Volume: 06 Issue: 06 Pages: 2549-2555 (2015) ISSN: 0975-0290

SAFETY: A Framework for Secure IaaS Clouds

Vivek Shrivastava
International Institute of Professional Studies, Devi Ahilya University, Indore-17
Email: shrivastava.vivex@gmail.com
D. S. Bhilare
Computer Centre, Devi Ahilya University, Indore-17
Email: bhilare@hotmail.com

ABSTRACT

Cloud Computing is benefiting to both cloud hosts and consumers by providing elastic services as a utility. These services are provided on the basis of Service Level Agreement (SLA). Security and privacy are major issues when dealing with a multi - tenant model of cloud. Consumers are provided computing power in terms of virtual machines (VMs). A consumer can have many VMs at a time. Multiple consumers can get different VMs from the same server. This may lead to cross-VM attacks. This paper introduces a new framework: SAFETY (Security Awareness Framework for Everyone's Task with You), for maintaining security from cross-VM attacks, Data leakage, VM theft, VM escape, Hyper jacking and VM Hopping. Experiments and results show that this framework is suitable and can be used for secure operations at cloud host side.

Keywords - **Cloud Computing, Security, IaaS, VM Scheduling, SAFETY.**

Date of Submission: April 09, 2015 Date of Acceptance: May 24, 2015

I. INTRODUCTION

Cloud computing is generally the delivery of software, platform and infrastructure as a service wherever and whenever needed in an elastic, scalable, self service provisioned, standardized interface, billing and service usage metering manner [1]. Elastic and scalable means availability of resource can be increased or decreased by allocation or revoking allocation on dynamic request of users or consumers. Self-service provisioned means resources can be provided and relinquished on demand, without going through a lengthy manual process. Standardized interface lets a consumer to link one or more services of cloud to each other and billing and service usage metering must follow pay-as-you-go model.

Cloud computing services can be provided through private, public or hybrid deployment model of cloud. Each deployment model has its security requirements to ensure secure availability, confidentiality, and integrity. Similarly, every service model has its own security requirements.

Cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) require different security needs. IaaS model is focusing on virtual machine management and its security. Security issues to handle in IaaS model are (1) data leakage protection and usage monitoring, (2) Authentication and authorization, (3) incident response and forensic capabilities, (4) Infrastructure hardening, and (5) End to end encryption [2], [3].

Cloud's multi-tenant model provides major research areas for security related issues. Data in flight and data at rest are required to be secured from potential attacks. Data can be encrypted to make secure from data theft. Algorithms like RSA, DES, and TDES are available to encrypt data [4], [5]. Data in flight (or motion) can also be encrypted and compressed on the fly during transmission.

Fig. 1 Issues to handle in IaaS security.

CIA (Confidentiality, Integrity and Availability) triad is a key requirement in the cloud security domain. AAA, i.e. Authentication, Authorization, Auditing is required to provide security. Multi-factor identification and Encryption techniques are also required to provide a secure cloud computing environment [6]. DiD i.e. Defense in Depth is used by many organizations for security. DiD provides layered approach security to organizations. (1) Perimeter (Physical) security, (2) Remote access control (Authentication, VPN, etc.), (3) Network security (firewall, demilitarize zone, etc.), (4) Compute security (hardening, anti-virus, etc.), (5) Storage security (encryption, zoning etc.) are the layers used in DiD. DiD gives additional time to detect and respond to any attack. Table-1 shows cloud security concerns and solutions and table-2 shows cloud security threats and solutions [7], [8].

Table-1 Cloud Security Concerns and their solutions.

Sr. No.	Cloud Security Concern	Solution
1.	Multi Tenancy	Isolation of VMs, isolation of data, isolation of network communication.
2.	Velocity of Attack	Defense in Depth
3.	Information Assurance	Encryption and access control mechanism.
4.	Data Privacy and Ownership	Regional legal regulations like UK data protection act 1988, European union data protection directives (EUDPD), UK computer misuse act 1990, Family Educational Right and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), etc. should be compliant by data privacy mechanisms [9].

Table-2 Cloud Security Threats and their solutions.

Sr. No.	Cloud Security Threat	Solution
1.	VM theft and VM escape [10]	Restrict copy and move VM files to unauthorized users.
2.	Hyper Jacking [11]	(1) Hardware assisted secure launching of the hypervisor, (2) Scanning hardware level details to assess the integrity of the hypervisor and locating the presence of rouge hypervisor.
3.	Data Leakage [12]	(1) End-to-end data protection mechanisms must apply to all concerned parties. (2) Cross-VM Side Channel Attacks (SCA) can be protected by placing only those clients that have no conflicts with one another on the same server.
4.	Denial of Service (DoS) Attack [13]	Resource consumption of every VM needs to be restricted.

