

A Safe and Secure Access for Distributed Resources for Enterprise Cloud

Anitha K L, T.R. Gopalakrishnan Nair



Abstract: Cloud computing is undergoing a perpetual advancement and new developments through distributed computing approaches and implementation of advanced virtualization technologies within the framework of recent powerful computing and web management systems. As Cloud computing evolves, the organizations can manage their data with small operational expenses. With the use of web services, cloud computing allows access to ubiquitous data storage and utilization of resources. On the other hand, the benefits of cloud computing come along with issues and challenges such as data security, reliability and availability of the resources in the cloud. In this paper, we present the design of a secure Resource Management System to monitor and control the geographically distributed resources in various segments under the enterprise scenario.

Keywords: Network Storage, Resource management, Data Storage, Cloud service provider.

I. INTRODUCTION

Research on the Secure Resource Management System primarily focuses on the deployment models like Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). In IaaS paradigm, providers offer the cloud infrastructure, physical processing, storage networking and the hosting environment for the IaaS consumers so that users can install and monitors the services for the IT infrastructure operations. The PaaS provider provisions and manages cloud infrastructure and middleware for the platform consumers so that the user can develop, test, deploy and manage their applications hosted in a cloud system. The SaaS provider installs, operates and maintains the applications hosted in the cloud. The SaaS users can use the application for business process operations. In the early days Hwa-Chun Lin [1] proposed a Web-based distributed network management architecture in which the HTTP protocol is used for console server and server-server communications such that network management server requires minimum system resources such as computation power, memory, disk space, etc. It is of particular importance

when a network management server is to be embedded. Louay Karadsheh [2] checks the risks came across by implementing Infrastructure-as-a-Service (IaaS) model and talked about the job of security policies, Service Level Agreement (SLA) and compliance for enhancing the security of the IaaS Service. Also, this paper discusses the possibilities of applying various types of security policies for enhancing the security level of IaaS to satisfactory, but they do not offer a Security Policy. Vaquero et al. [3] examine the security risks that multi-tenancy tempts the Infrastructure-as-a-Service clouds and present the mainly significant threats and significant state of the art of results. Also, in the same paper they continue analyzing the open security issues and challenges that should be addressed. Subashini and Kavitha [4] describe the common security issues posed by the Cloud Service Delivery Models and the security threats posed by the IaaS Delivery Model, but they do not provide a comprehensive analysis of the specific threats to be addressed by Cloud Providers.

II. VIRTUALIZATION

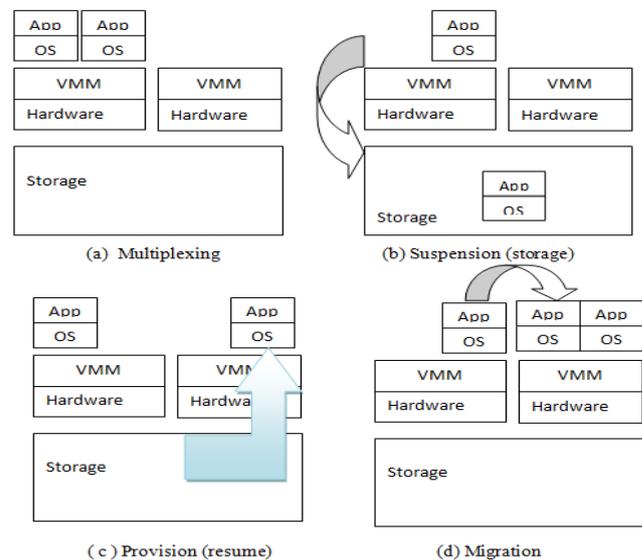


Fig. 1: VM multiplexing, suspension, provision, and migration in a distributed computing environment [5].
The VMs can be multiplexed, between hardware machines, a VM can be suspended and stored in stable storage, a suspended VM can be resumed or provisioned to a new hardware platform, and Virtual Machines can be migrated, from one hardware platform to another.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

Anitha K L*, Bharathiar University, Coimbatore, India. Email: anithakl07@gmail.com

T.R. Gopalakrishnan Nair, Networks and Security Research Group, Advanced Research Centre, Rajarajeswari Group of Institutions, India. Email: trgnair@gmail.com

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

These VM operations allow a VM to be provisioned to any available hardware platform. Also, the VM approach will extensively enhance the utilization of server resources. Multiple server functions can be consolidated on the same hardware to achieve higher system efficiency which eliminates server sprawl via deployment of systems as VMs, which enable transparency to the shared device.

