A Security Aware Leasing Policy and Algorithm for Iaas Clouds

Vivek Shrivastava
International Institute of Professional Studies,
Devi Ahilya University,
Indore, India

D.S. Bhilare
Computer Centre,
Devi Ahilya University,
Indore, India

***Abstract*—Resource management is a key task in the cloud ecosystem. Various lease policies are used to efficiently and effectively manage the resources at cloud host side. Advance Reservation, Best Effort and Immediate lease policies are the types of leases that can be used for providing resources in the form of virtual machines in IaaS clouds. Protection of resources requires a security policy at cloud host side that can take care of delivery of resources in a more secured manner. This paper focuses on SAFETY security policy [1], and finds it useful for secure scheduling of resources in IaaS cloud. Experiments and results show that the algorithm based on SAFETY policy provides isolation up to a proper level while considering backfilling for optimized resource management.**

Keywords—Cloud Computing; IaaS; Security; SAFETY;Haizea Lease Manager.

I. INTRODUCTION

Cloud services can be provided through public, private or hybrid deployment model of cloud. Public and hybrid models of cloud are more vulnerable in terms of security than private model. Private deployment model consists of a cloud having resources of one organization that are solely used by the one organization [2]. Public clouds offer multi-tenancy for maximum resource utilization that lets open loopholes in security provided by CSP.

IaaS model of cloud computing provides virtual machines (VMs) as computing infrastructure to consumers. Security threats can be sourced from the host and can be sourced from the cloud consumers of other VMs. Security threats sourced from the host can be handled at a cloud host level by adopting proper security measures. Services, applications and data can be captured by one of the cloud users with malafide intentions that can harm to reputation as well as can cause severe monitory loses to cloud host and cloud users.

Major security issue is unawareness of consumer about using best practices for hardening security on consumer's own side. Cloud host as well as cloud users can be severely affected and harmed by cloud users with wrong intentions. Cloud consumers are required to be properly educated about the best practices to keep safe from attackers and maintain their security. Every cloud consumer ought to know some security essential details that can be maintained by him. Essential security details were given in [1], which proposed a security tuple as shown in (1):

SAFETY Score= <PS, SN, ECF, AVAS, RUS, DNES, MUDF, OUPLP, WBS, FU, UGSP, IDS, IPS, MAuthe, MAutho, DiD, OCS, CGR, HA, HPM, SFOS> (1).

Parameters described by above variables are described in Table-1.

TABLE I. SECURITY PARAMETERS RESPONSIBLE FOR SAFETY SCORE [1].

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

Based on security parameters given in table-1, SAFETY score can be calculated by following four equations as given in [1]:

$$\text{SAFETY Score} = (\alpha*W1+ \beta*W2 + \gamma*W3)/ \textstyle\sum_{i=1..3} W_i \quad (1)$$

Where

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

$$\beta = (IDS*w_{11} + IDPS*w_{12} + MAuthe*w_{13} + MAutho*w_{14} + AIS*w_{15} + OCS*w_{16}) / \sum_{j=11..16} w_j \quad (3)$$

$$\gamma = (PS*w_{17} + CGR*w_{18} + HA*w_{19} + HPM*w_{20} + SFOS*w_{21}) / \sum_{j=17..21} w_j \quad (4)$$

This SAFETY score can be used to provide a secure environment to consumers' VMs in IaaS cloud.

The rest of the paper is organized as: Section 2 contains literature survey. Section 3 describes SAFETY leasing policy, Section 4 shows proposed algorithms. In section 5, details of experiments and results given, last section 6 is concluding our work.

II. Literature Survey

Cloud security is a major concern and key inhibitor in cloud adoption. Cloud resource management must be done in a way that it should take care of security concerns. Resources can be provided in the terms of virtual machines in IaaS clouds. Different types of leases are available to provision resources. Sotomayor et al. Suggested Haizea, a resource lease manager, that can act as a scheduling back end for OpenNebula in [3] , Haizea was suggested as a tool, which provides features that are not found in other cloud software or virtualization-based data centre management software.