In IaaS resource scheduling, different consumers can access IaaS services from same cloud. These consumers, intentionally or unintentionally can access data or services of other consumers due to multi-tenancy. Data security and privacy must be provided to consumers. SAFETY framework is proposed in this paper, to provide privacy and security to consumers' data and services. Experimental results are shown to advocate our proposal.

The rest of the paper is organized as: Section 2 contains related work. Section 3 proposes SAFETY cloud architecture, Section 4 shows SAFETY score calculation, and describes the need of introducing SAFETY. In section 5, Relative SAFETY score calculation are given, Section 6 proposes VM placement policy with SAFETY, Section 7 shows Experiments and results and last section 8 is giving conclusion and future work.

II. Related Work

Cloud computing paradigm enables on-demand access to computing infrastructure and data storage resources with minimum management overhead. In [14] recently discovered attacks on cloud providers and their countermeasures are described. Protection mechanisms, improving privacy and integrity of client's data and computations are also described by the authors.

Computing infrastructure is provided for consumer in the form of virtual machines. These VMs can be used for different types of needs. In an IaaS service model of cloud an organization's existing hardware can be used to provide hardware services to other organizations or same organization. So an organization can use a cloud for its services, i.e. hosting a private cloud or can become a cloud host and provide services to others i.e. hosting a public cloud [15].

Starvation of resources is the main problem when dealing with heterogeneous request environment. This type of situations can be handled by adopting starvation-removal technique proposed in [16]. Proper load should be provided with virtual machines on a server, so that they can be protected from overloading. Measurement of computing power can be done by CBUD Micro [17] for very little computing power devices. Resource request and acceptance rate also fall due to heavy request traffic for resources and slow response, and the completion time of requests for resources. These situations are handled by consumer rating index (CRI) as given in [18] and modified earliest deadline first algorithm (mEDF) as given in [19].

Security measure is one of parameters to consider while selecting a cloud service model, cloud deployment model and cloud service providers [20]. Security problems and their solutions related to scaling, transience, software life cycle, diversity, mobility, identity, and Data lifetime are

Volume: 06 Issue: 06 Pages: 2549-2555 (2015) ISSN: 0975-0290

described in [21]. Virtual environment's security vulnerabilities like (i) communication between VMs or between VM and host (ii) VM escape (iii) VM monitoring from the host (iv) VM monitoring from another VM (v) Denial of service (vi) Guest-to-Guest attack (vii) External modification of a VM (viii) External modification of the hypervisor are described in [22].

A combined VMM/OS approach was advocated in [23]. The authors argued that information system isolation provides better software security than a conventional multiprogramming operating system approach. In [24] the new risks of the cloud's image repository are explained, that are faced by administrators and users. An image management system that can control access to images, tracks the provenance of images, and provide users and administrators with efficient image filters and scanners that detect and repair security violations were proposed by the authors to handle the risks.

An in-VM measuring framework for increasing virtual machine security in clouds was given in [25]. This framework proposed a module that measures all executables in VMs and transfers the values to a trusted VM. These values were compared with a reference table containing trusted measurement values of running executable verifies executable status. Utility computing component of cloud requires measuring and billing with multiple level of providers. This requires proper care so that a consumer must be billed accurately. On demand billing system availability is also required and in [26] Amazon DevPay is provided as a solution. Revenue at cloud host side can be increased by providing competitive rates using COMMA policy as proposed in [27]. However, we are interested in providing a secure environment to every VM belonging to different consumers, running on same/ different servers. In this paper, we are proposing a new secured framework SAFETY that will take care of security features of VMs on a server and provide a rank to every consumer's request.

III. SAFETY CLOUD ARCHITECTURE

We propose the SAFETY framework, which helps the cloud scheduler to find the most suitable consumer's requests and therefore can schedule resources. The SAFETY framework provides features such as a consumer's request selection based on security requirements and ranking of consumers' requests. This ranking is based on parameters provided during cloud computing contract process. SAFETY framework can be treated as a scheduler's decision making tool, designed to provide a secure environment for virtual machines. The consumer may be demanding much secured or less secured environment according to its application, but for security purpose more secure consumer's request will be fulfilled first with affinity to equally or more secured consumer's request. Fig. 2 shows the key elements of the framework:

(1) SAFETY Cloud Broker: This component is responsible for interaction with consumers and understanding their security status. It collects all their requirements and performs calculation of a consumer's request and their security status, assigns them a score. This score can be used at the time of fulfilling VM requirements and scheduling.