Virtualization can be implemented, at various levels of System architecture [6]. Network Virtualization entails virtual IP management and segmentation. Memory Virtualization requires the aggregation of memory resources into a pool of single memory and managing the memory on behalf of the multiple applications using it. Storage Virtualization provides a layer of abstraction for the physical storage of data at the device level called as block virtualization or at the file level referred to as file virtualization. Block virtualization includes technologies such as storage area network (SAN) and network-attached storage (NAS) that can efficiently manage storage in a central location for multiple applications across the network rather than requiring the applications to manage their storage on a physically attached device. Processor Virtualization enables a processor to be shared across multiple application instances. Storage virtualization was widely used to describe the aggregation and to repartition of disks at very coarse time scales for use by physical machines. In a virtual environment, virtual storage includes the storage managed by VMMs and resident operating system. Meyer D, et al. [7] proposed Parallax which is scalable and especially suitable for use in cluster-based environments. To handle storage management easily, a cluster-wide administrative domain which manages the entire storage appliance VMs that connects the physical hardware device for block and network access. The storage appliance VM allowed functionality that is currently implemented in data-center hardware to be pushed out and applied on individual hosts. This system enabled advanced storage features such as snapshot facilities to be implemented in software and delivered above commodity network storage targets. Parallax uses Xen's block tap driver to handle block requests, and it is applied as a tapdisk library. This library acts as a single block virtualization service for all client VMs on the same physical host. Parallax is a set of per-host storage appliances that share access to a common block device and presents virtual disks to client VM.

III. CLOUD STORAGE

Data storage is the holding of data in an electromagnetic form for access by a computer processor. Hierarchical storage management (HSM) is a data storage technique, which automatically moves data between high-cost and low-cost storage media. HSM systems exist because of high-speed storage devices, such as hard disk drive arrays, are more expensive (per byte stored) than slower devices, such as optical discs and magnetic tape drives. While it would be ideal to have all data available on high-speed devices all the time, this is expensive for many organizations. Instead, HSM systems store the bulk of the enterprise's data on slower devices and then copy data to faster disk drives when needed. In effect, HSM turns the fast disk drives into caches for the slower mass storage devices. The HSM system monitors the way data is used and makes best guesses as to which data can

be, safely moved to slower devices and which data should stay on the active devices [8].

The advantages of HSM technology include [9]:

- A large amount of data can be stored in a relatively small storage space.
- Reduced data storage costs.
- Simplified data retrieval from lower level devices.
- Transparency

Storage security deals with any security around the storage architecture and the data stored on it. Regarding data we need to think about how the data is created, where it has been stored, and the value assigned to the data and most important the security of the data. We can use Storage Area Network (SAN) or Network Attached Storage (NAS) or any other product to store the data wherein the security needs of a type of data must reflect the value of that data. Therefore, data storage security is a challenging part of any organization. We need to think about the confidentiality, integrity and availability of data. Regarding technical solutions, enterprise organizations have to decide whether data needs to be encrypted or not. Typically, data should be encrypted when it is at rest and in motion. Therefore we need to think about encryption key management, access control visibility for the user for accessing the data at any given stage, duplication of data, disaster recovery. Enterprise should ensure that the data should be available at any time wherein the stored data does not impose on security if you need to access the data at short notice. Cloud storage means storing data online so that we can access it from any computing device without actually carrying the data servers with us. Cloud storage can be classified, into four types: Mobile Cloud Storage: This is a type of cloud storage that we use in our daily life. We use Android and i-phone these days, for our safety we have already synced our phones online so that even if our phone is lost, we can backup it on the new device anytime as per our convenience. Public Cloud Storage: In this type, the user uses a publicly available cloud wherein the user can avail the services by either rented or subscribed for a period of time. The user can access the data from anywhere by using the login credentials.