Chavan et al. investigated the complex security challenges introduced in Infrastructure as a Service (IaaS)-based cloud computing. Availability, Authenticity, and Privacy are marked essential concerns for both Cloud providers and consumers as well by them. They suggested a lack of security in IaaS model can certainly affect the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. They presented an elaborated study of IaaS components' security and determined vulnerabilities and countermeasures. Finally, they proposed a Security Model for IaaS (SMI) to guide security assessment and enhancement in IaaS layer [4].

Arshad et al. described their efforts to quantify security for Clouds to facilitate provision of assurance for quality of service, which is one of the factors contributing to dependability in [5]. They focused on delivering customized security solutions such as effective intrusion prevention and detection. They demonstrated the applicability of their work, by incorporating requirements in the resource acquisition phase for Clouds.

Chokhani et al. advocated the inclusion of three important features to mitigate shortcoming in Haizea. First, they introduced a new class of lease: Dynamic lease to accommodate resource changes. Second, they examined virtual machine resource utilization to decide about the demand and need of allocation change and third, lease introduced by them accommodated the expected changes in resource allocation by introducing two new sub-leases which allow dynamic resource allocation in the schedule [6].

Shrivastava et al. suggested starvation of resources as the main problem when dealing with heterogeneous request environment in [7]. This type of situations can be handled by adopting starvation-removal technique proposed in [8]. Scheduling of resources can be done on the basis of capacity of available resources. To evaluate performance of the computing capacity CBUDMicro for very little computing power devices was introduced in [9]. Cloud resources can also be scheduled according to priority of consumers. To give a proper priority, Consumer Rating Index (CRI) has been calculated in [10]. Resource request and acceptance rate can fall due to heavy request traffic for resources and slow response, and the completion time of requests for resources. To handle this type of situations modified Earliest Deadline First algorithm (mEDF) was given in [11]. Scheduling of resources can also be done according to market oriented policies that can invoke more profit to CSPs and cloud users. COMMA: A Cost Oriented, Market and Migration Aware Leasing Policy and Algorithm were proposed in [12] to schedule VMs. COMMA maintained a balance between cost, profit as well as VM migrations during peak loads [12].

In [1], SAFETY- a secure IaaS cloud framework was proposed to mitigate cross-VM side channel attacks. In this paper SAFETY is extended and implemented in Haizea lease manager with slight modifications in it and experimented to validate the introduced framework.

III. SAFETY Leasing Policy

In our work, we are extending use of SAFETY leasing policy with its parameters' values to schedule VMs to cloud consumer in a way that every good VM gets a good neighbourhood VM. Security parameters can have different values from 0 to 5 based on their nature. So there numeric values along with their values are given in following tables from table no. 2 to table no. 10.

TABLE II. Secure Network Numeric Values.

SN Value	Values
1	If consumer has configured the wireless network to use WPA2-AES encryption for data confidentiality.
2	if consumer has changed default user name and password with SN=1,
3	if consumer has started conducting MAC address filtering with SN=2,
4	If consumer has changed default wireless SSID for security purpose with SN=3.
0	If consumer is not aware of network security.

TABLE III. Enable and Configure a Firewall Numeric Values.

ECF Value	Values
1	If consumer is using operating system's firewall.
2	If consumer is using home router firewall with ECF=1.
3	If consumer has set a strong password to protect it against unwanted changes with ECF=2.
0	If consumer is not aware of ECF.

TABLE IV. Anti Virus and Anti Spyware Program Numeric Values.

AVAS Value	Values
1	If consumer has installed reputed Anti-Virus system on its machines.
2	If consumer is using a good Anti-Spyware software with AVAS=1.
3	If consumer's machines are configured for automatic updates and signatures are up-to-date.
0	If consumer is not aware of AVAS.

