IJRECE VOL. 4 ISSUE 3 JULY.-SEPT. 2016 ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)
DOI: 10.13140/RG.2.1.3643.2883

# Effect of Access Control Policy on Resource Utilization in Cloud Computing – A Comparative study between RBAC and RiskBAC Policy

Iqbalinder Singh Sohal[1] , Amardeep Kaur[2]
[1]*Student (M.Tech),* [2]*Assistant Professor*
*Punjabi University Regional Centre for Information Technology and Management, Mohali*

***Abstract-*** Access control is one of the most important security mechanisms in cloud computing. It permits denies or limits the access of a particular resource to the requesting user. There is various access control policies which cloud are deployed according to the requirement of the organization. Role based access control policy is a traditional role oriented access technique while Risk based access control is a risk aware access control technique which access the requesting user after calculating the trade-off between permitting access to an unauthorized access request and denying an access to an authorized user. It has a calculated value for every instance which is in the form of matrix that's used while deciding the access permissions. In RBAC, users get access to a particular resource depending on the role of that user in the organization. The access control models are developed according to the security need of the organization caring little about the effects they can produce on the utilization of resources. As resource efficiency is one of the fundamental aspects of cloud computing, it is very important to study the effects of access control policies on the resource utilization in cloud computing. No work has been done to study the effects of access control policies on the resource utilization in the cloud computing environment. In this paper, effect of the role based access control policy and risk based access control policy were evaluated on resource utilization in a cloud environment with the resource utilization metrics of processor, RAM and network response time. This study provides an initial exploration of this continuing inquiry. Evaluate results and compare with other techniques for checking utilization over a cloud working environment.

***Keywords-*** Access *Control, privacy model, cloud services and role based access control.*

## I. INTRODUCTION

Cloud computing is the usage of calculating assets (software & hardware) that are transported as a facility done interacting (classically the Internet). Cloud computing assigns distant services with an operator's information, software & calculation. Because various extra computers can be placed into a computer room nowadays than a few years ago, power consumption, air-conditioning, & tools weight, all became imperative reflections [3] for scheme projects. Software tasks likewise arise in this atmosphere for inscription software that cans revenue full benefit of the collective computing power of several machineries is far-off extra challenging than inscription software for a solitary, faster mechanism [2].

Cloud computing be contingent on distribution of resources to prosper unity & frugalities of scale equal to a utility (like the electricity grid) complete a method [4]. Cloud providers identify in detailed submissions & services, & this ability permits them to capably complete elevations & maintenance, replacements, difficulty recover, & failover functions [5, 6]. With cloud computing, officialdoms can display current requirements & make on-the-fly variations to upsurge or reduction ability, obliging points in request devoid of paying for fallow capability during sluggish times. Aside from the possible to minor charges, institutions & campuses gain the litheness of being capable to reply rapidly to needs for novel services by procuring them from the cloud. Cloud computing reassures IT groups & suppliers to growth standardization of conventions & procedures so that the several fragments of the cloud computing perfect can interoperate appropriately & professionally. Cloud computing's scalability is additional key advantage to advanced education, principally for research plans that need vast quantities of storing or dispensation capability for a incomplete time. Particular corporations have built information centres near bases of renewable energy, such as storm farmhouses & hydroelectric services, & cloud computing gives entrance to these suppliers of "green IT." Finally, cloud computing permits institution & campus IT suppliers to create IT costs obvious & thus equal ingestion of IT services to those who pay for such facilities [7].

### *A. Role Based Access Control*

Role Based Access Control (RBAC) using Orientation Ontology offerings a RBAC[8] exemplary by part ontology for Multi-Tenancy structural design for precise field. Figure 1 shows a role based model diagram. Model Ontology change procedures are labelled to associate the comparisons of dissimilar ontology. It delivers profit to decrease the difficulty of arrangement design & application [13].

DOI: 10.13140/RG.2.1.3643.2883

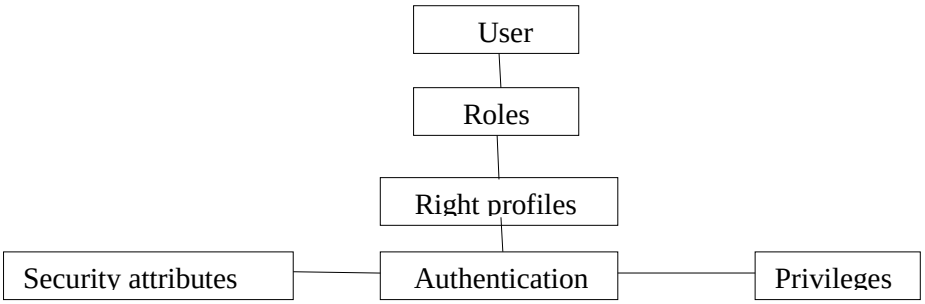


Fig.1 Role Based Access Control Model Working

*B. Three Main Procedure are indistinct for in Role Based Access Control:*

1. Role task: A user can request for resource only if the user is designated a role.
2. Role approval: A user's role request is approved by the system. By instruction 1 overhead, this status safeguards that users can perform on behalf of which they are authorized [9].
3. Authorization approval: Authorization individual [10] if the consent is official for the matter's lively part. With instructions 1 & 2, this rule guarantees that operators can work out only consents for which they are allowable.

