techtarget.com/ definition/role-based-access-control-RBAC.

[6] Blaze, M., FeigenBaum, J. and Keromytis, A.D. (1998). Keynote: Trust management for public-key infrastructures. *Cambridge Security Protocols 1998, LNCS*, Berlin: Springer, Heidelberg, 1550, pp. 59-63.

[7] Alattab, B.S., Fadewar, H.S. (2014). Security Issues and Challenges in Cloud Computing. *International Journal of Emerging Science and Engineering (IJESE)*. ISSN: 2319–6378. 2(7), pp. 22-26.

[8] Alattab, B.S. (2015). Role-Based Access Control's Framework for Cloud Computing. *In Conference: 103rd Indian Science Congress*, At Mysore University.

[9] Choudhury, A.J., Kumar, P., Sain, M., Lim, H. and Jae-Lee, H. (2011). A strong user authentication framework for cloud computing. *In: proceedings of 2011 IEEE Asia-Pacific Services Computing Conference*, pp. 110-115.

[10] Hu, V.C., Kuhn, D.R. and Ferraiolo, D.F. (2006). The computational complexity of enforceability validation for generic access control rules. *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, 1.

[11] Hu, V.C. and Scarfone, K. (2012). Guidelines for access control system evaluation metrics. *National Institute of Standards and Technology,* NISTIR 7874.

[12] Ferraiolo, D.F., Barkley, J. and Kuhn, D.R. (1999). A role-based access control model and reference implementation within a corporate intranet. *ACM Transaction on information and System Security (TISSEC),* 2(1), pp. 34-64.

[13] Jin, X., Krishnan, R. and Sandhu, R. (2012). A unified attribute-based access control model covering DAC, MAC and RBAC. *In Proceedings of IFIP Annual Conference on Data and Applications Security and Privacy*, Lecture Notes in Computer Science, SpringerLink, 7371, pp. 41-55.

[14] Keromytis, A.D. and Smith, J.M. (2007). Requirements for scalable access control and security management architectures. *ACM Transactions on Internet Technology (TOIT)*, 7(2).

[15] Almutairi, A., Sarfraz, M., Basalamah, S. and Aref, W.G. (2012). A distributed access control architecture for cloud computing. *IEEE Software*, 29(2), pp. 36-44.

[16] Crago, S., Dunn, K., Eads, P., Hochstein, L., Kang, D.L. and Kang, M. et al. (2011). Heterogeneous cloud computing. *In IEEE International Conference on Cluster Computing (CLUSTER)*, Austin, TX, USA.

[17] Patil, V., Mei, A. and Mancini, L.V. (2007). Addressing interoperability issues in access control models. *In ASIACCS 2007, Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pp. 389-391.

[18] Kaur, G. and Singh, S. (2013). Implementing XML-based Role and Schema Migration Scheme for Clouds. *International Journal of Engineering and Technology (IJET),* 5, pp. 220-225.

[19] Goyal, V., Pandey, O., Sahai, A. and Waters, B. (2006). Attribute-based Encryption for Fine-Grained Access Control of Encrypted Data. *Proceedings of the 13th ACM Conference on Computer and Communications Security,* pp. 89-98.

[20] Bethencourt, J., Sahai, A. and Waters, B. (2007). Cipher text-Policy Attribute-Based Encryption. *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 321-334.

[21] Yang, K. and Jia, X. (2012). Attribute-based Access Control for Multi-Authority Systems in Cloud Storage. *Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems*, pp. 536-545.

[22] Ristenpart, T., Tromer, E., Shacham, H. and Savage, S. (2009). Hey, You, Get off my Cloud: Exploring Information Leakage in Third-Party Compute Clouds. *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Chicago, USA, pp 199-212.

[23] Shafiq, B., Joshi, J.B.D., Bertino, E. and Ghafoor, A. (2005). Secure Interoperation in a Multi-domain Environment Employing RBAC Policies. *IEEE Transactions on Knowledge and Data Engineering,* 17(11), pp. 1557-1577.

[24] Ruj, S., Nayak, A. and Stojmenovic, I. (2011). DACC: Distributed Access Control in Clouds. *Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications.* pp. 91-98.

[25] Zhu, Y., Hu, H., Ahn, G.J., Huang, D. and Wang, S. (2012). Towards Temporal Access Control in Cloud Computing. *2012 Proceedings IEEE INFOCOM*, IEEE, USA, 2012.

[26] Kaur, M., Wadhwa, P. (2014). An Analytical Review of Role Based Access Control Over Cloud Computing. *International Journal of Latest Scientific Research and Technology*. pp. 15-18.

[27] Harnal, S. and Chauhan, R.K. (2016). Multimedia Support from Cloud Computing: A Review. *In International Conference on Microcom-2016, IEEE*, NIT, Durgapur.

[28] Chenthara S., Ahmed, K., Wang, H. and Whittaker, F. (2019). Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing. *IEEE Access, IEEE*, 7, pp. 74361 – 74382.

[29] Wang, H., Yi, X., Bertino, E. and Sun, L. (2016). Protecting outsourced data in cloud computing through access management. *Concurrency and Computation: Practice and Experience, Wiley Online Library,* Special issue paper, 28 (3), pp. 600-615.

[30] Kabir, E., Mahmood, A., Wang, H. and Mustafa, A. (2015). Microaggregation Sorting Framework for K-Anonymity Statistical Disclosure Control in Cloud Computing. *IEEE Transactions on Cloud Computing, IEEE,* pp. 1-1.

[31] Wang, H. and Zhang, R., (2013). Role-based access control to outsourced data in cloud computing. *Proceedings of the Twenty-Fourth Australasian Database Conference*. 137.

[32] Wang, H., Jiang, X. and Kambourakis, G. (2015). Special issue on Security, Privacy and Trust in network-based Big Data. *Information Sciences*, *Elsevier Science Inc.,* 318(C), pp. 48-50.

[33] Wang, H., Cao, J. and Zhang, Y. (2005). A flexible payment scheme and its role-based access control. *IEEE Transactions on Knowledge and Engineering, IEEE,* 17(3), pp. 425-436.