Infrastructure as a Service: Exploring Network Access Control Challenges

Shadha Mohamed ALAmri and Lin Guan
Department of Computer Science
Loughborough University
United Kingdom
S.AL-Amri@lboro.ac.uk,l.guan@lboro.ac.uk

***Abstract*—Cloud Computing Infrastructure as a Service (IaaS) is a great model for outsourcing IT infrastructure. It is built to offer fascinating features to support business development, such as elasticity, multi-tenancy, configurability and dynamicity. However, IaaS faces security challenges on account of its flexible nature. For this article, we studied the IaaS characteristics and investigated their related security challenges. We then elaborated these security challenges by exploring the security threats on live virtual machine migration as it is one of the main IaaS operations. We found that proper access control techniques and models are a critical element in enhancing IaaS and mitigating the identified security threats. Therefore, we investigated and contrasted the implemented and the proposed firewall architectures in IaaS as a firewall is a basic security appliance that enforces access control. We also explored and contrasted the proposed access control models in the IaaS. It was found that the traditional firewalls and access control models were not sufficient for IaaS. Therefore, there is a need to develop a proper access control model and enforcement techniques to mitigate IaaS security threats. Based on the security research trend and the results obtained in this articles exploration, we endorse an IaaS access control system built on a computational intelligent approach.**

Keywords*—IaaS; live virtual machine migration; access control; firewall; security

I. INTRODUCTION

Cloud Computing emerges on a distributed computing paradigm. It utilises the huge computing resources among multiple customers with minimal expense and effort compared to traditional computing facilities. Since Cloud Computing emerged from a business perspective, the different clouds may not be compatible with each other as they follow different standards [1, 2]. Although Cloud Computing has incredible benefits, some governments and enterprises hesitate to transfer their computing technology to the Cloud due to security aspects. Cloud computing services consist of three layers: at the top, the Software as a Service (SaaS) cloud, which provides software applications; the Platform as a Service (PaaS) cloud, which provides programming language and needed libraries; and at the bottom, the Infrastructure as a Service (IaaS), which provides computing infrastructure resources. Cloud is deployed via three main models: public where different customers (cloud users) can share the cloud service, private where only one organisation owns the cloud infrastructure and hybrid, where the cloud combines public and private features[3].

The IDC survey shows that 75% of customers are not tending to move to Cloud Computing because of the security and privacy concerns [4]. Securing the IaaS layer is vital, as all the other layers are built on top of it. In this article, we focus on the security issues raised in the IaaS layer due to its features, such as elasticity, dynamicity and its large scale. Based on the authors best knowledge, this paper differs from other research papers in the field by combining the identification of security limitations of both the access control models and the access control enforcement mechanisms in IaaS. We attempt to give an understanding of the big picture of access control component in the IaaS security architecture.
The aim of this paper is to identify those IaaS access control security challenges and the approaches used to mitigate them. Specifically, the following objectives are set for this research:

- Identify the security threads in IaaS that emerged from its core features and explore the security issues related to one of the IaaS services operations, namely live virtual machine migration.
- Investigate limitations of the well-known network access control enforcement mechanisms in IaaS, which are firewall and VLAN.
- Explore the limitations of the proposed access control model approaches in IaaS.

On the view of computer security systems, the IaaS security requirements based on its characteristics are defined in Section II. Then, the security of live virtual machine migration operation as an example of IaaS operations is identified in Section III. IaaS firewall as an access control enforcement mechanism is investigated in Section IV. IaaS access control models are explored in Section V. An overall discussion is presented in Section VI with a recommended approach to mitigating access control limitation in IaaS. Finally, we conclude in Section VII.

II. SECURITY CHALLENGES OF INFRASTRUCTURE AS A SERVICE

The characteristics of Infrastructure as a Service (IaaS) encouraged ICT customers to adopt it as the next generation model for outsourcing IT infrastructure [5]. IaaS is capable of controlling and managing the virtualised environment represented in a virtual machine life circle by providing the virtual machine (VM) with the requested resources, such as storage, network and processing power [6].
IaaS features offer business advantages, such as rapid elasticity and fast resource pooling, since IaaS deploys virtualisation technology which supports several innovations, such as multi-core chips and live migrations [7]. A key component in

building a virtualisation environment is to operate it via the hypervisor, although the hypervisor on its own cannot build IaaS. Therefore, a cloud-stack is required to build IaaS, such as OpenStack, CloudStack and OpenNebula. According to the current industry, OpenStack is likely to become a dominant cloud-stack [1].

On the other hand, the flexibility characteristics of IaaS introduce several security challenges linked to access control implementation.