Private Cloud Storage: In private cloud storage the company sets up the data center and the cloud storage services, in the user's allocated space. The primary motive behind having privately available cloud storage is the necessity of a secure platform and private access to the data.

Hybrid Cloud Storage: In this case, the data is available publicly, but some parts of the data are private and hence are restricted to some users only. Therefore, this is an on and off model where it can be switched from public to private or private to the public anytime as per user's convenience [10].

Advantages of Cloud Storage

- Data can be accessible from anywhere from any computing devices.
- Increased work efficiency.
- Reduces cost of operations.
- Remote data backups as per user convenience.
- Reduces the costs to set up the disaster recovery and backup units.

Disadvantages of Cloud Storage

- Increased usage of bandwidth to access the data that increases the costs of operations a bit.
- Internet connection is not having a high speed; you might not be able to access the data [10].

Table- I: various types of operating systems.

Operating Systems	Administration	Resources
Desktop Operating System	Local machine administration only	Manages internal resources like memory, CPU, io, etc.
Server Operating System	Centralized Administration	Manages network resources along with internal resources.
Cloud Operating System	Operate within cloud computing and virtualization environments	Manages the operation of one or more virtual machines, within a virtualized environment.

Cloud Computing enables Internet-based computing wherein you can run the virtual application within a browser from any location at any time. Table I shows the different types of operating systems. Cloud computing enable enterprises improved use IT resources to enhance flexibility and performance. The user can run virtual applications and can compute the data within a browser from anywhere. This cloud-based approach helps the enterprises to access the computing resource at any time. The operating system has to be designed to develop the cloud platform in such a way that the end user gets benefited by balanced workloads that can scale in a safe manner. VMs add complexity to the storage environment. Virtualization revolves around multiple virtual machines (VMs) sharing physical resources. Virtualization file systems, such as VMware's VMFS, let several physical servers simultaneously read and write to the same LUNs. It is enabled by a unique locking mechanism that ensures that multiple hosts have exclusive access to each of their VMs on a shared LUN. Adding to the complexity of the environment are high availability and workload load balancing across virtualization clusters. Besides, VMware's vMotion and Storage vMotion can move running VMs across hosts and storage devices, respectively. The features that allow for the movement of VMs can also cause problems for storage and virtualization managers, because of the dynamic nature of the relationships among VMs, their physical hosts and the storage device in which their virtual disk resides. These relationships have the greatest impact on troubleshooting and performance monitoring. Neither the storage administrator nor the virtualization administrator can see what occurs at the virtualization layer and the storage layer, respectively; as a result, neither the administrator can see the overarching picture [11]. An accurate task scheduling mechanism is necessary to minimize execution time and to improve the efficiency in cloud computing. Tasks can be scheduled by specifying a particular resource from all the available resources in order that run the efficiency of the computing environment enlarges [12]. A modeling and performance

evaluation of hierarchical job scheduling is described in [13], and in a web service-oriented grid authors [14] offered a novel stochastic algorithm for QoS-constrained workflows job scheduling.

IV. SECURE RESOURCE MANAGEMENT SYSTEM

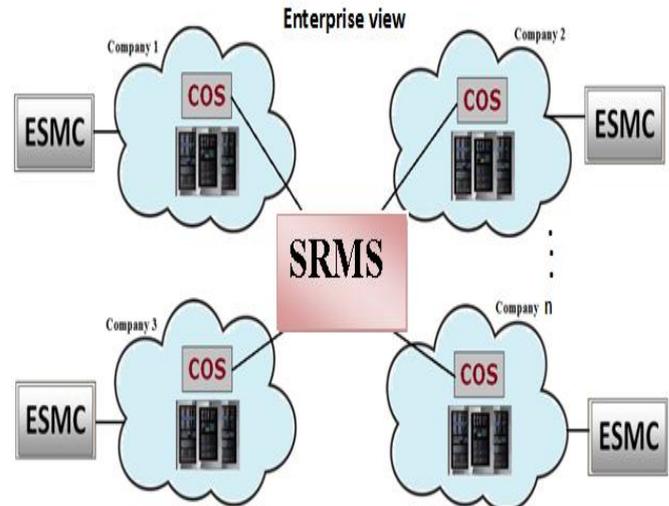


Fig. 2: Secure Resource Management System (SRMS).

