Research Article

iMedPub Journals
http://www.imedpub.com/

American Journal of Computer Science and Information Technology
ISSN 2349-3917

2017
Vol.5 No.2:09

DOI: 10.21767/2349-3917.100009

User Authentication Framework with Improved Performance in Multi-cloud Environment

R Thandeeswaran[1*] and M A Saleem Durai[2]

[1]School of Information Technology and Engineering, VIT University, Vellore, Tamilnadu, India

[2]School of Computer Science and Engineering, VIT University, Vellore, Tamilnadu, India

[*]**Corresponding author:** R Thandeeswaran, School of Information Technology and Engineering, VIT University, Vellore, Tamilnadu, India, E-mail: rthandeeswaran@vit.ac.in

Received date: July 11, 2017; **Accepted date:** December 05, 2017; **Published date:** December 12, 2017

Citation: Thandeeswaran R, Durai MAS (2017) User Authentication Framework with Improved Performance in Multi-cloud Environment. Am J Compt Sci Inform Technol 5: 2. doi: 10.21767/2349-3917.100009

Abstract

Cloud computing is an internet-based computing where shared resources, software and information provided to the end-users, on demand. The end users can be comfortable with the cloud as its features on-demand self-services, broad network access, resource pooling, rapid elasticity and measured service, make it more efficient. Security is one of the major issues which hamper the growth of cloud. Confidentiality–Integrity–Availability are the major security goals to be ensured by the security mechanisms. Authentication could provide a better solution in all three aspects. Various authentication based methodologies proposed by experts are in the field, with their own strength and weakness. This paper proposed an authentication scheme along with performance enhancement. Initial phase of the proposal differentiates the request as wired or wireless network. Based on which, appropriate authentication protocol comes into play, wired adopts keystroke behaviour and wireless follows SSID. In the second phase, users behaviour were analysed and credits assigned to them, based on which resource accessibility is restricted. In the third phase, performance characteristics were taken into account. Analytical results support the claim to enhance the security services and also the performance factors such as resource utilizations and cost.

Keywords Cloud; Security; Authentication; Behaviour; SSID; Access control; Performance

Introduction

Cloud paradigms overruled the globe and dominated the IT industry over a decade. Researchers, Service providers and end-users enjoyed the benefits of cloud services. At the same time, concerns were also arose as common in other types of networks, the dominating issues such as security and performance were thrown on cloud.

The security services, Confidentiality–Integrity–Availability (C-I-A), are considered as security goals. Confidentiality, addresses to not to reveal the data, becomes a security attack when the information is revealed to unauthenticated users. Integrity, focuses on data alteration, becomes a security attack when the data modified by an unauthenticated user. Availability, resource accessibility on need, becomes an attack when they are depleted by simultaneous authorised or unauthenticated user requests. Major security goals can be achieved without a compromise when the users are rightly authenticated.

Authentication could be insisted both on the message and the user. Message authentication deals with content modification whereas user authentication is to identify the person's originality. This proposal focuses on user authentication in three different phases.

The main challenges in multi-cloud deployments, regarding cloud interfacing, are image management, network management and fault tolerance.

- **Cloud interfacing**: Cloud interoperability is probably one of the aspects that are receiving more attention by the community. The need for interoperable clouds is two folded: first, the ability to easily move a virtualized infrastructure among different providers would prevent vendor lock-in and secondly, the simultaneous use of multiple clouds that are geographically distributed can also improve the cost-effectiveness, high availability or efficiency of the virtualized service.
- **Network management**: Resources running on various cloud providers are located in different networks and may use different addressing schemes (public, private, NAT). But some services need all their components to have a uniform IP address so it is necessary to build an overlay network above a physical network for the communication purpose with different service components.
- **Fault tolerance and HA**: If there is a failure in one node then the entire process fails. Number of nodes cannot be changed dynamically. Also, the cloud cannot be accessed easily and any time needed due to network traffic and other issues.

- **Absence of map reduces**: Special feature of the grid gain engine which is concerned for dynamic scheduling of jobs among the available nodes.
- **Security**: No security is provided for accessing the clouds.