The elasticity feature of IaaS allows the cloud user (customer) to scale up and scale down to meet their project requirements. This leads to a rapid change in the infrastructure configurations. However, elasticity introduces security challenges in respect to providing an administrative separation between the customers virtual environments. There is a need for a security mechanism that enforces a proper configuration and change management, as well as a fine-grained and predefined access control mechanism [8].

The multitenant nature of IaaS which facilitates the ideal usage of infrastructure by sharing resources between multiple users faces some security challenges as well [1]. Therefore, it is more likely that there is a need for a new type of access control policy between tenants in intra-cloud communication [9]. A tenant can be an enterprise in the context of a public cloud or a department within an enterprise in the context of a private cloud [10].

The flexibility feature of IaaS enables the user to configure their own virtual machines and computing infrastructure [11]. Hence, it is prone to misconfiguration that can lead to a security violation [12]. Therefore, there is a need to monitor cloud behaviour to figure out unexpected errors. For example, in April 2011 an infrastructure outage caused Amazons Compute Cloud EC2 to be unavailable for its customers [13]. Therefore, there is a need to monitor IaaS behaviour. In the literature, an approach constructed on role-based access control has been proposed [14].

The dynamicity of IaaS facilitates virtual machine (VM) mobility among physical machines for different aspects, such as server consolidation, load balancing, data recovery and green computing, through a technique called live virtual machine migration (LVMM). The LVMM allows the movement of virtual machines between the physical machines at the run time with a minimum downtime [15]. Although live migration supports IaaS dynamicity, it introduces some security threats. The protocol used for live migration moves the virtual machine state in plain text, which allows hackers to snoop it through the network links. Even encryption is not able to secure it, as illustrated experimentally [16]. Therefore, there is a need for re-thinking the existing access control and isolation mechanism.

Moreover, the dynamicity feature of IaaS affects firewall functionality since the VM gets a dynamic IP address through a DHCP server that assigns a lease time for the client IP address. The virtual machine must renew its IP address when the lease time expires. Upon renewing its IP address, it may or may not receive the same IP address that it received previously [17]. A source IP address and a destination IP address are basic information to generate a firewall rule. The firewall rules remain constant unless there is an explicit need to change the policy as a result the firewall cannot adapt to real-time threats [18]. Any system that uses predetermined and fixed IPs might impose some limitation on the dynamism and the scalability of IaaS [19].

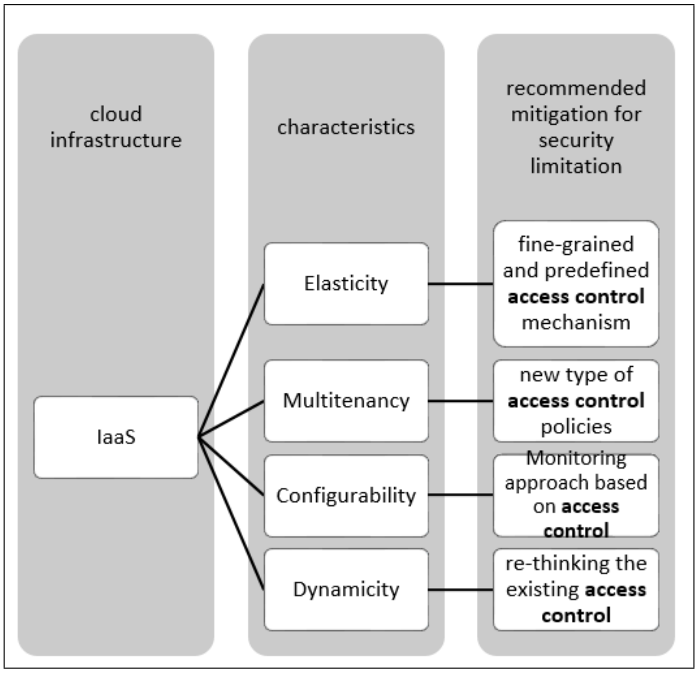
cloud infrastructure
characteristics
recommended mitigation for security limitation
IaaS
Elasticity
Multitenancy
Configurability
Dynamicity
fine-grained and predefined **access control** mechanism
new type of **access control** policies
Monitoring approach based on **access control**
re-thinking the existing **access control**

Fig. 1: Recommended mitigation for some of IaaS security challenges

A firewall is a critical network access control mechanism, therefore it will be discussed in more detail in Section IV. The above IaaS security challenges analysis shows that there are several security vulnerabilities occurring as a side effect of the substantial IaaS characteristics. Fig. 1 reveals that a proper design and implementation of access control is a critical element that can contribute to mitigating the majority of the security IaaS challenges.