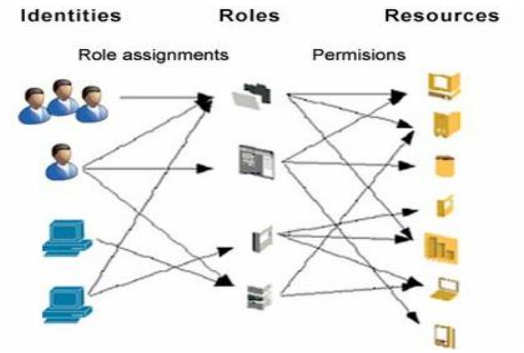


Fig.2 Main Process of RBAC

RBAC diverges as of Admission Controller Lists (ACLs) as shown in Figure 2, castoff in old-style optional admission controller structures, in that it allocates consents to detailed processes by connotation in the society, slightly than to stumpy equal information substances. For instance, an admission regulator incline possibly will be castoff to funding or repudiate inscribe admission to a specific scheme folder, but then it would not command how that folder capacity be different. In an RBAC-based structure, process strength is to make a recognition description contract in a monetary tender or to desert a plasma dearest level check best ever in a medicinal submission [11]. The project of approval to achieve a specific process is expressive, since the processes are granulated with sense within the submission. RBAC has been exposed to be mainly fine suitable to Separation of Duties (Sod) supplies, which safeguard that 2 or extra persons necessity be complicated in permitting dangerous processes. Essential & satisfactory circumstances for security of Sod in RBAC have been examined. A fundamental code of Turf is that no separate ought to be talented to touch an opening of sanctuary finished double pleasure.

## II. RELATED WORK

L. Popeet.al (2010) Admission switch simulations can be usually considered into 3 kinds: (1) Optional (2) Obligatory & (3) Role-based. In the Optional admission controller (OAC) perfect, the proprietor of the article chooses its admittance authorizations for additional customers & groups them [1]. Zhong et.al(2011) RBAC as perfect, a user cannot obtain part consents of a portion, & a fragment cannot receive portion sanctions of additional part[2]. A well grained admission regulator based on RBAC model is planned in this paper. The actions for resolving the usual of authorizations belongs to a role or a user are obtainable. H. A. J. Narayanan et.al (2011) **RBAC as** Consents are definite on work specialist. Procedures on the thing are interested grounded on the approvals. RBAC replicas are additional climbable than the optional & required admittance regulator representations, additional appropriate for custom in cloud computing surroundings, expressly when the operators of the facilities cannot be followed with a stationary distinctiveness[3]. S. Sank et.al(2010) Aimed at together the network calculating & cloud multiplying patterns, there is a mutual necessity to be intelligent to outline the devices complete which regulars determine, appeal, & usage capitals as long as by third-party dominant amenities, & similarly gadget extremely equivalent & dispersed calculations that perform on these resources [4]. E. E. Mon et.al (2011) In a role-based access control (RBAC) perfect, the part of an operator is allocated founded on the smallest honor idea – i.e. the appeal through the minimum quantity of agreements or functionalities that is essential for the occupation to be complete [5].

## III SIMULATION MODEL

We implemented the RBAC and RiskBAC Architecture as shown in figure 3, to study the effects on the resource utilization in cloud computing with some additional features in cloud working structure. The results of both the access control policies were evaluated and then compared to check the performance over a cloud working environment.