(2) Ranking System: This component ranks each and every consumer according to its score calculated by the SAFETY score calculator. This system finds the possibility of placement of consumers' VMs affinity with other consumers. This system uses relative consumer scores to compare different consumers' security status.

(3) Security Parameter Catalogue: This component act as back end for storage of security parameters of various consumers for further use.

(4) Scheduler: This component is responsible for scheduling of VMs to different consumers' request. Scheduler schedules isolated VMs to consumers having similar security status in affinity on different servers based on rank provided by SAFETY.

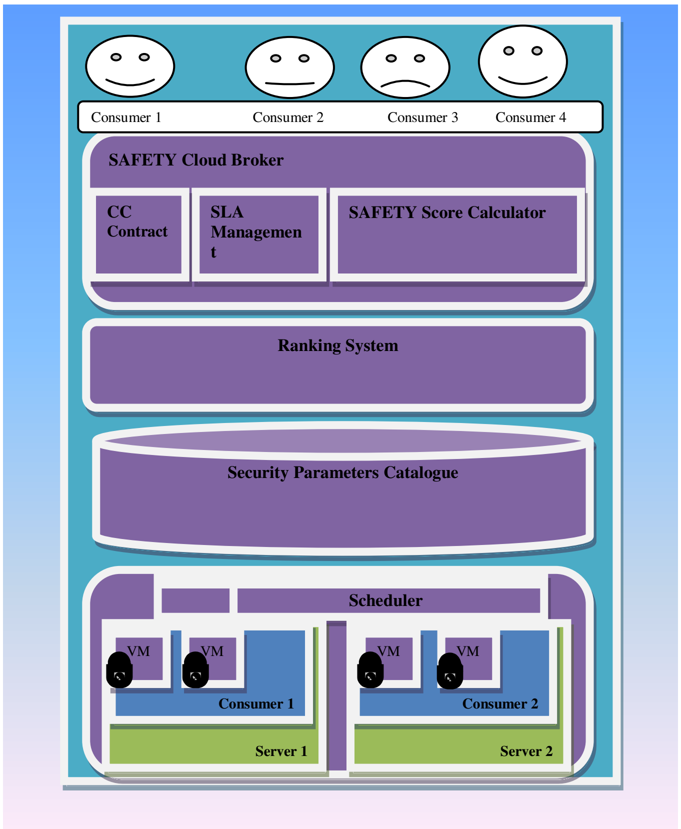

Fig. 2 SAFETY Cloud Architecture.

IV. SAFETY SCORE CALCULATION

Consumers' requests are categorized according to their SAFETY score. A high score means a more secured request for VMs and low score leads to late response time to a consumer's request. If two or more consumers have same score, then they can be allowed VMs from the same server at the same time in a first come first serve manner. Individual access to a server to a consumer's request can only be allowed in the case that, only one consumer's request is present at that time or request is so big that it occupies whole capacity of providing VMs. Consumer's SAFETY score using SAFETY calculator can be calculated by following set of parameters:

SAFETY Score= <PS, SN, ECF, AVAS, RUS, DNES, MUDF, OUPLP, WBS, FU, UGSP, IDS, IPS, MAuthe, MAutho, DiD, OCS, CGR, HA, HPM, SFOS>

The parameters described by above variables are described in table-3.

Table-3 Security Parameters and their abbreviations used.

Sr. No.	Parameters	Full Form
1.	PS	Physical Security
2.	SN	Secure Network
3.	ECF	Enable and Configure a Firewall
4.	AVAS	Anti Virus & Anti Spyware Programs
5.	RUS	Remove Unnecessary Software
6.	DNES	Disable Non Essential Services
7.	MUDF	Modify Unnecessary Default Features
8.	OUPLP	Operate Under the Principal of Least Privilege
9.	WBS	Web Browser Security
10.	FU	Future Updates
11.	UGSP	Use Good Security Practices.
12.	IDS	Intrusion Detection System
13.	IDPS	Intrusion Detection and Prevention System
14.	MAuthe	Method of Authentication
15.	MAutho	Method of Authorization
16.	AIS	Auditing Information Security
17.	OCS	Use of Other Cloud Services that may from a private/ public/ hybrid cloud.
18.	CGR	Compliance with Government Rules
19.	HA	History of Attacks
20.	HPM	Hardware Protection Mechanisms
21.	SFOS	Security Focused Operating Systems