This paper focuses on segregating legitimate from malicious, authenticating the users, categorising the users based on their behaviour and improving the performance of the environment in a multi-cloud deployment model. Analytical results seem to enhance the security services and also the performance factors such as resource utilizations and cost.

The proposed work is organised as follows: Section 2 analyses the in-field related work. Section 3 introduces the overview of the newly proposed approach. Section 4 elaborates on the detailed description of the work. Section 5 showcases the results obtained in the real-time deployments. Section 6 briefs the advantages of the proposed approach and Section 9 concludes the work.

Related Work

The problem of authenticating users and authorizing them to access variety of resources and services provided by the Cloud Service Providers (CSP) in multicloud environment are studied extensively. The various methodologies and schemes are proposed to secure the cloud infrastructure in [1-4]. The users in wireless LAN are authenticated using Service set identifier [5] and based on the behaviour of the existing users credits are assigned to authorize them to access the cloud resources [6]. The various authentication mechanisms are proposed to secure multicloud in [7-11]. To improve the performance of cloud services, Energy-efficient algorithm for dynamic consolidation of Virtual machine [12], scheduling policy for compute-intensive workflow applications in multi-tenant cloud computing environments [13], Efficient workload allocation to reduce delay and power consumption [14], fault tolerant mechanism for virtual machine [15], task allocation method for minimizing execution time and energy has proposed in [16].

Unlike most existing proposed solutions, we authenticate users separately from wire and wire free networks. To authorize the users to access the cloud resources, we assign the credits based on their behaviour. We also focus on improving the performance, cost, availability, interoperability, and throughput while providing secure cloud environment to the legitimate users.

Proposed Mechanism–User Authentication Framework

The Proposed user authentication framework focuses on user authentication followed by performance metrics. Framework operates at three different phases, as shown in Figure 1. Identified phases are:

- Phase I: Identifying the working environment
- Phase II: Assigning behaviour based credits
- Phase III: Enhancing performance metrics in multi-cloud

Individual phases of the proposed model is explained in detail in the following section.

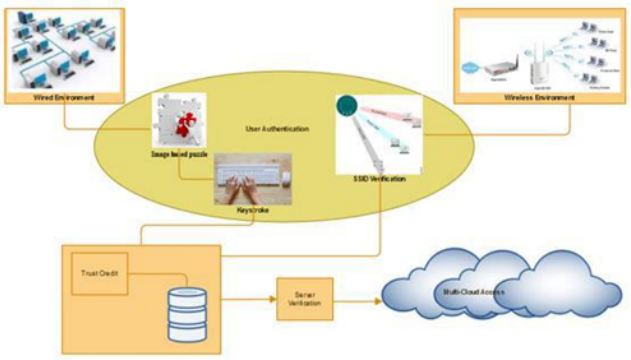

Figure 1: Architecture of the proposed user authentication mechanism

Phase I: Authenticating the user based on environment

Users are authenticated based on the environment they work. This phase has three major steps as shown in Figure 2.

- Step 1: Identifying the Working Environment
- Step 2: User Authentication in Wired Environment
- Step 3: User Authentication in Wireless Environment

Step 1: Identifying Working Environment

Work environment is segregated with the incoming user's request. As a normal procedure, users are logging into their systems with well-known login credentials. Router discriminates the incoming packet as if it arises from either wired or wireless environment. The packet header protocol aids us to identify the type of network. This discrimination is executed only for simplicity and to reduce the processing complexity. Upon identification, different mechanisms were adopted.

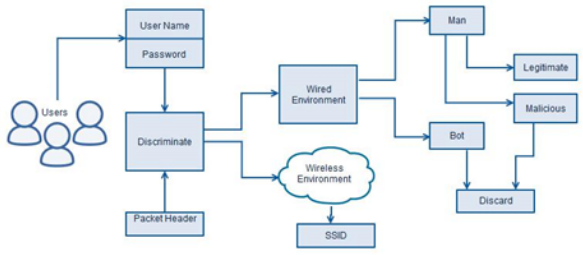

Figure 2: User authentication based on the working environment

Step 2: Authenticating User at Wired Environment

Wired connection transactions are more secure than wireless connection. Hence it is more than enough to identify the user as a man or a machine. Man and machine separation is done with the very simple logical testing, an improved CAPTCHA known as

SILTCHA, uses both sentence and image. Real-time implication, tested with 50 users, proved that the proposed methodology serves the requirement better. After dislocating machine from man, it is more important to discriminate the legitimate users from ill-minded users as shown in Figure 3.