DOI: 10.13140/RG.2.1.3643.2883

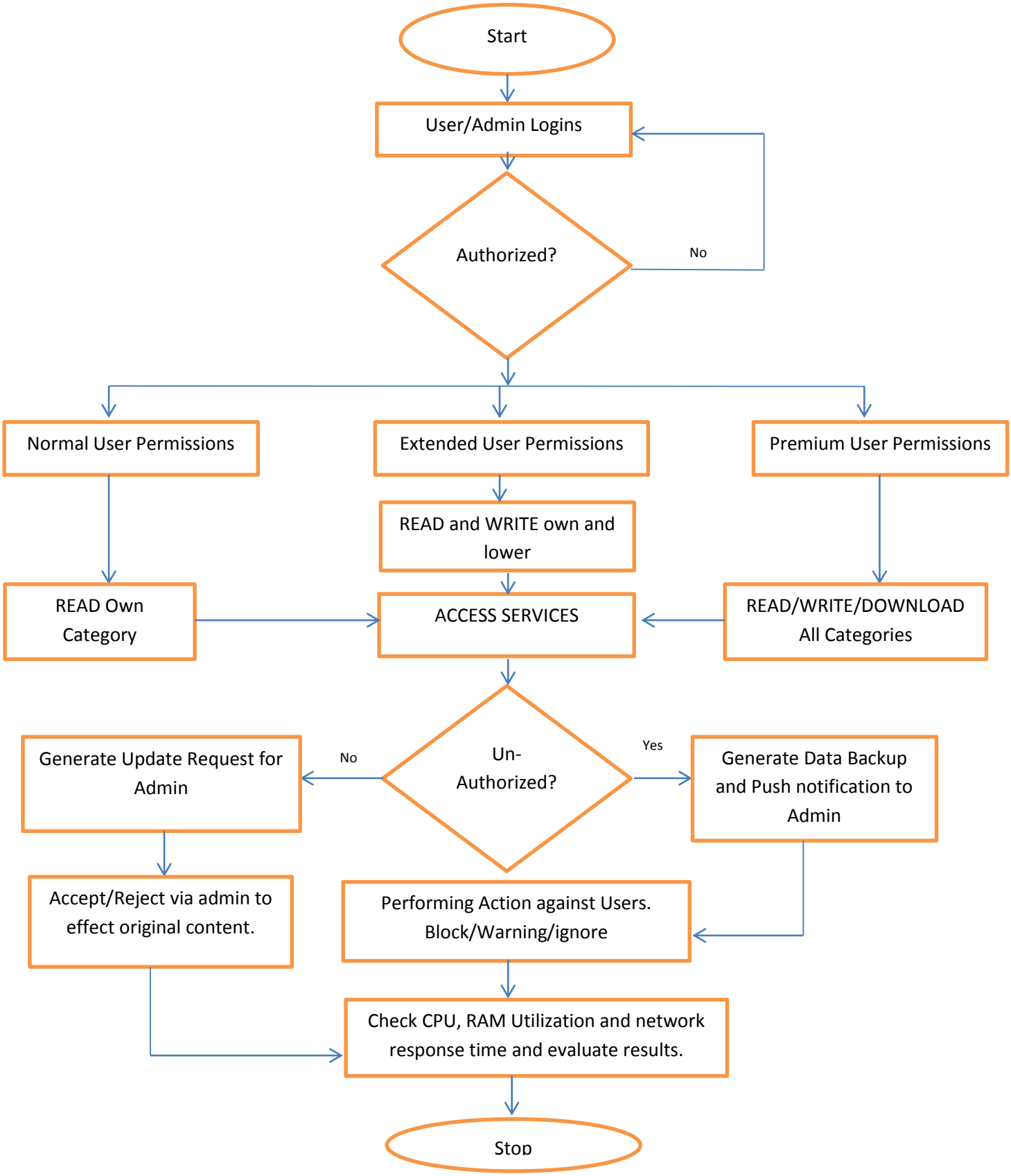



Fig.3 Proposed Flow Chart

DOI: 10.13140/RG.2.1.3643.2883

## IV RESULT ANALYSIS

This section comprises the results of all the scenarios on which RBAC and Risk BAC access control policies are discussed. 4 scenarios were selected on the base of resources and number of users requesting to get access over those resources. Scenario 1 was created with RBAC policy, where the numbers of resources were fixed while the numbers of users were varied. Scenario 2 was also created with RBAC policy, where both the numbers of resources and numbers of users were varied. Scenario 3 was created with RiskBAC policy, where the numbers of resources were fixed while the numbers of users were varied. Scenario 4 was also created with RiskBAC policy, where both the numbers of resources and numbers of users were varied. The numbers of users were varied as 5, 100, 200, 1000 and 2000 in each of the scenarios while the number of resources for scenario 1 and 3 were 10 while the number of resources for scenario 2 and 4 were varied according to the number of users. Five consecutive executions were performed at each case and an average for each case was evaluated. In each scenario, result of the performance metrics i.e. processor utilization, memory utilization, network response time along with access bound is presented below:

### *A. Scenarios comparisons*

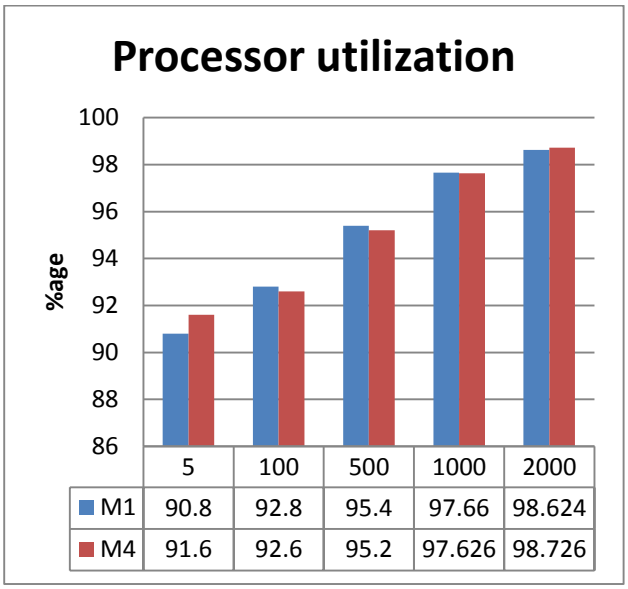
In this section, comparative study is done between various scenarios to check the amount of changes occurred with the change of environment i.e. number of resources and number of users. The results are shown in the form of graphs.