A. System Model

The model for Secure Resource Management System (SRMS) is shown in Fig. 2. Consider there are n companies under the same organization. Each company has a Cloud Operating System (COS) and data centers wherein it is connected to its enterprise sub unit management center (ESMC). The jobs are categorized into two: local jobs and global jobs. The local jobs will be carried out in the enterprise sub unit management centre itself. The global jobs will be performed, by sharing the resources globally. A secured centralized job when it is getting distributed it will go to unsecured level. This is because, there is no de-facto agreement or quantifiable security level at all companies getting connected with the main system for combined operations. Some jobs can be accessible to the public also. So we need to think about the security measurements taken in this distributed environment. In enterprise cloud computing jobs can be randomly generated, demand-driven configuration. There is a finite set of mutually excluding unique and independent features that implements cloud management system effectively with maximum efficiency. They include:

- On demand scalability of the cloud maintaining management consistency.
- Tracking analytics of performance on a real time mode for deeper visibility.
- Validating the compliance adherence and creating reports.

- d) Cloud management system must quantitatively and qualitatively access the performance in parameters like bandwidth, data domain, bottlenecks etc.
- e) Cloud management system must have capability and compatibility to interact and expand across clouds.

The security concern is pertinent interconnected towards the network, storage and the resources which are geographically distributed, across various companies under the same organization. You have to define the policies for its access, data transport over network, etc. SRMS provides uniform access to the resources and monitor and controls the resources which are located geographically. The virtual machine has more power in handling storage. VM map of storage can be classified into: physically migrate and logically coupled. In logically coupled VM map of storage, segments can be coupled. i.e., segment one and segment two will be coupled. We can add more power to the VMs for handling user request for expansion of storage. SRMS is an interconnection of Cloud Operating Systems thereby provides high availability for the resources. It enforces active and dynamic resource mapping across multiple cloud operating system and enterprise sub unit management centers.

B. Protocols of security for resource attachment and detachment in SRMS

1. Security Management

In order to access the resources which are geographically located, the user needs to be authenticated. Fig. 3 shows the user authentication for the secure resource management system. To access the Secure Resource Management System, the user from one company has to send the security credential information like User ID, Company logo, digital signature and an email id to SRMS. SRMS accepts these security credentials and generates a token which is sent to the user. Now the user can login to SRMS by using the token and can access for the resource which is not there in their company. This token is vital for allocating the target resources for the user from elsewhere in the enterprise. SRMS verifies the token and the requested resource will be given to the company if it is available. Thereby SRMS prevents unauthorized access of the resources in an enterprise system.

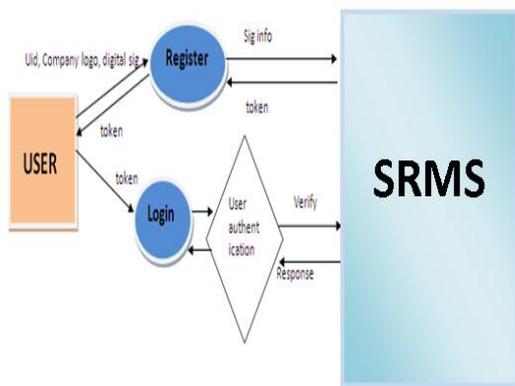


Fig. 3: User Authentication for SRMS

Resource Cluster consists of various resources like virtual machine, communication channel, memory etc. We need to analyze the security of service while allocating and

reallocating the resources in the cloud operating system. A fixed path can be provided through the security driven software. Operational consistency needs to be maintained while allocating the resources from geographically distributed resources. SRMS is responsible to examine the dynamic pool of resources in various companies which are geographically apart. User can submit the local computing jobs directly to the ESMC. Local jobs can be processed in the ESMC and the global jobs are processed globally through SRMS. Consequently any enterprise sub unit management centre consists of local jobs and the global jobs from other company where there is a lack of resources needed to execute the job. SRMS takes the decision to allocate the jobs to different companies. Each company has a Cloud Operating System which contains the information about the resources like available memory, CPU speed, virtual machine etc.