The presence of all these parameters can be asked from the consumer during cloud computing contract process. The weight of these parameters (i.e. W1, W2, W3 and w1 to w21) can be decided by the cloud host. SAFETY score of every consumer's request can be calculated as follows:

$$\text{SAFETY SCORE} = \frac{\alpha * W_1 + \beta * W_2 + \gamma * W_3}{\sum_{i=1}^{3} W_i} \quad (1)$$

Where

$$\alpha = (SN*w_1+ECF*w_2+AVAS*w_3+RUS*w_4+DNES*w_5+MUDF*w_6+OUPLP*w_7+WBS*w_8+FU*w_9+UGSP*w_{10}) / \sum_{j=1..10} w_j \quad (2)$$

$$\beta = (IDS*w\_11+IDPS*w\_12+MAuthe*w\_13+MAutho*w\_14+AIS*w\_15+OCS*w\_16) / \sum_{j=11..16} w_j \quad (3)$$

$$\gamma = (PS*w\_17+CGR*w\_18+HA*w\_19+HPM*w\_20+SFOS*w\_21) / \sum_{j=17..21} w_j \quad (4)$$

V. RELATIVE SAFETY SCORE

Let C1, C2, C3, … , Cn are the SAFETY score of n consumer's security status. Following security matrix represents the consumers' security position relative to each others:

C1 C2 C3 … …… Cn

$$\begin{matrix} \mathbf{C1} \\ \mathbf{C2} \\ \mathbf{C3} \\ \mathbf{\dots} \\ \mathbf{Cn} \end{matrix} \begin{bmatrix} C1/C1 & C1/C2 & C1/C3 & \dots\dots. & C1/Cn \\ C2/C1 & C2/C2 & C2/C3 & \dots\dots. & C1/Cn \\ C3/C1 & C3/C2 & C3/C3 & \dots\dots. & C3/Cn \\ \dots\dots & \dots\dots & \dots\dots & \dots\dots & \dots\dots \\ Cn/C1 & Cn/C2 & Cn/C3 & \dots\dots & Cn/Cn \end{bmatrix}$$

So if we have 5 consumers' requests say C1 to C5 and let their scores are 2, 6, 3, 4, 5 respectively then this security matrix can be shown as:

$$\begin{matrix} & \mathbf{C1} & \mathbf{C2} & \mathbf{C3} & \mathbf{C4} & \mathbf{C5} \\ \mathbf{C1} & 1 & 0.3 & 0.6 & 0.5 & 0.4 \\ \mathbf{C2} & 3 & 1 & 2 & 1.5 & 1.2 \\ \mathbf{C3} & 1.5 & .5 & 1 & 0.7 & 0.6 \\ \mathbf{C4} & 2 & 0.6 & 1.3 & 1 & 0.8 \\ \mathbf{C5} & 2.5 & 0.8 & 1.6 & 1.2 & 1 \end{matrix}$$

Row1 of the security matrix shows C1's VMs with C1's VMs. It has a score 1 i.e. 100% so C1 is 100% secured with his all VMs on the same server. C2's VM are 33% secured with C1's VM, while C1's VM are 300% secured with C2 and so on.

VI. VM PLACEMENT POLICY

VM placement can be done according to above security matrix, e.g. if C2's VMs are required to place first then C2's row can be sorted in descending order, and after placement of all C2's VM, VM's from sorted list can be

Volume: 06 Issue: 06 Pages: 2549-2555 (2015) ISSN: 0975-0290

placed in sequence. Following are the placement sequences for C1, C2, C3, C4, and C5:

C1= {C1, C3, C4, C5, C2}
C2= {C2, C1, C3, C4, C5}
C3= {C3, C1, C4, C5, C2}
C4= {C4, C1, C3, C5, C2}
C5= {C5, C1, C3, C4, C2}

VII. EXPERIMENTS AND RESULTS

Five consumers who were using SaaS cloud were provided forms for filling their security status since IaaS actual consumers were not available at testing time. Their security scores and SAFETY scores are calculated according to eq. 1, 2, 3, and 4. These scores are shown in tables 4, 5, 6, 7. We have used w1 to w21 arbitrarily 5 and W1 to W3 also 5 arbitrarily, as it will be decided by cloud host in actual runs. Based on the final SAFETY scores, consumers' VM placement can be done according to their security matrix.