The remaining sections of this article will identify the limitations of the traditional network access control enforcement mechanisms which are firewall and VLAN. Then it will explore the existing access control models and investigate their ability to accommodate IaaS security requirements.

As an example of IaaS operations, live virtual machine migration (LVMM) operation is explored since LVMM can reflect most of the essential IaaS characteristics. The LVMM security challenges are raised as a consequence of elasticity, multi-tenancy, configurability and dynamicity.

III. LIVE VIRTUAL MACHINE MIGRATION SECURITY CHALLENGES

The IaaS layer consists of several components, such as virtualization, networking, storage and processing. Virtualisation is one of the key components; furthermore, the main core services in IaaS are Virtual Machine (VM) provisioning and VM migration [7]. Security of LVMM is considered one of the major challenges in IaaS and a critical research topic [7, 20–22].

There is a default LVMM algorithm in most popular hypervisors, such as Xen, VMWare and KVM [23]. A typical

LVMM mechanism consists of four main stages, as shown in Fig. 2 , which start with several iterations that aim to transfer VM memory pages from the source physical machine to the destination, where a new location for VM has been selected.

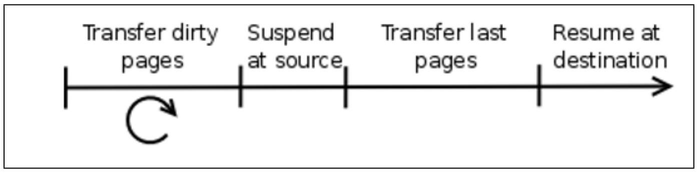

Fig. 2: LVMM Process Steps [24]

The ideal migration process is to copy the complete state of the VM, including memory, disk and network connection [23]. From a networking point of view, there are two categories of LVMM: moving VMs belonging to the same sub-network and moving VMs between different sub-networks. The latter requires a change of IP address and introduces another challenge that limits migration in cloud computing [25].

LVMM has been penetrated via man-in-the-middle attacks, as well as successfully attacked by through flag migration [16, 26, 27]. LVMM introduces important security issues because it includes VM state transfer through communication links, which can be attacked by ARP spoofing, DNS spoofing and route Hijacking [28]. Live Virtual Machine Migration (LVMM) security vulnerabilities are related to the security exposures in virtualisation technology [21, 28–33]. The following illustrates LVMM vulnerabilities, which have been categorised into three sources of threat, as follows:

- The first vulnerability is through the network link, as live migration involves a lot of network state transfer. Encryption techniques can be involved in mitigating this risk, but there should be a careful consideration of downtime since LVMM runs in real time. IPsec has been used in some security approaches to mitigate live migration threats, hence it introduces a huge computational delay [34, 35]. Moreover, encryption is not able completely to mitigate this security hole [16].
- The second vulnerability is through the host (physical machine), where it can be attacked or it can host an untrustworthy VM. As a consequence, the migrated VM security can be compromised since it will be in a shared environment with malicious components. Attacks can also be initiated in migrated VMs through the hypervisor if its corresponding host has been successfully compromised.
- The third vulnerability is based on security configuration consistency and efficiency. This is as a result of the different natures of physical appliances and virtual appliances, such as a firewall. This vulnerability occurs due to various factors, such as firewall placement and the policy configurations [36]. Moreover, elasticity introduces security flaws caused by misconfiguration after a migration is triggered [37]. Network state consistency can also be affected after migration where some network packets might be lost during LVMM downtime [38].

To sum up, LVMMs main security issues arise as a consequence of an environment shared between different customers (cloud users), which is a multi-tenancy feature of IaaS, as well as dynamicity and elasticity features which raise the need to update access control policies as the virtual machine changes its location. We can conclude that LVMM security is a critical issue in IaaS and it faces serious security challenges that need to be addressed and considered as an open research topic.

There is a trend to secure LVMM through vTPM [39]. Nevertheless, TPM-based measurements are ineffective for detecting a malicious cloud service provider as well as having limitations in verifying the hypervisor integrity in public clouds via remote attestation [40].

To secure LVMM, there is a need to design an access control policy that allows the administrator to manage migration privileges. The existing access control model in IaaS should be upgraded to cope with the emerging security challenges [16]. Similarly, existing firewall approaches should be modified to meet IaaS characteristics.

IV. IAAS FIREWALL SYSTEM

IaaS dynamicity and rapid infrastructure changes, due to adding and removing virtual machines and virtual machine migration, introduce a challenge to the firewall as there is a need to update firewall entries frequently. This leads to increasing maintenance overheads as firewall policies need to be updated in such large scale environment [9]. If the firewall is not well constructed, managed and updated, the IaaS will be at risk, resulting in facilitating for hackers the access to the cloud interface on behalf of legitimate users [40, 41].