#### *a) Compare Scenario 1 and Scenario 2*

This scenario compares the mean values taken from the results of scenario 1 and scenario 2. The following graphs shows the changes occurred in the utilization of resources when one results are taken keeping the resources fixed while in other results the resources are large in number.

1) *Comparison of Processor utilization:* This comparison is done between M1 and M4 i.e. the mean values of processor utilization under scenario 1 and scenario 2 as shown in Figure 4.

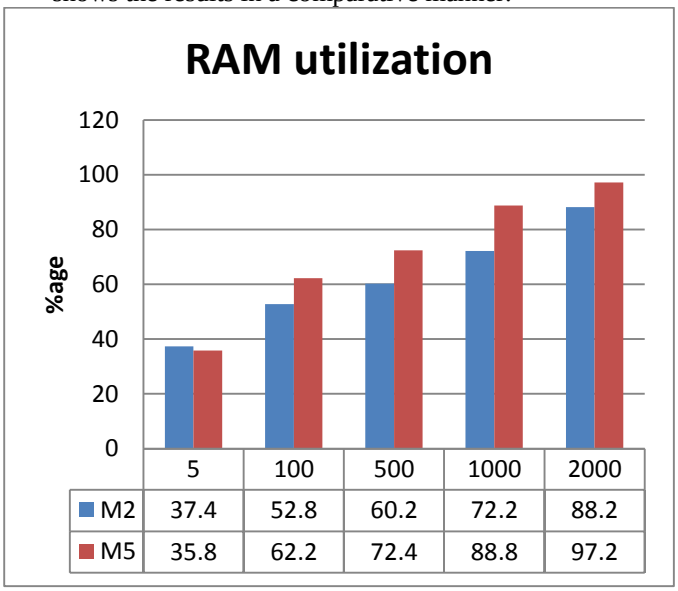
The Figure 4 shows the comparative study of processor utilization where M1 is the calculated value under 10 resources while M4 is calculated under variable number of resources. The processor utilization for 100 and 500 users is less for in M4 while in other cases the processor utilization of M4 is more than M1.




| | 5 | 100 | 500 | 1000 | 2000 |
|---|---|---|---|---|---|
| M1 | 90.8 | 92.8 | 95.4 | 97.66 | 98.624 |
| M4 | 91.6 | 92.6 | 95.2 | 97.626 | 98.726 |

Fig.4 Comparisons M1 and M4

2) *Comparison of RAM utilization*: This comparison is done between M2 and M5 i.e. the mean values of RAM utilization under scenario 1 and scenario 2. Figure 5 shows the results in a comparative manner.




| | 5 | 100 | 500 | 1000 | 2000 |
|---|---|---|---|---|---|
| M2 | 37.4 | 52.8 | 60.2 | 72.2 | 88.2 |
| M5 | 35.8 | 62.2 | 72.4 | 88.8 | 97.2 |

Fig.5 Comparison M2 and M5

This comparison clearly shows that the RAM utilization remains high for scenario 2 in all the cases except for the case when the numbers of users are very less in an environment having large number of resources.

3) *Comparison of Network response time:* This comparison is done between M3 and M6 i.e. the mean values of Network response time under scenario 1 and scenario 2. Figure 6 shows the results in a comparative study.

DOI: 10.13140/RG.2.1.3643.2883

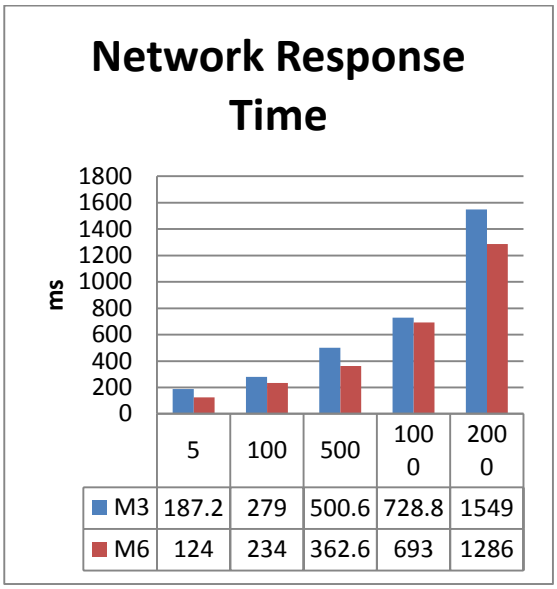



Fig6 Comparison M3 and M6

The Figure 6 shows that the network response time is better for a situation where the numbers of resources are 10 i.e. less. The response time increases because of the network traffic due to large number of shared pool of resources. As the response time of scenario 2 is less. It is easily derived that the performance of scenario 2 is better than scenario 1 as long as network response time is concerned.