VIII. CONCLUSION AND FUTURE WORK

SAFETY framework benefits every consumer and cloud host by providing security status of them. It provides a proper method to choose right fellow VMs placements that produces secure environment. Hypervisor hijacking, VM Escape, VM Hopping, and VM theft can be prevented by using our proposed framework. Calculation of SAFETY score makes VM placement lengthy first time but, in long run by providing secure environment it saves time and provides protection from unsecure environments.

Future work may use SAFETY scores with CRI as proposed in [18]. This work also suggests other factors like infrastructure capacity required, cost and profit to take into account when dealing with multiple consumers' requests in IaaS clouds.

Table-4 Values of variables provided by consumers for Eq. -2.

Consumers	SN	ECF	AVAS	RUS	DNES	MUDF	OUPLP	WBS	FU	UGSP
c1	3	2	2	1	1	1	1	2	1	2
c2	3	3	2	1	1	0	1	3	1	3
c3	3	3	1	0	0	0	0	0	0	1
c4	4	3	3	1	1	1	1	3	1	4
c5	2	1	1	0	0	0	0	0	0	1

Table-5 Values of variables provided by consumers for Eq. -3.

Consumers	IDS	IDPS	MAuthe	MAutho	AIS	OCS
c1	4	1	2	3	2	2
c2	4	2	3	3	2	2
c3	2	1	1	1	1	1
c4	5	2	3	4	3	3
c5	1	1	1	1	0	0

Table-6 Values of variables provided by consumers for Eq. -3.

Consumers	PS	CGR	HA	HPM	SFOS
c1	2	1	1	1	1
c2	2	0	0	0	1
c3	1	1	1	0	0
c4	3	1	2	1	1
c5	1	0	0	0	0

Table-7 Consumers SAFETY score calculated using Eq. -1.

Consumers	α	B	γ	SAFETY Score
c1	1.6	2.333333	1.2	1.711111
c2	1.8	2.666667	0.6	1.688889
c3	0.8	1.166667	0.6	0.855556
c4	2.2	3.333333	1.6	2.377778
c5	0.5	0.666667	0.2	0.455556

References

[1] H.K. Mehta and E. Gupta. Economy Based Resource Allocation in IaaS Cloud, *International Journal of Cloud Applications and Computing, 3*(2), 2013, 1-11.

[2] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing, *Journal of network and computer applications, 34*(1), 2011, 1-11.

[3] SaaS, PaaS, and IaaS: A security checklist for cloud models, retrieved from http://www.networkworld.com/article/2199393/security/saas--paas--and-iaas--a-security-checklist-for-cloud-models.html on 3-September, 2014.

[4] S. Mondal and S. Maitra. Data security-modified AES algorithm and its applications, ACM *SIGARCH Computer Architecture News 42*(2), (2014), 1-8.

[5] L. Wang and T. Su. A Personal Information Protection Mechanism Based on Ciphertext Centralized Control in Logistics Information, *Proc. 3rd International Conference on Logistics, Informatics and Service Science,* Springer Berlin Heidelberg, 2015 1207-1212.

[6] P. Ranjan P. Mishra, J. S. Rawat, E. S. Pilli, and R. C. Joshi. Improved Technique for Data Confidentiality in Cloud Environment, Networks and Communications (NetCom2013), 183-193. Springer International Publishing, 2014 183-193.

[7] J.J. Stapleton, *Security Without Obscurity: A Guide to Confidentiality, Authentication, and Integrity* (CRC Press, 2014).

[8] D. Chen and H. Zhao. Data security and privacy protection issues in cloud computing, Proc. *IEEE International Conference on Computer Science and Electronics Engineering (ICCSEE),* Hangzhou, China, 2012, 647-651.

[9] C. Moore. The growing trend of government involvement in IT security, *Proc. ACM, the 1st annual conference on Information security curriculum development*, Kennesaw, GA, USA 2004, 119-123.

[10] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan. A survey on security issues and solutions at different layers of Cloud computing, *The Journal of Supercomputing, 63*(2), 2013, 561-592.

[11] K. Skapinetz. Virtualisation as a blackhat tool, *Network Security, 2007*(10), 2007, 4-7.

[12] C. Wang, Q. Wang, K. Ren, and W. Lou. Privacy-preserving public auditing for data storage security in cloud computing, *Proc.IEEE Conf. on* INFOCOM, San Diego, CA. 2010 1-9.