A. Security Group

A firewall system is a critical network access control enforcement mechanism in most computing environments. A Cloud service provider (CSP) provides a firewall functionality in the form of a security group. For example, Amazon, Windows Azure and OpenStack implement the concept of the security group to provide a firewalling service to their customers.

In general, the security groups are set to deny everything by default and individual services must be enabled by the client. The security group allows customers to restrict traffic to and from their VMs. All VMs which belong to the same security group will have the same firewall policy [1].

This makes a cloud firewall service relatively user-friendly, but it lacks many of the features commonly found on local firewall products [42]. The security groups alone are insufficient to prevent attackers from communicating with the external network [43]. There are two methods of setting up firewall policy through security group: either to create an entry for each VM in the security group or to group VMs in one entry based on their IP prefix. The first method faces scalability limitations in IaaS, while the second method complicates VM address management [9]. Therefore, Cloud can bring some potential security threats to the organisation by not having an organisation specific firewall [44].

B. IaaS firewall security threats and limitations

As IaaS provides several features that introduce flexibility into the cloud infrastructure, it initiates complexity in firewall configuration and installation. Due to the large scale of IaaS infrastructure, a simple policy can lead to a large number of fine-grained rules [45].
The effectiveness of firewall security depends on its policies. However, firewall policies are often error prone due to the complex nature of firewall configurations as well as the lack of systematic analysis mechanisms and tools [46]. In a distributed environment, detecting anomalies in firewalls has become a complex task [47]. According to an empirical study of middle-box failures over two years in a service provider network, it was found that firewalls crash more than other security systems, such as IPDS and VPN, and that 33% of firewall failures are due to misconfiguration, faulty failovers and software version mismatch [48]. Therefore, the firewall policy management area is an evolving research field, as policy correctness and consistency among firewall systems is an essential element for enhancing firewall security [49, 50]. To get a cloud firewall policy configuration pattern, intensive experiments are needed to make security policy complete [51].
Therefore, several researchers are concerned with improving firewall policy strategies; for example, the Tree-Rule firewall, which uses the NF-IP-FORWARD algorithm to improve the performance of firewalls in cloud policy configurations [52].
Another main problem with firewalls in cloud computing is their placement; too few firewalls can cause a large number of communication flows. The placement of firewalls in cloud computing is critical in maximising the security benefits they offer. Traditional firewall placement is not sufficient in cloud computing, as it will introduce traffic overhead to the network switches and hypervisors [45].
A major network security risk in cloud computing is due to the limits of traditional firewall connections [53]. Traditional firewall settings are not sufficient for optimal fine-grained decisions and application-level as they are not able to deal with dynamically opened server ports for encrypted connections [54].
Several researches consider firewalls and VLAN to be less effective in the cloud environment, as a consequence for time consuming in configuration and management, limitation of the geographic zones, limitation to the number of users and static nature [9, 19, 38, 55].
The firewalls can be breached in cloud environments by a mechanism using UDP coordinating with TCP [56]. An analytical experiment shows that there is a time interval where LVMM is not under firewall protection. A firewall cannot differentiate normal traffic from attack traffic if it accesses the network through port 80 [57]. Moreover, 42% of firewall failures are due to DDoS attack at the network layer [48]. Traditional packet-level firewall mechanisms are not suitable for cloud platforms in cases of complex attacks [58].

The limitations of firewall configuration in cloud computing according to this investigation are summarised in Fig. 3. We can notice that traditional access control enforcement mechanisms are not sufficient in cloud computing. Therefore, there is a need to redesign a firewall system that suits IaaS characteristics.