TABLE V. Remove Unnecessary Software Numeric Values .

RUS Value	Values
1	If consumer has removed unnecessary software.
0	If consumer is not aware of RUS.

TABLE VI. Disable Non Essential Services Numeric Values.

DNES Value	Values
1	If non-essential services like file sharing etc. have been disabled by consumer
0	If consumer is not aware of DNES.

TABLE VII. Modify Unnecessary Default Features Numeric Values.

MUDF Value	Values
1	If unnecessary default features have been modified like auto run feature of software.
0	If consumer is not aware of MUDF.

TABLE VIII. Operate Under the Principal of Least Privilege Numeric Values.

OUPLP Value	Values
1	If consumer gives the consent of using principle of least privilege like administrator's account will only be used when required otherwise least privilege user's account will be used.
0	If consumer is not aware of OUPLP.

TABLE IX. Web Browser Security Numeric Values.

WBS Value	Values
1	If mobile code on less trusted web site is disabled.
2	If options to set cookies are disabled so that attacker cannot log into already visited website.
3	If different trust levels have been maintained by consumer with different sites.
0	If consumer is not aware of WBS.

TABLE X. Future Updates Numeric Values .

FU Value	Values
1	If updates to patches or fix vulnerabilities, flaws and weaknesses in software released by their software vendors are enabled.
0	If consumer is not aware of FU.

TABLE XI. Use Good Security Practices Numeric Values

UGSP Value	**Values**
1	If consumer uses reputed updated anti-malware software.
2	If consumer uses reputed updated anti-IP spoof, anti-Phishing software.
3	If consumer is aware of caution about e-mail attachments and un-trusted links.
4	If consumer has strong passwords, passphrases and hard to crack security questions.
0	If consumer is not aware of UGSP.

TABLE XII. Intrusion Detection System Numeric Values.

IDS Value	Values
1	If consumer uses network IDS with anomaly based approach.
2	If consumer uses network IDS with signature based approach.
3	If consumer is aware of caution about e-mail attachments and un-trusted links.
4	If consumer uses host IDS with signature based approach.
5	If consumer uses integrated IDS with all of the features from 1 to 4.
0	If consumer is not aware of IDS.

TABLE XIII. Intrusion Detection and Prevention System Numeric Values.

IDPS Value	Values
1	If consumer is using IDPS that auto responds to suspicious activities by resetting the connections.
2	If consumer is using IDPS that auto responds to suspicious activities by reprogramming the firewall to block network traffic from the suspicious network source.
0	If consumer is not aware of IDPS.

TABLE XIV. Method of Authentication Numeric Values.

Mauthe Value	Values
1	If consumer is using a multifactor authentication and/or a strong password or passphrase.
2	if consumer is using token based authentication system, ATM card, smart card or one-time password, digital signature, digital certificate etc.
3	if consumer is using biometric authentication schemes like figure-print, retina scan, Iris scan, hand geometry etc.
0	If consumer is not aware of Mauthe.

TABLE XV. Method of Authorization Numeric Values.

Mautho Value	Values
1	If consumer is using different types of privileges for different type of users at its site.
2	If consumer is using roles and aware of uses and restrictions of roles.
3	If consumer is using resource limitations to different users at its site.
4	If consumer is aware of how profiles are determined and used.
0	If consumer is not aware of Mautho.

TABLE XVI. Auditing Numeric Values.

Auditing Value	Values
1	If auditing is done for data centre security.
2	If auditing is done for network security along with 1.
3	If auditing is done for application security along with 2.
0	If consumer is not aware of Auditing information security.

TABLE XVII. Other Cloud Services using private/ public/ hybrid cloud Numeric Values .

OCS Value	Values
1	If consumer is using services from other public cloud service provider.
2	If consumer is using services from hybrid cloud services provider, other than this cloud host.
3	If consumer is using services from private cloud. This private cloud may be on-premise or off-premise cloud.
0	If consumer is not aware of OCS.