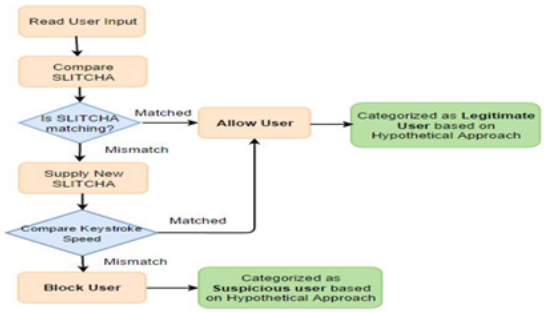

Figure 3: User segregation based on puzzle solving and key stroke

User segregation is possible with the number of requests over a period of time. It is assumed that attackers raise multiple requests without waiting for response i.e. lesser the interval between tickets, intention is bad. To a granular level, this has been enhanced with a key press speed.

Step 3: User Authentication in Wireless Environment

Wireless environment is less secure than wired network due to its shared medium. Service Set Identifier (SSID) helps to identify the network from where the request is initiated. Within the infrastructure, there could be multiple network settings. It is the responsibility of SSID to identify the network attached with. The address space of single IPV4 address can be used to design the network for the system in the company. The network device like routers, virtual router and gateway translate the Internet Service Providers (ISP) IP to private IP using Network Address Translator (NAT) as per the required number of systems in the company. The access to the private network can be made secure by using Wireless Enabled Protocol (WEP), Wireless Protected Access Pre-Shared Key (WPA2) authentication and encryption techniques. Some companies even secure their network by using Hidden Service Set Identifier (SSID) which does not broadcast the SSID. So that intruder cannot catch the network easily. All these techniques are vulnerable to Brute Force attack and some hacking commands. In this paper, the encryption of Service Set Identifier is made to prevent the access of network from intruders. This makes the intruder hard to get the decrypted SSID without knowing the algorithm used and its preshared key. The network device used for NAT maintains access list of system's with its Media Access Control address to allow them to connect in the private network. The addition of encryption of SSID and maintaining access list increases the complexity to secure the connectivity in the private network.

Phase II: Assigning behaviour based credits

Users are authenticated depending on the credits. Based on the traffic flow (in the case of network level attack) and next on the interval between consequent service requests (in the case of service level attack). Credits are given to users based on this authentication upon which services are provisioned accordingly.

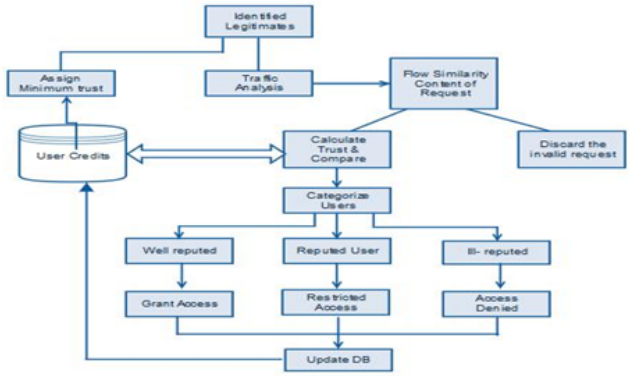

Figure 4: Behaviour Based User Access Grant

As shown in Figure 4, the proposed solution protects the CSP resources from the threat of Network Level as well as Service Level DDoS attacks. In Network Level attacks, the target will be flooded with numerous invalid illegitimate requests. Such requests are comparatively easier to discriminate from legitimate requests. But, in Service Level attack, the attacker floods the target with 'legitimate-like' requests and such request will have all traits similar to that of a legitimate request. It is observed that only the user behaviour can be used as a criterion to detect this kind of attack.