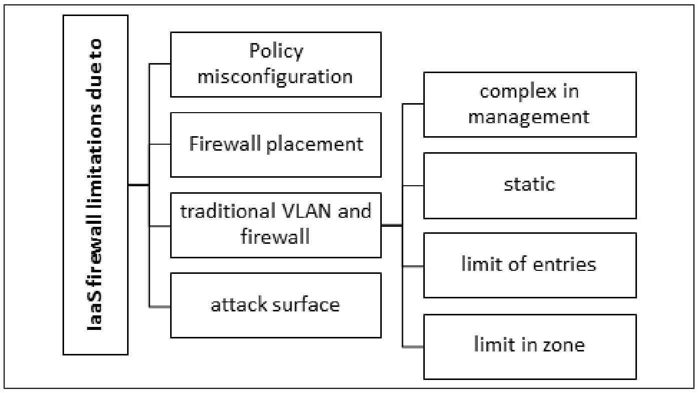

Fig. 3: IaaS firewall limitations

C. IaaS firewall approaches

Cloud users, such as companies and governments, might not rely on cloud-based firewalling approaches as these approaches still experience severe performance and reliability issues [59].
Ensuring network security in the current complex infrastructure which involves different vendors and cloud service providers (CSP) turns out to be difficult and time-consuming. Each CSP has their own API to manage the security mechanisms, such as traditional firewalls, virtual firewalls and security tools. Therefore, what looks like a simple application change may require tens or even hundreds of configurations [60].
As shown by Table 1, IaaS firewall approaches from the literature agree that the traditional firewall needs to be improved or replaced in order to cope with the IaaS environment. A trend of deploying virtual firewall is illustrated in most of the approaches. The firewall virtualisation allows dynamic deployment, so it suits IaaS characteristics and it can effectively improve firewall configuration [59, 61].
Most of the academic research assumes that the insiders in cloud service providers are not trusted [1, 18, 44]. To improve the trust in the cloud environment, a bridge virtual firewall can be designed and installed on the virtual machine in IaaS so that the cloud user can have full control on their firewall [44]. Bridge firewall improves the performance, but it limits the security of the live migration as this type of firewall cannot manage different types of policies. Moreover, massive attacks may compromise virtual firewall if they originate from outside the virtual domain [59].
The virtual firewall side effect can be mitigated if a proper firewall is designed among virtual machines and suitable firewall policies are defined [51].
Table 1 indicates the two approaches discussed regarding firewall systems administration in IaaS, which are centralised and distributed. The centralised approach was found to be less prone to misconfiguration failure as it monitored continually [48].
On the other hand, it has several drawbacks: it may lead the centralised controller to reach a bottleneck, it attracts more DDoS attacks and can introduce a single point of failure [9]. The centralised firewall set-up is argued to be unfeasible in the cloud due to performance and cost issues [62].
The distributed approach is used by many enterprises on the network edge [45]. To handle dynamic policy update in IaaS, a distributed firewall needs a complicated revocation and re-

propagation mechanism [63].

TABLE I: Firewall approaches in dynamic network

Ref.	Main problem	Proposed solution	Admin type
[9]	Conventional network access contorl: firewall and VLAN face several limitation in IaaS	Take the policy enforcement point out from the network and place it into the hypervisor	Centralised
[63]	Network states and traffic are frequently changed	Firewall Framework to cope up with SDN envirnomnt	Centralised
[45]	fine-grained rules are needed by CSP to get better control over individual network flows	For better scalability and performance, place the access control policy on both hypervisor and switch	Centralised
[59]	Cloud firewalling suffers from performance and reliability issues	Propose a framework consisting of phyical firewall and virtual firewall	Centralised
[58]	Packet level firewall mechanisism can not handle a complex attack on the cloud	Cloud firewall framework involves event level detection chain with dynamic resource allocation	Not mentioned
[18]	Network topology is not well defined, insiders are not trusted. Policies in Conventional firewalls are static and can not adapt to real-time threats	Propose a distributed firewall with a distributed active response by moving policy enforcement point from network firewall to end host	Distributed
[44]	CSP is not fully trusted	Propose a firewall system monitored by the cloud customers	Distributed

continued on next column

V. IAAS ACCESS CONTROL

The big picture of information security involves four issues: access to the system, secure communication, security management and development of secure information [64].Therefore, secure access is a critical element in building the overall security system.

Furthermore, the security techniques used in cloud can be classified into six based on the implemented security mechanism: encryption, signature, Intrusion Detection System (IDS)/Intrusion Preventions System (IPS), access control, authentication and trusted computing [65]. Thus, the access control is one of the basic security techniques in any computing system.

Authentication, access control, and audit together provide the foundation for information and system security. Consequently, access control is applied after authentication has been established [66]. In cloud computing, the authentication technique is fulfilled through identity management that supports access control based on user attributes [67]. Vaquero studied several virtualised (multitenant) datacentres and concluded that most reported systems employed access control techniques to secure their environment [19]. Fig. 4 illustrated that access control is one of the core elements in the big picuter of the information and systems security.

As has been discussed in IaaS security challenges in this article, it was found that an appropriate access control mechanism is needed to mitigate most of the explored threats. Unfortunately, the classical access control models such as mandatory, discretionary and role-based are not suitable for IaaS due to its characteristics [68–70].