From the above 3 graphs in the comparative study of scenario 1 and scenario 2, it is easy to evaluate that the RBAC policy has a better effect when the number of resources is large. It gives better performance in the situation where the numbers of users are very large. The study shows that the RBAC access control policy works better to utilize the resources in a cloud environment where the numbers of users as well as number of resources are large.

### *B. Compare Scenario 3 and Scenario 4*

This scenario compares the mean values taken from the results of scenario 3 and scenario 4 for the Risk based access control policy. The following graphs shows the changes occurred in the utilization of resources when one results are taken keeping the resources fixed while in other results the resources are large in number.

1) *Comparison of Processor utilization:* This comparison is done between M7 and M10 i.e. the mean values of processor utilization under scenario 3 and scenario 4. Figure 7 shows the comparison.

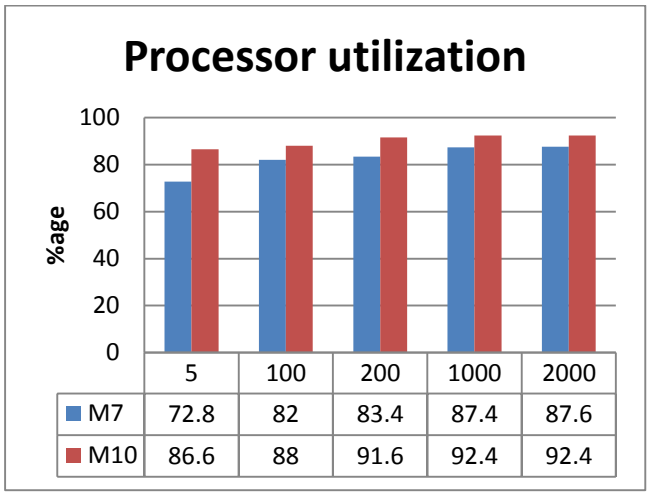



Fig.7 Comparison M7 and M10

The Figure 7 shows the comparative study of processor utilization where M7 is the calculated value under 10 resources while M10 is calculated under variable number of resources. The processor utilization is more in scenario 4 as compared to scenario.

2) *Comparison of RAM utilization:* This comparison is done between M8 and M11 i.e. the mean values of RAM utilization under scenario 3 and scenario 4. Figure 8 shows the results in a comparative manner.

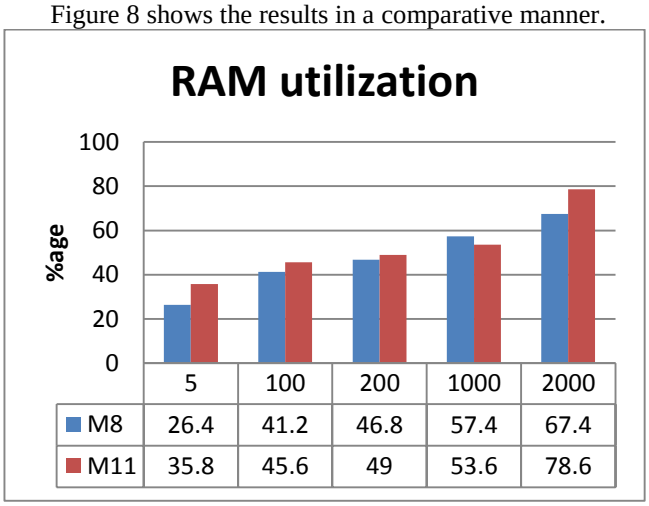



Fig.8 Comparison M8 and M11

This comparison clearly shows that the RAM utilization for 1000 users is good for scenario 3, while RAM utilization remains better for scenario 4 while accessing a cloud network having large number of resources.

3) *Comparison of Network response time*: This comparison is done between M9 and M12 i.e. the mean values of Network response time under scenario 3 and scenario 4. Figure 9 shows the results in a comparative study.

DOI: 10.13140/RG.2.1.3643.2883

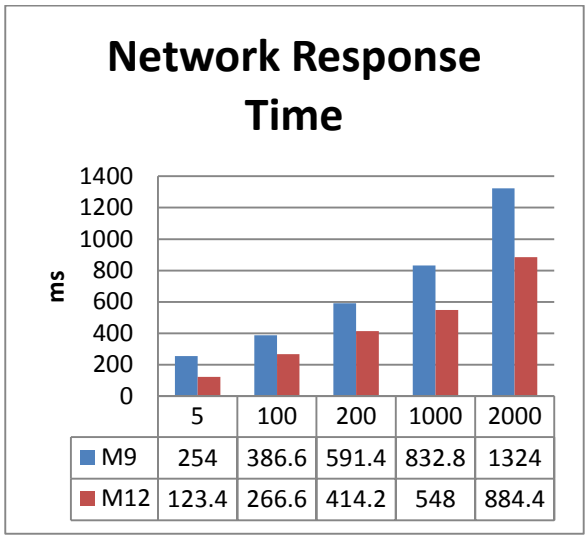



Fig.9 Comparison M9 and M12

This Figure 9 clearly shows that the value for scenario 4 is less as compared to scenario 3. It is already known that lesser the response time better the performance. This depicts that the performance of scenario 4 is better as compare to the performance of scenario 3. From the above comparative study between scenario 3 and scenario 4, it can easily be understood that the Risk based access control policy performs better when the number of resources are increased. It performs better even when the number of users are large having large number of resources.