The approach is an authentication based approach that classifies the users into 3 ranks of reputation, *viz.* well-reputed, reputed and ill-reputed. The users are given credits for this classification. The lower limit of credit is L_VALUE and the upper limit is H_VALUE. Initially, all users are given a credit equal to M_VALUE which is the mean of L_VALUE & H_VALUE. P_VALUE, a predetermined value (L_VALUE<P_VALUE<H_VALUE) is the deciding factor for reputation. Those users who acquired credit value greater than P_VALUE are designated as well reputed and are given full access to CSP resources. The users with credit value between L_VALUE and P_VALUE are given limited access by classifying them under group reputed. Others whose credit is less than L_VALUE are blocked and blacklisted.

The attackers form botnets by compromising vulnerable systems distributed across the network and installs malicious program codes in those systems. This can happen with or without the knowledge of that system. Whatever the case may, the instructions in such codes will make the systems to send requests to flood the target server. So, it is assumed that these request patterns will exhibit signs of similarity as they are the result of same program code installed in all zombies. This is our assumption used to defend Network-Level DDoS Attack.

Again, as it is the same program code or bot master that triggers all zombies, there will be a periodicity in the inter-arrival

time between consequent requests from a user. This is used as an assumption to defend against Service Level DDoS Attack.

Phase III: Enhancing performance metrics in multi-cloud

The simultaneous use of multiple clouds can provide several potential benefits, such as high availability, fault tolerance and reduced infrastructural cost. The model proposed which is the implementation of a secured multi-cloud virtual infrastructure consists of a grid engine on top of the multi-cloud infrastructure to distribute the task among the worker nodes that are supplied with various resources from different clouds to enhance cost efficiency of the infrastructure set up and also to implement high availability feature. The Oracle grid engine is used to schedule the jobs to the worker nodes (in-house and cloud). Worker nodes will be acting like listeners to receive the job from the Oracle grid engine master node. The Client after proper authentication procedure submits the job to the grid gain engine. Access control is a key concern as attacks by hackers are of a great risk. A potential hacker can be someone with approved access to the cloud. Job specified in this implementation is the Monte Carlo simulation (MCS) for calculating credit risk.

MCS performs risk analysis by generating models of possible results, substituting a range of values using probability distribution. Based on the range of estimations a random value is selected for each task. Calculation is done on this random value. The result is recorded and the process is repeated. The calculations are performed hundreds or thousands of times with each time using different randomly selected values. On completion, the simulation yields a large pool of results that are used to describe the probability of reaching various results in the model.

Oracle Grid Engine (OGE) is used to schedule [17] and dispatch jobs to the cloud with help of its special feature known as Map Reduce. When the client submits a job request, it is handled by the master node in the Grid Engine. In case of failure of master node, one shadow master will take charge. A monitor is always analysing the performance of Master host and Execution host.

Worker nodes acts as listeners for receiving jobs submitted by clients through OGE, where in the jobs are scheduled in the order of priority and job types. The simultaneous tasks are executed in different nodes which are deployed in-house or remotely. A different cluster configuration is maintained. The cloud providers or the external sites in this work are Amazon EC2 and Rackspace. Client must need an account with these cloud providers and the users have to pay on need basis for using the cloud infrastructure. AES algorithm [18] is used for secured data transfer [19,20] while accessing the cloud.

From worker node, the user will be programmatically accessing the Rackspace (through RMI) and Amazon (through HTTP request) cloud computing infrastructure in which the cloud exposes API. From the worker node, the user will be programmatically accessing the Rackspace (through RMI) and Amazon (through HTTP request) cloud computing infrastructure, in which the cloud exposes API. The steps following for accessing the cloud are Launch and control cloud servers, programmatically using a RESTful API, Assign server instances custom metadata using own key/value pairs, Reboot servers from any image specified, Create custom images and schedule backups of the cloud servers.(Figure 5)