Several attributes should be taken into consideration to set up proper access control for the cloud environment [9, 71, 72]. These are:

- The method of access to the cloud and cloud architecture. The users in the cloud are identified by their attributes or their characteristics, not by fixed

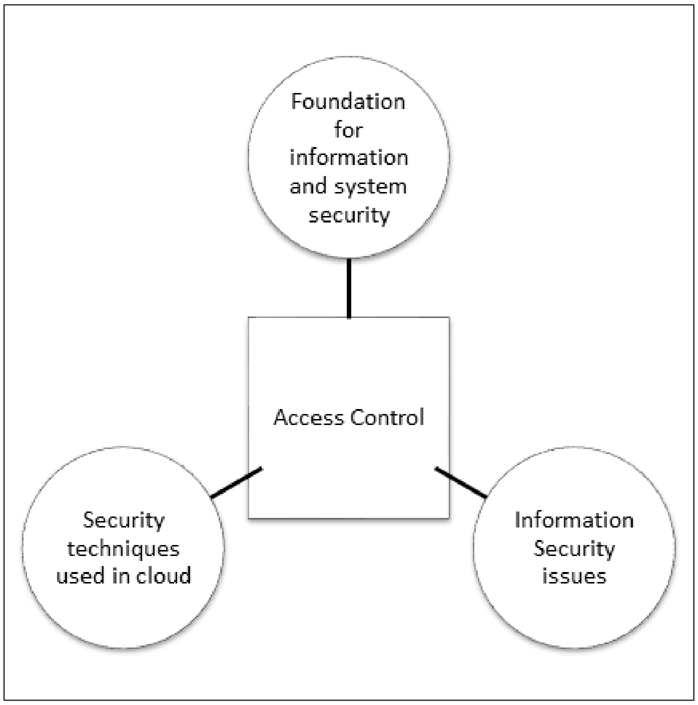
Foundation for information and system security
Access Control
Security techniques used in cloud
Information Security issues

Fig. 4: Access control in security body

IP address. Therefore, a dynamic access control is needed to achieve cross-domain authentication. The cloud access control should be network independence.

- The multi-tenancy feature in IaaS requires flexibility in seating access policy as different users are sharing the same infrastructure, although they are most probably not from the same organisation or country.

TABLE II: Access Control Approaches in IaaS

Ref.	Main problem	Proposed solution
[73]	Cloud server and the data owner are not in the same trusted domain, so server can not enforce access policy	Fine-grained attribute-based access controls mechanism
[12]	Obtain virial recources in a secure manner	Propose attribute-based constraints specification and enforcement
[10]	Multi-tenancy risks that arise in cloud IaaS	Attribute-based constraints specification and enforcement mechanism
[74]	Need to facilitate secure sharing between tenants	Propose access control models for secure information and resource sharing
[69]	Traditional access control model such as MAC, DAC and RBAC are not suitable for cloud	a framework based on the dynamic trustworthiness of users
[75]	Need for unified access control and authorisation of IaaS clouds	Propose a hybrid access control framework, named iHAC, which combines the advantages of both Role-based Access Control (RBAC) and Type Enforcement (TE) model
[68]	Classical access control models are not sufficient for dynamic environments such as cloud	An approach called CatBAC (CategoryBased Access Control), for building dedicated access control models starting from an abstract meta-model.
[76]	Ill-suited for addressing multifarious security breaches in the cloud	Proposes dynamic access control basid on semantic context-aware access control architecture

continued on next column

Table 2 summarises several IaaS access control approaches. The access control models based on the attribute are recommended by several researchers [10, 12, 70, 73]. On the other hand, it was claimed by Khamadja [68] that even the attribute-based model is not sufficient for cloud computing. Moreover, even identity-based security cannot be used in an open cloud computing environment [71]. The access control model used by most commercial clouds is the role-base model (Amazon, Verizon, Racspace, DimansionData) and the sub-users model (Joyent, Fujitsu, Softlayer, HP) while Google has its own model via OAuth2 [1].

VI. DISCUSSION AND OPEN RESEARCH

Infrastructure as a Service (IaaS) is a trend for infrastructure outsourcing. Its flexible characteristics add great benefits in deploying and managing resources from a business perspective. On the other hand, IaaS infrastructure brings with it several security challenges as it changes frequently, is shared among different customers, enables virtual machine configuration and allows virtual machine to move easily. As an example, for IaaS operations, live virtual machine migration (LVMM) can be attacked through the network link or through the physical host or even as a result of inconsistent policy configurations.

To mitigate these security challenges, a proper access control model and an enforcement mechanism are essential to enhance IaaS security. In this paper, the firewall as an access control enforcement mechanism is explored and the access control models for cloud computing are investigated. Through this investigation, it has been observed that the firewall faces several limitations in the cloud environment and even the firewall service offered by commercial clouds in form of security group has limited functionalities.