### C. *Compare Scenario 1 and Scenario 3*

This scenario compares the mean values taken from the results of scenario 1 which is using RBAC policy with the scenario 3 which is using Risk based access control policy. The following graphs shows the changes occurred in the utilization of resources with only change in the access control policy

1) *Comparison of Processor utilization:* This comparison is done between M1 and M7 as shown in Figure 10 i.e. the mean values of processor utilization under scenario 1 and scenario 3 respectively.

The Figure 10 shows the comparative study of processor utilization where both M1 and M7 are calculated with 10 resources. The study shows that the RBAC policy has better resource utilization than the RiskBAC access control policy.

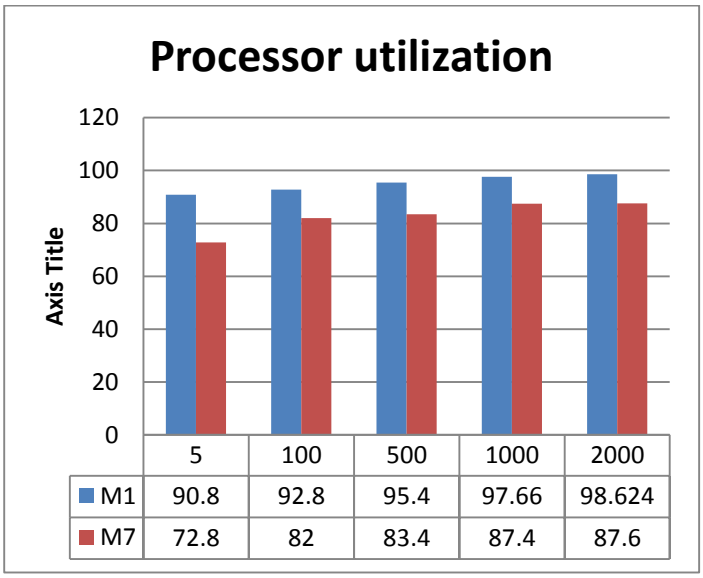



Fig.10 Comparison M1 and M7

2) *Comparison of RAM utilization:* This comparison is done between M2 and M8 i.e. the mean values of RAM utilization under scenario 1 and scenario 3. Figure 11 shows the results in a comparative manner.

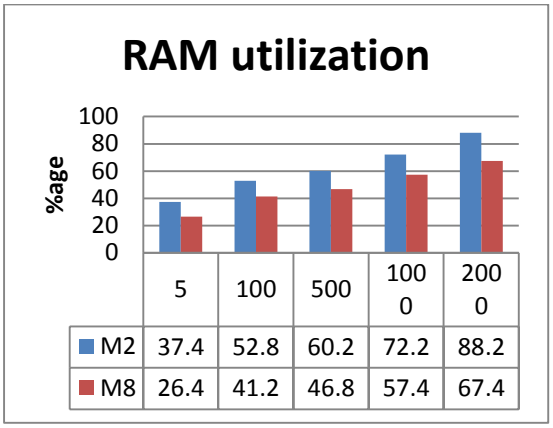



Fig.11 Comparison M2 and M8

This comparison clearly shows that the RAM utilization for scenario 1 is much more than the RAM utilization in scenario 3. This means that RBAC has better effect on the RAM utilization as compared to RiskBAC when it comes to limited number of resources.

3) *Comparison of Network response time:* This comparison is done between M3 and M9 i.e. the mean values of Network response time under scenario 1 and scenario 3. The Figure 12 shows the results in a comparative study.