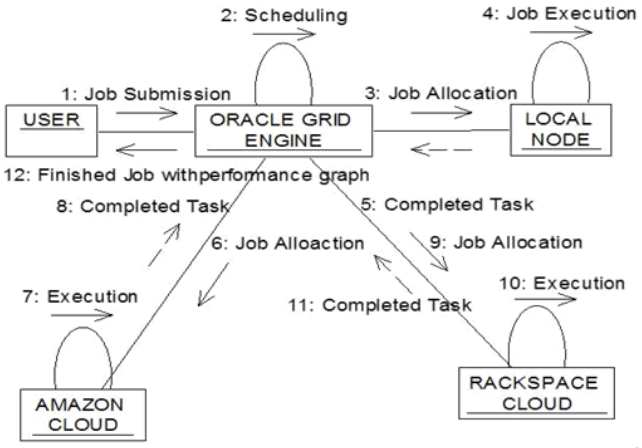

Figure 5: Performance enhancement architecture

Performance and Result Analysis

An experimental study consisted of 100 SILTCHA challenges that were created and presented to the 50 users. They were to solve as many as they could in one minute which averaged to 13 SILTCHAS per minute. The users out of 650 attempts solved 597 correctly (~92%). The failure rate was caused due to inability to associate the correct form of the word to match the image and also a very few cases where the text was unreadable by the user.

Table: 1 [2] presents the comparison among the various CAPTCHA with SILTCHA systems available based on different parameters.

Table 1: Comparison of various CAPTCHA systems and how SILTCHA fares against them

Parameter	Image Base	Math Base	Video	Re-CAPTCHA	SILTCHA
Security	Average	High	Average	High	High
Ease of Use	Easy	Hard	Hard	Hard	Average
Bandwidth Usage	~8 KB	~5 KB	~600 KB	~5 KB	~12 KB
Time to Solve	Depend	~10 s	~15 s	~8 s	~5 s
Challenges to Solve	Depend	1	1	2	1

The traffic at Data Center includes the requests from legitimate users as well as attackers. This will contribute to flooding. The proposed system has completely eliminated the requests from ill-reputed users whereas the well- reputed users

are given full access as before. As shown in Figure 6, the users 2 and 6 have submitted 500 tasks per second and user 9 and 10 has submitted about 250 tasks per second. The users 3 and 5 have also submitted around 100 requests per seconds.

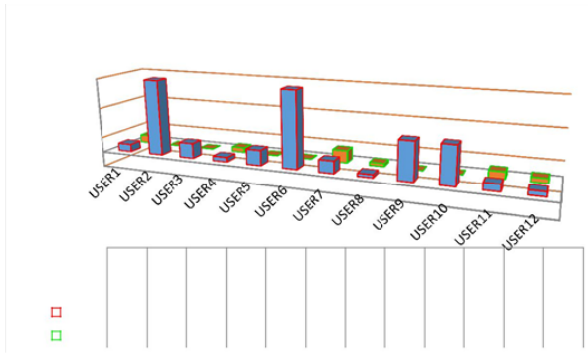

Figure 6: Traffic at the Datacenter before and After

The graph in Figure 7 depicts that well-reputed users such as users 1, 4, 7, 8, 11 and 12 are given full access to CSP resources. The users 3 and 5 who are suspicious are given limited access to resources whereas the users 2, 6, 9 and 10 are completely blocked from accessing the CSP resources. Earlier the users were given random resource allocation due to which well-reputed users also faced inefficient service delivery from CSP.