The finding illustrates that cloud firewall system should offer flexibility to the customer in addition to an acceptable level of trust. The virtual firewall as well adds an advantage to IaaS if it is designed and implemented accurately to be aligned with IaaS characteristics. The cloud firewall should also be built on a suitable access control policy to alleviate the security challenges faced by IaaS.

The centralised and the distributed administration approaches for a firewall system offer some useful gains alongside their limitations. We can point out that the distributed administrations approach for firewall looks to be more effective than the centralized one in the IaaS environment.

Researchers have proposed several approaches to putting forward a cloud firewall system. However, academic researchers recommend to take access control out of the network and place it in the hypervisor, basically into the host [9, 18, 75].

Moreover, the traditional access control models are not adequate for implementation in the cloud environment. Researchers have proposed several cloud access controls, but still some commercial clouds deploy a classic role-based access control model. Therefore, it is recommended to perform a thorough exploration on the proposed access control to come up with an improved model that is suitable for IaaS and can attract the commercial cloud to deploy it.

We recommend employing an intelligence security approach in implementing and monitoring the access control in IaaS to respond to the challenges faced by traditional firewalls and access control models. Intelligence security is a fertile approach, as most of the existing security paradigms suffer from reactive and fragmented approaches [77]. The cloud service provider may become a convenient candidate for offering security intelligence [78]. In a frequently changing infrastructure, it will be an advantage to deploy an agent-based mechanism [13].

VII. Conclusion

We have investigate access control in Infrastructure as a Service (IaaS) which covers enforcement techniques based on firewall and implemented access control models. It has been found that traditional firewall and access control mechanisms are not appropriate to enhance the security of IaaS due to cloud-specific characteristics which differ from regular data centres by providing an elasticity, multi-tenancy, configurability and dynamicity infrastructure. Ultimately, we endorse the use of computational intelligence for improving the proposed models and mechanisms to cope with this new computing environment provided by IaaS.

References

[1] W. Huang, A. Ganjali, B. H. Kim, S. Oh, and D. Lie, "The state of public infrastructure-as-a-service cloud security," *ACM Computing Surveys (CSUR)*, vol. 47, no. 4, p. 68, 2015.

[2] S.-S. Yeo and J. H. Park, "Security considerations in cloud computing virtualization environment," in *Grid and Pervasive Computing*, Springer, 2013, pp. 208–215.

[3] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "Nist cloud computing reference architecture: Recommendations of the national institute of standards and technology (special publication 500-292)," 2012.

[4] N. Leavitt, "Is cloud computing really ready for prime time?" *Computer*, no. 1, pp. 15–20, 2009.

[5] Y. Zhang, R. Krishnan, and R. Sandhu, "Secure information and resource sharing in cloud infrastructure as a service," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, ACM, 2014, pp. 81–90.

[6] R. Dukaric and M. B. Juric, "Towards a unified taxonomy and architecture of cloud frameworks," *Future Generation Computer Systems*, vol. 29, no. 5, pp. 1196–1210, 2013.

[7] R. Buyya, J. Broberg, and A. M. Goscinski, *Cloud computing: Principles and paradigms*. John Wiley & Sons, 2010, vol. 87.

[8] D. Owens and B. Americas, "Securing elasticity in the cloud," *Communications of the ACM*, vol. 53, no. 6, 2010.

[9] L. Popa, M. Yu, S. Y. Ko, S. Ratnasamy, and I. Stoica, "Cloudpolice: Taking access control out of the network," in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, ACM, 2010, p. 7.

[10] K. Bijon, R. Krishnan, and R. Sandhu, "Mitigating multi-tenancy risks in iaas cloud through constraints-driven virtual resource scheduling," in *Proceedings of the 20th ACM Symposium on Access Control Models and Technologies*, ACM, 2015, pp. 63–74.

[11] S. Zhang, X. Zhang, and X. Ou, "After we knew it: Empirical study and modeling of cost-effectiveness of exploiting prevalent known vulnerabilities across iaas cloud," in *Proceedings of the 9th ACM symposium on Information, computer and communications security*, ACM, 2014, pp. 317–328.

[12] K. Bijon, R. Krishnan, and R. Sandhu, "Virtual resource orchestration constraints in cloud infrastructure as a service," in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, ACM, 2015, pp. 183–194.

[13] F. Doelitzscher, C. Reich, M. Knahl, A. Passfall, and N. Clarke, "An agent based business aware incident detection system for cloud environments," *Journal of Cloud Computing*, vol. 1, no. 1, pp. 1–19, 2012.