Given a set C of companies and a set S of sub unit offices where in each enterprise sub unit management centre has local and global jobs. Local jobs will be taken care by the ESMC itself. Global job needs the resources which can be used from different companies under the same geographic area. Thereby the resources can be shared as per customer demand from the company so as to minimize cost. All customer demand d_i must be satisfied, and each resource has a demand capacity limit L. Let $y_j=1$ represent choosing company C to use a resource j and 0 otherwise. Also let $t_{ij}=1$ represent the task of user i to resource j, and 0 otherwise. This model can be formulated as the following integer linear program for global jobs as:

$$\text{Total cost} = \min \sum_{i \in S} \sum_{j \in C} [R_{ij} \text{ AND } t_{ij}] + \sum_{j \in C} f_j y_j \quad (1)$$

Subject to

$$\sum_{j \in C} t_{ij} = 1 \quad \forall i \in S \quad (2)$$

$$x_{ij} \leq y_j \quad \forall i \in S, j \in C \quad (3)$$

$$\sum_{i \in S} d_i t_{ij} \leq L y_j \quad \forall j \in C \quad (4)$$

$$t_{ij} \in \{0, 1\} \quad \forall i \in S, j \in C$$

$$y_j \in \{0, 1\} \quad \forall j \in C$$

The objective function (1) describes the total cost is the sum of the usage of resources R_{ij} between resource j from company C and its assigned user i from enterprise sub unit management centre S plus a fixed charge f_j for assigning a resource j to the subunit office from company C. The equation (2) ensures that each user is assigned to access a resource from any one company under same geo-graphic area based on availability of resources at any time. (3), ensures a user to execute a task if company C has the required resource. And (4) depicts the capacity limit at each company.

The resources can be processor, memory and communication channel. Then fixed charge for a particular resource is calculated by the unit price of the resources:



$$f_j = UP_{Ri} * N_{Ri} + UM_{Ri} * M_{Ri} + UC_{Ri} * NC_{Ri} \quad (5)$$

$$ixed\ cost = \sum_{i \in R0}^{Rn} (UP_{Ri} * NP_{Ri} + UM_{Ri} * NM_{Ri} + UC_{Ri} * NC_{Ri}) \quad (6)$$

If the tasks can be done locally, then there will be no cost for accessing the resource. The m resources are mapped under the rules and regulations of resource sharing. But maintaining security between resource clusters and the cloud operating system as well as intra COS is studied in this paper. Resource cluster will have challenge response protocol wherein a security key (Sk) is maintained for the resources in each company. SRMS has the information about Sk and the availability of the resources. To avoid communication overhead, the location information of every ESMC and COS will be stored in SRMS. Upon receiving the request for the resource from one company under the same geographic area, SRMS allocates the available resources to the trusted COS and the state of the resource is recorded. Thereby the process can be executed without any delay. It is a tightly coupled security between resource cluster and COS. Resources are switchable under the command and control by the operator. The status of the resources is updated dynamically in SRMS which allows the user to make use of the resources which is not available in their company. Instead of putting capital expenses, the resources can be shared under the same geographic area.

Table- II: Resource Table

RT			
C	S	R	A
C1	Sk1	R1	1
		R2	0
		.	.
		Rn	1
C2	Sk2	R1	1
		R2	1
		.	.
		Rn	1
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
Cm	Skk	R1	1
		R2	1
		.	.
		Rn	1

Here we use Resource Table (RT) to perform dynamic update operations for the resources.

RT consists of four main components:

- (i) Company index (C)
- (ii) Resource index (R)
- (iii) Security Key (S)
- (iv) Availability (A)

Status Table (ST) consists of user id (U), company id of the user (C), task (T), Allocation Index (Ai) and the availability (A). Status Table records the information about the user who

is accessing the resource for executing the task.