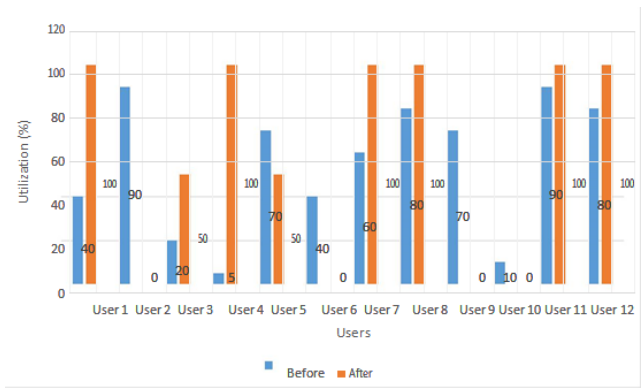

Figure 7: Resource Utilization based on credits

Processing cost

The processing cost here means the cost incurred at each Data Center in processing the requests from all users. The processing cost at each Data Center has decreased tremendously after the proposed method has been applied. Instead of giving as much task as possible to one Data Center, the load is distributed among the Data Centers which will, in turn, lessen the response time for serving clients requests. As shown in Figure 8, earlier only Data Centers 1 and 2 does all the processing and other DCs were idle. But, after implementing our proposed solution, all Data Centers contributed to CSP service delivery and hence helped in enhanced performance and reduced response time.

Figure 8: Processing Cost per Data Center

Once the task is completed by each worker node it is then gathered and given back to the user. Table 2 clearly shows the results for the implementation of multi-cloud virtual infrastructure. It denotes the node type, the time taken for simulation by each node in milliseconds (ms), the number of iterations for each node and finally the total time taken for the given 10000 iterations in milliseconds. This resultant values will not be constant every time since it depends upon the network and dynamic scheduling done by the Map Reduce of the grid gain engine. (Figure 9)

Table 2: Time taken to execute Monte-Carlo Simulation in cluster nodes

Node Type	Time taken for simulation (ms)	Number of iterations	Total time taken for 10000 iterations (ms)
Rackspace	3619	3333	22.439
Amazon	2380	3333	22.439
In-house node	1934	3334	22.439

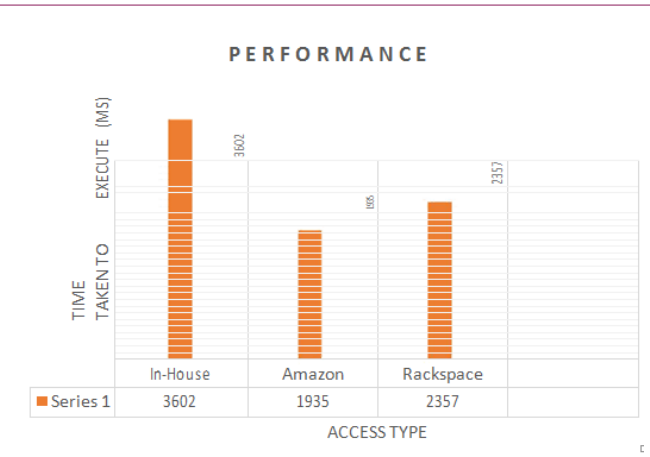

Figure 9: Performance in Multi-cloud environment

Performance analysis

Performance analysis [21] is been done for individual nodes such as in-house node–Figure 10, Amazon–Figure 11 and Rack space for three rounds, Figure 12. The study reveals that the throughput, i.e, the number of jobs executed per second varies for each round and also the throughput is high in the case of the combination of in-house, Amazon and Rackspace nodes indicating that performance is high in the case of multi-cloud deployment rather than using a single cloud.