DOI: 10.13140/RG.2.1.3643.2883

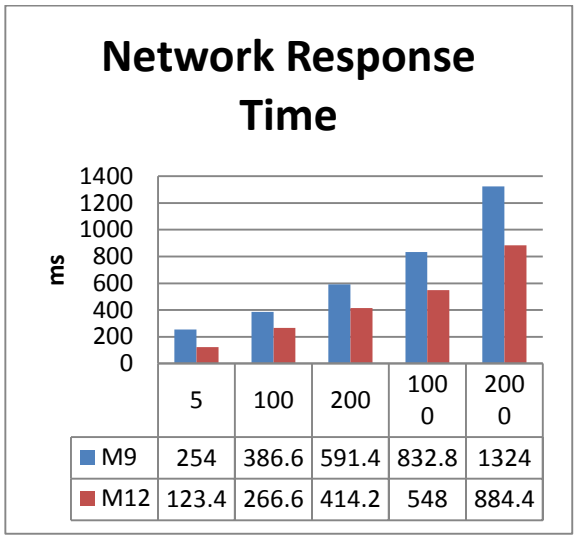



Fig.12 Comparison M3 and M9

This Figure 12 clearly shows that the value for scenario 3 is less as compared to scenario 1. This shows that the Network response time for RiskBAC is better as compared to RBAC. This is because of the reason that RiskBAC doesn't allow all the risky users to get access over any resource in the network making it less traffic in the network and giving response time. From the above comparative study between scenario 1 and scenario 3, it can easily be derived that the RBAC has a better Processor as well as RAM utilization but because the RiskBAC works between the trade-off of the cost of permitting access to unauthorized users and cost of denying authorized user from access a resource, the network traffic comes out to be less hence taking lesser time to do a job while keeping the RAM and Processor free and less utilized as compared to the RBAC access control policy.

*D. Compare Scenario 2 and Scenario 4*

This scenario compares the mean values taken from the results of scenario 2 which is using RBAC policy with the scenario 4 which is using Risk based access control policy. In these scenarios, both the numbers of users as well as number of resources are varying. The following graphs shows the changes occurred in the utilization of resources with only change in the access control policy

1) *Comparison of Processor utilization:* This comparison is done between M4 and M10 i.e. the mean values of processor utilization under scenario 1 and scenario 3 respectively as shown in fugure 13 .

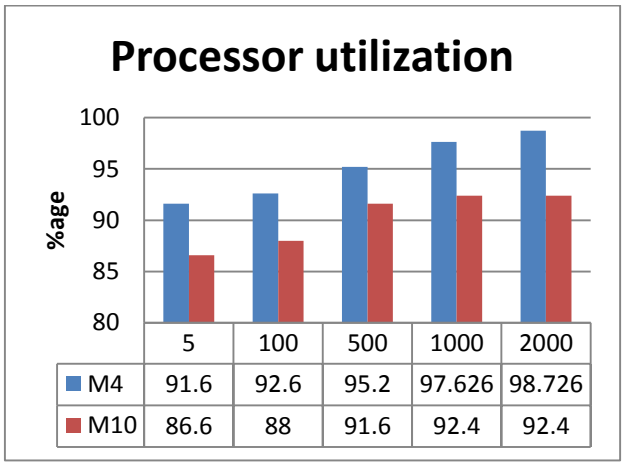



Fig.13 Comparison M4 and M10

The Figure 13 shows the comparative study of processor utilization where both M4 and M10 are calculated under varying number of users as well as large pool of resources. The study shows that the RBAC policy has better resource utilization than the RiskBAC access control policy.

2) *Comparison of RAM utilization:* This comparison is done between M5 and M11 i.e. the mean values of RAM utilization under scenario 2 and scenario 4. Figure 14 shows the results in a comparative manner.

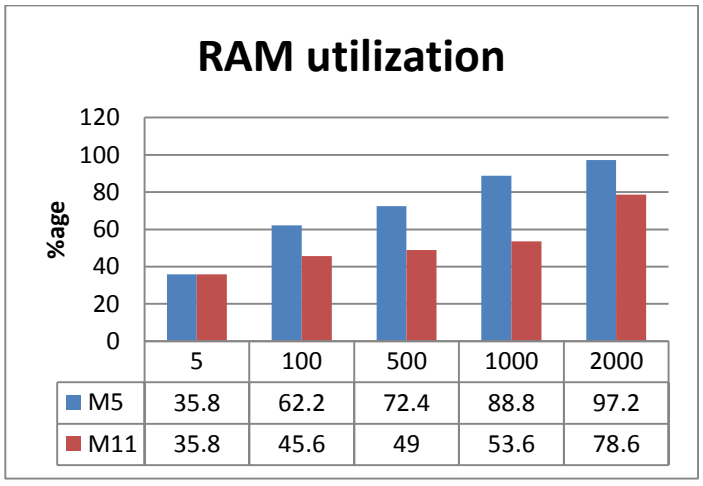



Fig.14 Comparison M5 and M11

This comparison clearly shows that the RAM utilization for scenario 2 is much more than the RAM utilization in scenario 4. This means that RBAC has better effect on the RAM utilization as compared to RiskBAC when it comes to limited number of resources.

3) *Comparison of Network response time:* This comparison is done between M6 and M12 i.e. the mean values of Network response time under scenario 2 and scenario 4 respectively. Figure 15 shows the results in a comparative study.