TABLE XVIII. COMPLIANCE WITH GOVERNMENT RULES NUMERIC VALUES.

CGR Value	Values
1	If consumer maintains compliance with government rules in cloud host country.
0	If consumer is not aware of CGR.

TABLE XIX. HISTORY OF ATTACKS NUMERIC VALUES .

HA Value	**Values**
1	If history of attacks is poor.
2	If history of attacks is clean i.e. consumer has not been attacked yet by attackers.
0	If consumer is not aware of HA.

TABLE XX. HARDWARE PROTECTION MECHANISMS NUMERIC VALUES.

HPM Value	**Values**
1	If consumer uses trusted platform modules as hardware protection mechanisms.
0	If consumer is not aware of HPM.

TABLE XXI. SECURITY FOCUSED OPERATING SYSTEMS NUMERIC VALUES.

SFOS Value	**Values**
1	If security focused operating systems are used at consumer's side.
0	If consumer is not aware of SFOS.

IV. PROPOSED ALGORITHMS

Algorithm based on leasing policy SAFETY is given in this section. System description and algorithm are also described here. Computing environment is described in the former paragraph and Sample lease requests are described in later paragraph.

In Haizea, input of leases can be done with the help of XML based files called lease workload file (lwf), further applications can enter lease request in XML file and then this XML files can be given as input to Haizea lease manager. The following specifies a collection of 4 nodes, all with one CPU, four with 1024MB of memory and eight with 2048MB of memory as used in [11]:

```
<nodes>
    <node-set numnodes="4">
    <res type="CPU" amount="100"/>
    <res type="Memory" amount="1024"/>
    </node-set>
    <node-set numnodes="8">
    <res type="CPU" amount="100"/>
    <res type="Memory" amount="2048"/>
    </node-set>
</nodes>
```

Sample lease request in modified lwf is shown below:

```
<lease-workload name="sample">
    <description>
            A simple trace where so many leases with
      SAFETY score as saix is specified.
    </description>
<lease-requests>
    <!-- First lease request-->
    <lease-request arrival="00:00:00">
    <lease preemptible="true">
    <nodes>
            <node-set numnodes="4">
            <res type="CPU" amount="100"/>
            <res type="Memory" amount="1024"/>
            </node-set>
    </nodes>
    <start></start>
    <duration time="10:00:00"/>
    <software>
            <disk-image id="foobar.img"
        size="1024"/>
    </software>
    <saix  index="4"/>
</lease>

</lease-request>
<!-- Second lease request -->
<lease-request arrival="01:00:00">
    <lease preemptible="true">
    <nodes>
            <node-set numnodes="4">
            <res type="CPU" amount="100"/>
            <res type="Memory" amount="1024"/>
            </node-set>
    </nodes>
    <start></start>
    <duration time="10:00:00"/>
    <software>
            <disk-image id="foobar.img"
        size="1024"/>
    </software>
    <saix index="2"/>
    </lease>
</lease-request>
<!-- Third lease request -->
<lease-request arrival="02:00:00">
    <lease preemptible="true">
    <nodes>
            <node-set numnodes="4">
            <res type="CPU" amount="100"/>
            <res type="Memory" amount="1024"/>
    </node-set>
    </nodes>
    <start></start>
    <duration time="10:00:00"/>
    <software>
            <disk-image id="foobar.img"
      size="1024"/>
    </software>
    <saix index="1"/>
```

```
        </lease>
    </lease-request>
    <!-- Fourth lease request -->
    <lease-request arrival="03:00:00">
        <lease preemptible="true">
        <nodes>
                <node-set numnodes="4">
                <res type="CPU" amount="100"/>
                <res type="Memory" amount="1024"/>
                </node-set>
        </nodes>
        <start></start>
        <duration time="10:00:00"/>
        <software>
                <disk-image id="foobar.img"
            size="1024"/>
        </software>
        <saix index=”3”/>
        </lease>
    </lease-request>
```

Attributes and their sub attributes like lease, lease id, nodes, start, duration time, and software are already available with Haizea installation. We have introduced new attribute saix, which represents SAFETY score of consumer. This SAFETY score will be calculated by cloud host with the help of equation (3.1) and SLA entries, according to its needs, application area and present situations.