Availability (A) indicates the availability of the resources by the value 0 and 1. If a user from one company is accessing a resource at a particular point of time Ai value changes from 1 to 0. That shows the resource is not available. When that user releases the resource, A value change back to the original state and the RT will be updated dynamically.

$$A = \begin{cases} 1 & \text{use R,} \\ 0 & \text{Otherwise} \end{cases}$$

Table- III: Status table

ST				
U	C	T	Ai	A
u1	C2	t1	C1R2S1	1

A Security Key (Sk) is provided for accessing the resource for each company and will be recorded in the status table. Only the authenticated user who has already registered to SRMS can only access the resources from the companies under the same geo-graphic area. Fig. 4 shows a security driven model for the cloud operating system and the resource cluster. The resources can be accessed based on the level of the security.

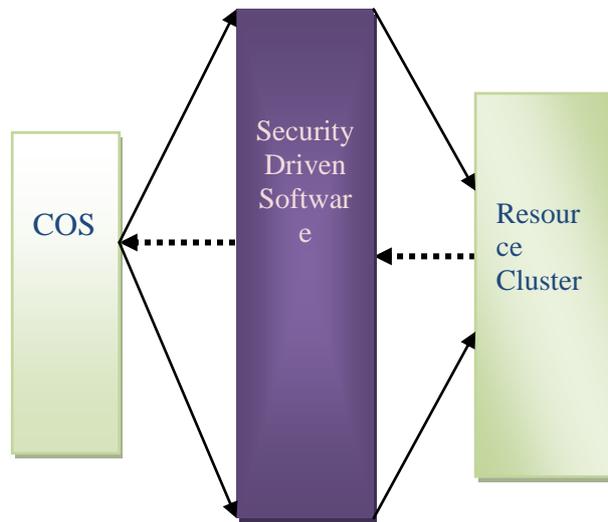


Fig. 4: Security driven model for COS and Resource Cluster.

A security policy addresses several different users with diverse expectations. Each group users, owners, and beneficiaries uses the security policy in a different way. Therefore, the security driven software can be modeled for 3 levels of security like common level security, medium level security and superior level security. A normal user can access the notifications which are made public by common level security. A department level user is identified as a company employee by user authentication and can access the data and resources in a medium level security. For superior level security user authentication will be done using the token as a security key and each company is maintaining the same security key to share the resources to authenticated users. If a user wants to access the shared resource he has to login using the token and can access the resource.

Data centers hold the greater part of valuable data and information. Even data centers contain sensitive data which is the main aim of attackers and which need high level of security.

2. Resource Management

Let us assume there are 4 companies C1, C2, C3, C4 and each company is having 4 resources. Thus we get C x R matrix. Cm x Rn. ie, R1, R2,.. Rn is attached to C1. These resources are mapped into Secure Resource Management System.

	R			
C	C1R1	C1R2	C1R3	C1R4
	C2R1	C2R2	C2R3	C2R4
	C3R1	C3R2	C3R3	C3R4
	C4R1	C4R2	C4R3	C4R4

SRMS maintains a Resource Table and a Status Table in order to know the state of the resources of each company wherein we use Hungarian method [15] to find out the cost of assigning the resources based on availability to perform the task. By using this method we can find an optimal assignment to perform efficient load balancing based on the dynamic user requests. Let us assume that we have n available resources from various company and n global jobs. Then we get an n x n cost matrix. Analytical Model: Let $c_{i,j}$ be the cost of assigning the i th resource to the j th job. We define the cost matrix to be the $n \times n$ matrix

$$C = \begin{matrix} C_{1,1} & C_{1,2} & \dots & C_{1,n} \\ C_{2,1} & C_{2,2} & \dots & C_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ C_{n,1} & C_{n,2} & \dots & C_{n,n} \end{matrix}$$

The Hungarian method is an algorithm which finds an optimal assignment for a given cost matrix. Let us consider that we have 4 available resources from various company and 4 global jobs need to be executed. Then we get a 4 x 4 cost matrix. The cost of assigning a resource to a particular job is shown in the matrix below.

R/J	J1	J2	J3	J4
R1	120	40	65	82
R2	25	65	33	41
R3	13	28	86	75
R4	93	56	33	18

Cost matrix=

Follow the steps to minimize the total cost.