DOI: 10.13140/RG.2.1.3643.2883

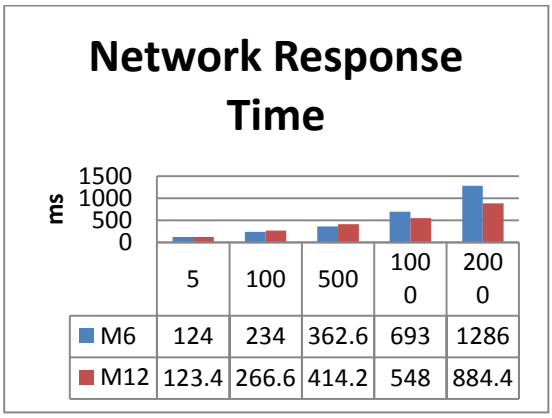



Fig.15 Comparison M6 and M12

It clearly shows that the value for scenario 4 is less as compared to scenario 2 when it comes to large number of resources as well as large number of users. The reason behind this good result by RiskBAC is same as already explained in Network response time in comparative scenario1and scenario 3 i.e. RiskBAC doesn't allow all the risky users to get access over any resource in the network making it less traffic in the network and giving lesser network respond time to complete a task.

## V. CONCLUSION

Access control policies are the basic security aspects of cloud computing which control the access of the cloud resources. The access control by the access control policies for the requested resources by the authenticated and authorized users has direct effect on the utilization of the resources. The effect of access control policies on the resource utilization is the most fundamental outcome of this study. There are many access control policies which has different algorithms which permit access to the resources according to their architecture. This means that the various access control policies affect the resources differently. In the present study, the effects of RBAC and RiskBAC were evaluated according to the parameters i.e Processor utilization, RAM utilization and Network response time. The results of the parameters varied when both access control policies under study were implemented. After analyzing the results, RBAC proved to be better when it comes about the resource utilization as the processor and RAM utilization by RBAC was always on a higher note. The Network response time was better in the case of RiskBAC as it doesn't allow all the users to enter in the scheduling queue directly for resource allocation process. RiskBAC uses a matrix to check the risk between allocating a resource to an unauthorized access with the denying of access to an authorized user. From the above analysis, it can be derived that the performance of risk based access control policy is better but the resource utilization is less. Which means that need to develop new access control policies are required which will have a better resource utilization alongside the performance it produce while securing a cloud environment, Such supplies request skilled policy administrators, who are able to alteration policies to support associations, while confirming that the policies fulfil their important purpose, i.e. they control approved and unconstitutional access. Requirement on well-designed and well-operating access control policies will greatly effect in the better structuring, designing and implementing the access control policies in the cloud computing environments.

## VI. REFERENCES

[1]. L. Pope, M. Yu, S. Y. Kop, S. Ratnasamy & I. Stoical, "Cloud Police: Taking Access Control out of The Network," Proceedings of the 9th ACM Workshop on Hot Topics in Networks, October 2010.

[2]. Zhong, Hu, Yang Dong-yong, & Chen Jin-yin. "Fine-Grained Access Control Model Based on RBAC." Control, Automation & Systems Engineering (CASE), 2011 International Conference on. IEEE, 2011.

[3]. H. A. J. Narayanan & M. H. Guns, "Ensuring Access Control in Cloud Provisioned Health Care Systems," Proceedings of the IEEE Consumer Communications & Networking Conference, 2011.

[4]. S. Sank, C. Hot & M. Rajarajan, "Secure Data Access in Cloud Computing," Proceedings of the 4th IEEE International Conference on Internet Multimedia Services, December 2010.

[5]. S. Yu, C. Wang, K. Ran & W. Lou, "Achieving Secure, Scalable, & Fine-grained Data Access Control in Cloud Computing," Proceedings of the 29th IEEE International Conference on Information Communication, pp. 534-542, 2010.

[6]. E. E. Mon & T. T. Naming, "The Privacy-aware Access Control System using Attributed-and Role based Access Control in Private Cloud," Proceedings of the 4th IEEE International Conference on Broadband Network & Multimedia Technology, pp. 447-451, October 2011.

[7]. V. Goal, O. Pander, A. Sashay & B. Waters, "Attribute-based Encryption for Fine-Grained Access Control of Encrypted Data," Proceedings of the 13th ACM Conference on Computer & Communications Security, pp. 89-98, 2006.

[8]. J. Bettencourt, A. Sashay & B. Waters, "Cipher text-Policy Attribute-Based Encryption," Proceedings of the IEEE Symposium on Security & Privacy, pp. 321-334, 2007.

[9]. K. Yang & X. Jiao, "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, 2012.

[10]. T. Ristenpart, E. Trimmer, H. Sachem & S. Savage, "Hey, You, Get off my Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proceedings

DOI: 10.13140/RG.2.1.3643.2883

of the 16th ACM Conference on Computer & Communications Security, pp. 199-212, 2009.

[11]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, et al., "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[12]. T. Fininet. Al (2008), "ROWLBAC – Representing Role Based Access Control in OWL", ACM SACMAT'08, Vol.11.

[13]. Soofi, Aized Amin, & M. Irfan Khan. "A Review on Data Security in Cloud Computing." International Journal of Computer Applications 94 (2014).

[14]. Kaur, Gurpinder, & Er Monika Bharti. "Securing Multimedia on Hybrid Architecture with Extended RBAC."

[15]. Wolf, William. The Griffiss Institute Summer Faculty Program. GRIFFISS INST INC ROME NY, 2013.