[13] H. Liu. A new form of DOS attack in a cloud and its avoidance mechanism, *Proc.The 2010 ACM workshop on Cloud computing security workshop*, Chicago, Illinois, USA, 2010, 65-76.

[14] E. Aguiar, Y. Zhang and M. Blanton. An Overview of Issues and Recent Developments in Cloud Computing and Storage Security, in High Performance Cloud Auditing and Applications, (Springer New York 2014) 3-33.

[15] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. Foster. Virtual infrastructure management in private and hybrid clouds, *Internet Computing, IEEE, 13*(5), 2009, 14-22.

[16] V. Shrivastava and D. S. Bhilare. Algorithms to Improve Resource Utilization and Request Acceptance Rate in IaaS Cloud Scheduling, *International Journal of Advanced Networking and Applications, 3*(5), 2012, 1367-1374.

[17] V. Shrivastava and D. S. Bhilare. CBUD Micro: A Micro Benchmark for Performance Measurement and Resource Management in IaaS Clouds, *International Journal of Emerging Technology and Advanced Engineering 3*(11), 2013, 433-437.

[18] V. Shrivastava and D. S. Bhilare. CRI: A Novel Rating Based Leasing Policy and Algorithm for Efficient Resource Management in IaaS Clouds, *International Journal of Computer Science and Information Technologies, 3*(2014), 2014, 4226-4230.

[19] V. Shrivastava and D. S. Bhilare. mEDF: Deadline Driven Algorithm for Minimizing Response Time and Completion Time in IaaS Clouds, International Journal of Application or Innovation in Engineering and Management, *3*(6), 2014, 16-22.

[20] H. Mehta, P. Kanungo, and M. Chandwani. Performance enhancement of scheduling algorithms in web server clusters using improved dynamic load balancing policies, *Proc. 2nd National Conference on INDIACom-2008 Computing For Nation Development*, New Delhi, India, 2008, 651-656.

[21] T. Garfinkel and M. Rosenblum. When Virtual Is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments, *Proc. 10th Workshop on Hot Topics in Operating Systems, Santa Fe, NM, 2005,* available at https://www.usenix.org/legacy/events/hotos05/prelim_papers/garfinkel/garfinkel_html/.

[22] J. S. Reuben. A survey on virtual machine security, *Helsinki University of Technology* ,2 2007, 36-40 available at http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf

[23] S.E. Madnick and J. J. Donovan. Application and analysis of the virtual machine approach to information system security and isolation, *Proc. ACM, the workshop on virtual computer systems*, Cambridge, Massachusetts, USA 1973, 210-224.

Volume: 06 Issue: 06 Pages: 2549-2555 (2015) ISSN: 0975-0290

[24] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning. Managing security of virtual machine images in a cloud environment, Proc. *The 2009 ACM workshop on Cloud computing security*, Chicago, Illinois, USA, 2009, 91-96.

[25] Q. Liu, C. Weng, M. Li, and Y. Luo. An In-VM measuring framework for increasing virtual machine security in clouds, *Security & Privacy, IEEE,* 8(6), 2010, 56-62.

[26] Amazon Devpay, retrieved from http://aws.amazon.com/devpay/ on 3-September, 2014.

[27] V. Shrivastava and D. S. Bhilare. COMMA: A Cost Oriented, Market and Migration Aware Leasing Policy and Algorithm in IaaS Clouds, *Proc. the 2014 ACM International Conference on Information and Communication Technology for Competitive Strategies*, Udaipur, Rajasthan, India, 2014, 52-59.

Authors Biography

Vivek Shrivastava is a research scholar at School of Computer Science and IT under the guidance of Dr. D.S. Bhilare. He is M.Tech. (Computer Sc.), MCA, and UGC-NET qualified in Computer Sc. & Applications. He is working as an Assistant Professor at International Institute of Professional Studies, Devi Ahilya University, Indore. His areas of interest are Cloud Computing, Ubiquitous Computing and Information Security.

D.S. Bhilare received his Ph.D. (Computer Science), M.Tech. (Computer Sc.), M.Phil. (Computer Sc.) and MBA from Devi Ahilya University, Indore. Worked as a senior project leader for ten years in the industry and developed various business applications for different industries. For the last twenty years, he is working at the University as a Senior Manager & Head Computer Centre. He has registered a patent. He has presented several papers in national & international conferences and published in reputed journals and international conference proceedings in the area of Information Security.