1. Subtract row minima: subtract smallest cost from each row.

R/J	J1	J2	J3	J4
R1	80	0	25	42
R2	0	40	8	16
R3	0	15	73	62

R4	75	38	15	0
----	----	----	----	---

2. Subtract column minima: subtract smallest cost from each column

R/J	J1	J2	J3	J4
R1	80	0	17	42
R2	0	40	0	16
R3	0	15	65	62
R4	75	38	7	0

3. Cover all zeros with a minimum number of lines.

R/J	J1	J2	J3	J4
R1	80	0	17	42
R2	0	40	0	16
R3	0	15	65	62
R4	75	38	7	0

4. The optimal assignment

R/J	J1	J2	J3	J4
R1	80	0	17	42
R2	0	40	0	16
R3	0	15	65	62
R4	75	38	7	0

5. Zeros corresponds to the following optimal assignment in the original cost matrix

R/J	J1	J2	J3	J4
R1	120	40	65	82
R2	25	65	33	41
R3	13	28	86	75
R4	93	56	33	18

The resources are assigned to execute the global jobs by minimizing the cost.

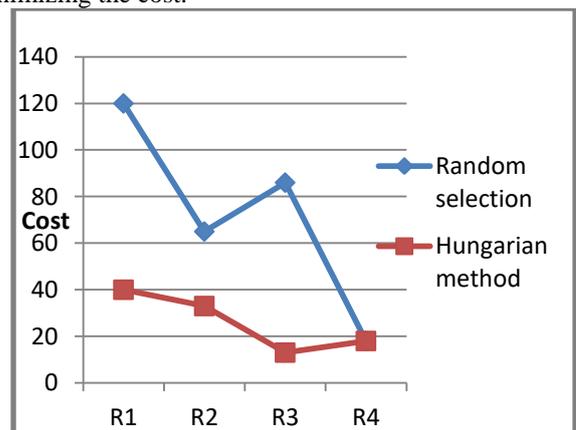


Fig. 5: Resource allocation by using random selection and Hungarian method.

R1, R2, R3, R4 are the resources. The allocations of resources by using random selection are R1 → J1, R2 → J2, R3 → J3, R4 → J4

The total cost of this optimal assignment is 120 + 65 + 86 + 18 = 289.



The allocations of resources by using Hungarian algorithm are as follows:

$R1 \rightarrow J2, R2 \rightarrow J3, R3 \rightarrow J1, R4 \rightarrow J4$

The total cost of this optimal assignment is $40 + 33 + 13 + 18 = 104$.

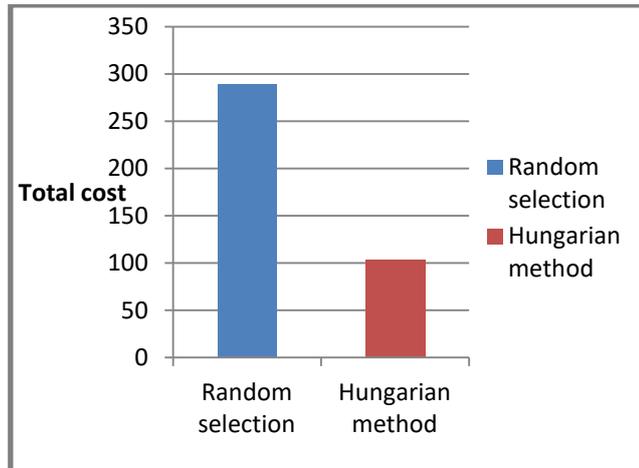


Fig. 6: Total cost of resource allocation by using random selection and Hungarian method.

Once the job gets executed the resources are released and the RT and ST get updated.

3. Logical Management

Free one to one mapping can be made by using $C \times R$ matrix and the jobs will not cut across the cos. Any C element can be mapped with any R element. Sustainability factor is not a constant under any mode of expansion of cloud sub domains. But it is a dynamically varying factor based on the level of coherence existing in the subsystems of resultant cloud. In any company the Resource (R) and Security (S) will have index values differing in enterprise sub unit management centers. If different companies are there under the same organization, which are distributed geographically, then we need to provide uniform access to the resources. Each company is having its cloud operating system intended to operate within virtualization environments. Each cloud operating system manages one or more virtual machines, virtual servers, and the resources within the virtualized environment. Each company has subunit offices to perform tasks locally or globally. We propose a Secure Resource Management System which has the full control over the resources in various cloud companies thereby provides better availability. Even though all the cloud companies are geographically distributed, it works as if they were located in a single cloud. Global jobs which are initiated by the user can be done by distributing the workloads across multiple computing resources under same organization which are distributed geographically. It improves resource utilization, maximize throughput and minimize the response time.