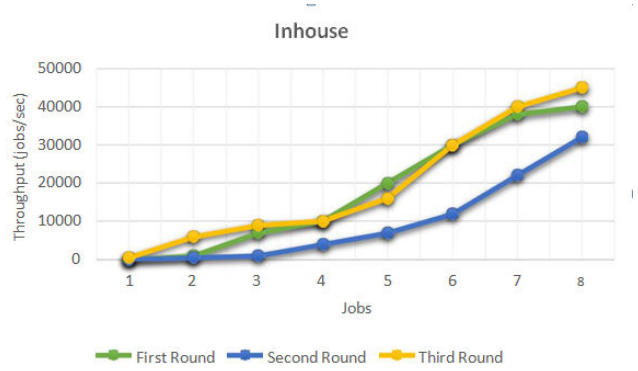

Figure 10: Performance graph for in-house node

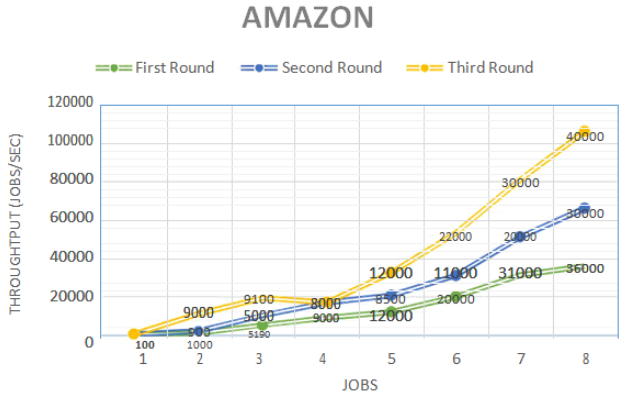

Figure 11: Performance graph for Amazon node

The cost analysis [22] is also been done along with the performance analysis since cost plays a vital impact for setting up a multi-cloud infrastructure. A comparative study is done with the three nodes namely In-House Node (IHN), Amazon Cloud (AC) and Rackspace Cloud (RC). The result of the study states that performance increases by using multi node deployment rather than using a single node. The higher the number of nodes, the higher the performance is, shown in Figures 10-12.

Number of node α performance. It is important to analyse, not only the total cost of the infrastructure, but also the ratio between performance and cost, in order to find the most optimal configurations. In spite of the higher cost of cloud resources with respect to in-house nodes, the other configurations exhibit better performance cost ratio than in-house node.

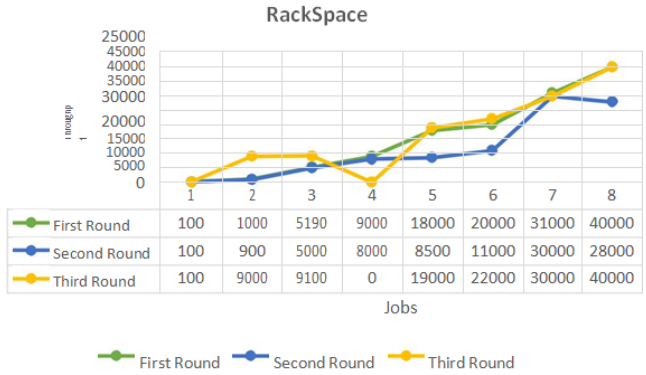

Figure 12: Performance graph for Rackspace node

This proves that the proposed multi-cloud implementation is an efficient and effective solution, not only from the performance point of view, but also from the cost perspective, as shown in Figure 13.

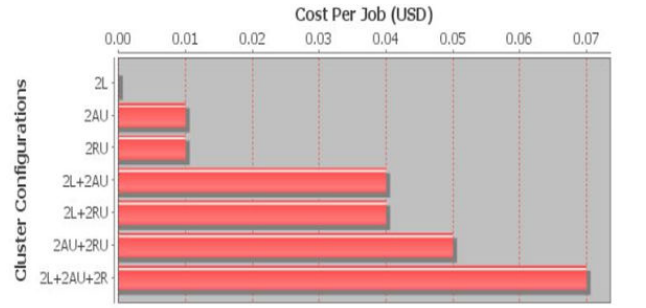

Figure 13: Graph representing Cost for each nodes

Conclusion

In **Phase 1**, work environment has been successfully classified into wired or wireless using packet header information. Separate authentication mechanisms were proposed and tested for wired and wireless networks, only to reduce the processing complexity. Authentication mechanisms best suit the network type and could serve the purpose very well.

In **Phase 2**, user behaviours were captured and analysed. Based on their work art, credits were assigned to them. Users are classified according to their earned credits. Access permissions were granted/denied as per their classification. Our implementation test-bed showed the claim met its specification.

In **Phase 3**, the features, such as high availability and fault tolerance were provided through dynamic allocation of the nodes. The numbers of iterations were equally divided among the nodes and also the architecture supports interoperability. The throughput increases linearly as the number of nodes of clouds inside the cluster increases. As the cloud nodes cause no overhead, it doesn't cause any performance degradation. The hybrid configurations of in-house and remote nodes exhibit better performance-cost ratio proving multi-cloud solution is

good in cost perspective also. Thus the infrastructure cost is also reduced. Hence, this work could improve security without compromising quality.