We have implemented our algorithms in Python and integrated them with Haizea to test and run. Procedure Calculate_SAFETY_Score is used to calculate security scores of each consumer. Procedure Enqueue_Lease is used to append a new request to lease queue. We have modified BE leases according to our need to implement SAFETY leases so, we are interested in only BE lease environment. Procedure Sort_Queue_Reverse is used to sort all available leases using saix score as primary key in descending order. Serve_Leases procedure is used to do operations of Haizea normally i.e. managing available lease requests.

Algorithm

```
Procedure Calculate_SAFETY_Score()
for each consumer in consumers list
    begin
        Calculate SAIRAM score as according to equation-1.
        Assign score in saix attribute to corresponding consumer’s lease.
    end
End of Calculate_SAFETY_Score()
```

```
Procedure Enqueue_Lease()
Begin
    if scheduling lease type = BE then:
        insert_in_queue(lease, saix)
    call Sort_Queue_Reverse (lease, saix)
    end if
End of Enqueue_Lease()
```

```
Procedure Sort_Queue_Reverse(lease, saix)
Begin
    Sort all leases in descending order of saix
    call Serve_sorted_leases()
End of  Sort_Queue_Reverse(lease, saix)
```

```
Procedure Serve_Leases()
Begin
    if resources are available then:
    Pick leases from sorted queue and allot VMs demanded.
    if VM_shutdown=true then:
            Relinquish VMs for other leases.
        else
            put leases in wait queue
        end if
    end if
End of Serve_Leases()
```

V. EXPERIMENT AND RESULTS

Table-XXII shows consumers’ requests under test run. This batch of consumers’ requests is generated only for checking the validity of our proposed leasing policy and algorithm in lab. Parameters Lid, SAFETY, NumNodes, C_No are used in table, where Lid is lease id usually given in ascending order in order of appearance of leases, SAFETY score is calculated according to equations 1, 2, 3, and 4 on random test data. NumNodes is number of nodes required by consumer in present lease, and C_No is completion number of that lease.

TABLE XXII. SCHEDULING VMS ACCORDING TO SAFETY SCORE AND THEIR COMPLETION NUMBER.

Sr. No.	Lid	SAFETY Score	Num_Nodes	C_No
1	1	4	4	5
2	2	3	2	4
3	3	5	2	6
4	4	1	4	1
5	5	2	4	3
6	6	2	2	2
7	7	6	1	7

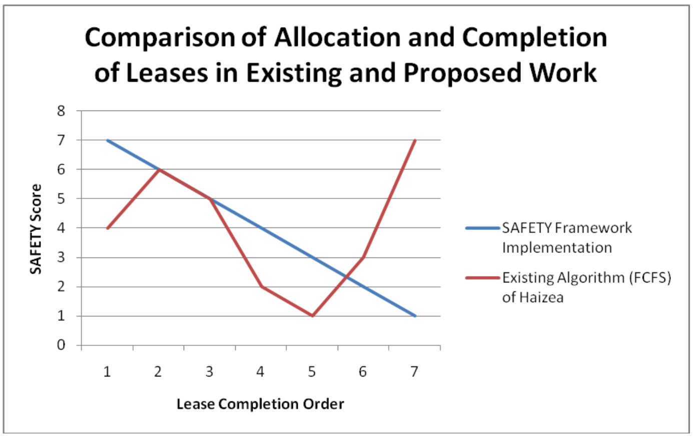

Fig. 1. Graph showing comparison between SAFETY framework implementation and existing algorithm.