V. CONCLUSION

The advances in cloud paradigm are changing in the IT industry and provide many advantages to the organizations. Despite these progresses, the cloud is still vulnerable to many security challenges. In this paper, we proposed a robust methodology for managing the resources as well as user demand for processing. Secure Resource Management System (SRMS) provides effective methods to allocate cloud

resources to various jobs emanating from different users under the SRMS. Mapping of the resources and a scheme for calculating the cost of assigning the resources is also presented. Global jobs are executed by assigning the resources from various companies. We use Hungarian method and random selection method for the allocation of the resources wherein Hungarian method shows minimum cost for the execution of the jobs.

REFERENCES

1. Hwa-Chun Lin and Chien-Hsing Wang, "Distributed Network Management by HTTP-based remote invocation", Global Telecommunications Conference – Globecom '99.
2. European Commission. "Official Journal of the European Union On Data protection guidelines for the Early Warning and Response System", 9 February 2012 L 36/31.
3. Vaquero M., Rodero-Merino L., and Moran D., "Locking the Sky: A Survey on IaaS Cloud Security Computing". Springer. Press, January 2011, vol. 91, Number 1, pp. 93-118. doi: 10.1007/s00607-010-0140-x.
4. SUBASHINI, S. & KAVITHA, V. (2011) A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34, 1-11.
5. M. Rosenblum, Recent Advances in Virtual Machines and Operating Systems, Keynote Address, ACM ASPLOS 2006.
6. 3 E. Bauer, R. Adams, Reliability and Availability of Cloud Computing, John Wiley & Sons, 2012.
7. Meyer D, et al. Parallax: Virtual disks for virtual machines. In: Proceedings of EuroSys. 2008.
8. https://en.wikipedia.org/wiki/Hierarchical_storage_management.
9. <https://www.techopedia.com/definition/1086/hierarchical-storage-management-hsm>
10. <http://www.opencloudmanifesto.org/what-is-cloud-storage-types-advantages-and-disadvantages/22>
11. <http://searchstorage.techtarget.com/feature/Storage-management-for-virtualized-servers>.
12. Maryam Masoudi Khorsand, Mehdi Effatparvar and Mahdi Kanani, "A survey of Scheduling Algorithms in Grid Computing," International Journal of Research in Computer Applications and Robotics, ISSN 2320-7345, Volume 2, Issue 2, Pg. 118-126, February 2014.
13. Z. Shan, C. Lin, Modeling and performance evaluation of hierarchical job scheduling on the grids, in Sixth International Conference on Grid and Cooperative Computing, GCC 2007, 2007.
14. Y. Patel, J. Darlington, A novel stochastic algorithm for scheduling QoS-constrained workflows in a Web service-oriented grid, in 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops, WI-IAT 2006 Workshops, 2006.
15. H. Kuhn and B. Yaw, "The Hungarian Method for the Assignment Problem," Naval Research Logistics Quarterly, pp. 83–97, 1955.

AUTHORS PROFILE



Anitha K. L. is a research scholar in the Department of Computer Science, Bharathiar University, Coimbatore, India. Anitha K L received post graduate degree in Master of Computer Applications and B.Sc. degree in Computer Science from the University of Kerala. Her research interests include cloud computing security, virtualization, data center and networking and distributed computing.



T.R. Gopalakrishnan Nair, a Fellow of Institution of Engineers, has 34 years of experience in professional field spread over Research, Industry and Education. Currently, he is the Rector for Rajarajeswary Group of Institutions in India. He was the Aramco Endowed Chair in Technology in PM University, KSA. He holds degrees M.Tech. (I.I.Sc., India) and a Ph.D. in Computer Science. His areas of interest include Advanced networks, Cognitive Systems and Multidisciplinary studies including Brain and physical systems. He is a senior member of IEEE, ACM and few other professional bodies.