References

1. Thandeeswaran R, Durai SMA (2016) Wide-ranging survey on authentication mechanisms. Int J App Eng Res 11: 4114-4117.
2. Thandeeswaran R, Durai SMA (2016) Dual phase cloud infrastructure authentication. Int J Comm Net Info Sec 8: 197-202.
3. Thandeeswaran R, Durai SMA (2017) Bi-level user authentication for enriching legitimates and eradicating duplicates (EnEra) in cloud infrastructure. Int J Comp Aided Eng Tech, Inderscience Publisher, In Press.
4. Thandeeswaran R, Subhashini S, Jeyanthi N, Durai SMA (2012) Secured multi-cloud virtual infrastructure with improved performance. Cybernetics Info Tech 12: 11-22.
5. Thandeeswaran R, Ankita, Jeyanthi N (2016) Securing service set identifier of wireless network. Int J Pharma Tech 8: 16605-16610.
6. Jeyanthi N, Shabeeb H, Thandeeswaran R, Durai SMA (2014) RESCUE: Three phase authentication to detect and prevent DDoS attacks in cloud computing environment, Int J Eng Transact B: App 27: 1137-1146.
7. Jeyanthi N, Thandeeswaran R, Vinithra J (2014) RQA based approach to detect and prevent DDoS attacks in VoIP networks, Cybernetics Info Tech 14: 11-24.
8. Rawat A, Singh AK, James J, Jeyanthi N, Thandeeswaran R (2016) RSJ approach for user authentication, ACM International Conference on Advances in Information Communication Technology & Computing, Bikaner.
9. Moreno-Vozmediano R, Montero RS, Llorente IM (2011) Multi-cloud deployment of computing clusters for loosely coupled MTC applications. IEEE computer society, IEEE transact parallel distributed sys 22: 924-930.
10. Demchenko Y, Ham JV, Yakovenko V (2011) On-demand provisioning of cloud and grid based infrastructure services for collaborative projects and groups. In: IEEE conferences, Collab Tech Sys 978: 134-142.
11. Lian Y, Huanga X, Mu Y (2014) SA3: Self-adaptive anonymous authentication for dynamic authentication policies. Fut Gen Comp Sys 30: 133-139.
12. Khoshkholghi MA (2017) Energy-Efficient Algorithms for Dynamic Virtual Machine Consolidation in Cloud Data Centers. IEEE Access.
13. Rimal, Maier (2017) Workflow scheduling in multi-tenant cloud computing environments. IEEE Transact Parallel Distributed Sys 28: 1.
14. Deng (2016) Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption. IEEE Internet Things J 3: 6.
15. Amoon M (2016) Adaptive Framework for Reliable Cloud Computing Environment. IEEE Access 4.
16. Yaqoob I (2016) Heterogeneity-aware task allocation in mobile ad hoc cloud. IEEE Access.
17. Lovesum, DD, SPJA (2011) Novel approach for scheduling service request in cloud with trust monitor Signal Processing, Communication, Comput Networking Tech (ICSCCN) 509-513.
18. Hwang J J, Chuang H K, Hsu Y C, Wu C H (2011) A business model for cloud computing based on a separate encryption and decryption service. In: ICISA Int Conference 1-7.
19. Ray C , Ganguly U (2011) An approach for data privacy in hybrid cloud environment. In: ICCCT 2nd Int Conference 316-320.
20. Han S, Xing J (2011) Ensuring data storage security through a novel third party auditor scheme in cloud computing. In: Cloud Computing and Intelligence Systems (CCIS). IEEE Int Conference 264-268.
21. Montero RS, Moreno-Vozmediano R, IML Lorente (2010) An elasticity model for high throughput computing clusters. J Parallel Distributed Comput.
22. Simarro JLL, Moreno-Vozmediano R, Montero RS, Lorente IML (2011) Dynamic placement of virtual machines for cost optimization in multi-cloud environments. IEEE 1-7.