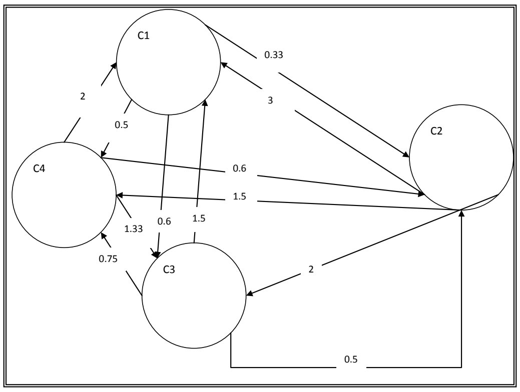

Fig. 2. Directed Graph Showing Relative SAFETY Scores of Consumers.

Figure 2 shows a directed weighted graph. This graph shows consumers' request as vertex and edges as relative safety score between two consumers' requests that can be used in taking scheduling decisions.

VI. CONCLUSION

Resource security of every user from other users of cloud is necessary for efficient and effective conduct of cloud operations. Cloud hosts and users both require a line of control (LOC) that should not be crossed by other users of cloud. SAFETY algorithm and its implementation show a way, that resources can be protected by increasing awareness of cloud users.

REFERENCES

[1] V. Shrivastava and D. Bhilare, ' SAFETY: A Framework for Secure IaaS Clouds', *International Journal of Advanced Networking and Applications* , vol. 6, no. 6, pp. 1367-1374, 2015.

[2] H. Mehta and E. Gupta, 'Economy Based Resource Allocation in IaaS Cloud', *International Journal of Cloud Applications and Computing*, vol. 3, no. 2, pp. 1-11, 2013.

[3] B. Sotomayor, R. Montero, I. Llorente and I. Foster, 'Virtual Infrastructure Management in Private and Hybrid Clouds', *IEEE Internet Comput.*, vol. 13, no. 5, pp. 14-22, 2009.

[4] P. Chavan, P. Patil, G. Kulkarni, R. Sutar, and S. Belsare. 'IaaS Cloud Security', In proc. of International Conference on Machine Intelligence and Research Advancement (ICMIRA), 2013, pp. 549-553. IEEE, 2013.

[5] A. Junaid, P. Townend, and J. Xu. 'Quantification of security for compute intensive workloads in clouds' In proc. of 15th International Conference on Parallel and Distributed Systems (ICPADS), 2009, pp. 479-486. IEEE, 2009.

[6] P. Chokhani, and G. Somani. 'Dynamic resource allocation using auto-negotiation in Haizea' In proc. of Sixth International Conference on Contemporary Computing (IC3), 2013, pp. 232-238. IEEE, 2013.

[7] 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*, vol. 3, no. 05, pp. 1367-1374, 2012.

[8] V. Shrivastava and D. Bhilare, 'CBUD Micro: A Micro Benchmark for Performance Measurement and Resource Management in IaaS Clouds', *International Journal of Emerging Technolgy and Advanced Engineering*, vol. 3, no. 11, pp. 433-437, 2013.

[9] 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*, vol. 3, no. 2014, pp. 4226-4230, 2014.

[10] 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 & Management*, vol. 3, no. 6, pp. 16-22, 2014.

[11] V. Shrivastava and D. Bhilare, 'COMMA: A Cost Oriented, Market and Migration Aware Leasing Policy and Algorithm in IaaS Clouds' In Proc. of the 2014 International Conference on Information and Communication Technology for Competitive Strategies (ICTCS '14). ACM, New York, NY, USA, , Article 52 , 7 pages. DOI=10.1145/2677855.2677907 http://doi.acm.org/10.1145/2677855.2677907.

[12] Sotomayor, Borja. "The Haizea Manual." *2010-05-19). http://haizea. cs. uchicago. edu* (2010).