[14] H. Raj and K. Schwan, "Extending virtualization services with trust guarantees via behavioral monitoring," in *Proceedings of the 1st EuroSys Workshop on Virtualization Technology for Dependable Systems*, ACM, 2009, pp. 24–29.

[15] T. Erl, R. Puttini, and Z. Mahmood, *Cloud computing: Concepts, technology, & architecture*. Pearson Education, 2013.

[16] J. Oberheide, E. Cooke, and F. Jahanian, "Empirical exploitation of live virtual machine migration," in *Proc. of BlackHat DC convention*, Citeseer, 2008.

[17] A. X. Liu, "Firewall policy change-impact analysis," *ACM Transactions on Internet Technology (TOIT)*, vol. 11, no. 4, p. 15, 2012.

[18] J. L. Thames, R. Abler, and D. Keeling, "A distributed firewall and active response architecture providing pre-

emptive protection," in *Proceedings of the 46th Annual Southeast Regional Conference on XX*, ACM, 2008, pp. 220–225.

[19] L. M. Vaquero, L. Rodero-Merino, and D. Morán, "Locking the sky: A survey on iaas cloud security," *Computing*, vol. 91, no. 1, pp. 93–118, 2011.

[20] L. Wang, R. Ranjan, J. Chen, and B. Benatallah, *Cloud computing: Methodology, systems, and applications*. CRC Press, 2011.

[21] M. Anala, J. Shetty, and G. Shobha, "A framework for secure live migration of virtual machines," in *Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on*, IEEE, 2013, pp. 243–248.

[22] K. Nahrstedt and R. Campbell, "Security for cloud computing," *A Report: Directorate for Computer and Information Science and Engineering (CISE)*, pp. 1–19, 2012.

[23] V. Medina and J. M. García, "A survey of migration mechanisms of virtual machines," *ACM Computing Surveys (CSUR)*, vol. 46, no. 3, p. 30, 2014.

[24] P. Svärd, B. Hudzia, J. Tordsson, and E. Elmroth, "Evaluation of delta compression techniques for efficient live migration of large virtual machines," *ACM Sigplan Notices*, vol. 46, no. 7, pp. 111–120, 2011.

[25] Z. Tavakoli, S. Meier, and A. Vensmer, "A framework for security context migration in a firewall secured virtual machine environment," in *Information and Communication Technologies*, Springer, 2012, pp. 41–51.

[26] M. Ver, "Dynamic load balancing based on live migration of virtual machines: Security threats and effects," 2011.

[27] A. Duncan, S. Creese, M. Goldsmith, and J. S. Quinton, "Cloud computing: Insider attacks on virtual machines during migration," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on*, IEEE, 2013, pp. 493–500.

[28] D. Perez-Botero, "A brief tutorial on live virtual machine migration from a security perspective," *University of Princeton, USA*, 2011.

[29] F. Zhang, Y. Huang, H. Wang, H. Chen, and B. Zang, "Palm: Security preserving vm live migration for systems with vmm-enforced protection," in *Trusted Infrastructure Technologies Conference, 2008. APTC'08. Third Asia-Pacific*, IEEE, 2008, pp. 9–18.

[30] H. Zhou, J. Wang, and H. Zhang, "A trusted vm-vtpm live migration protocol in clouds," in *Int. Workshop on Cloud Computing and Information Security (CCIS)*, 2013, pp. 9–11.

[31] W. Wang, Y. Zhang, B. Lin, X. Wu, and K. Miao, "Secured and reliable vm migration in personal cloud," in *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on*, IEEE, vol. 1, 2010, pp. V1–705.

[32] P. Schoo, V. Fusenig, V. Souza, M. Melo, P. Murray, H. Debar, H. Medhioub, and D. Zeghlache, "Challenges for cloud networking security," in *Mobile Networks and Management*, Springer, 2010, pp. 298–313.

[33] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1–13, 2013.

[34] B. Sulaiman, N. Azman, and H. Masuda, "Evaluation of a secure live migration of virtual machines using ipsec implementation," in *Advanced Applied Informatics (IIAIAAI), 2014 IIAI 3rd International Conference on*, IEEE, 2014, pp. 687–693.

[35] P. H. Shah, "Security in live virtual machine migration," PhD thesis, Wichita State University, 2011.

[36] K. Xu, C. Lin, Z. Chen, K. Meng, and M. Hakmaoui, "An effective policy relocation scheme for vm migration in software-defined networks," in *Computer Communication and Networks (ICCCN), 2015 24th International Conference on*, IEEE, 2015, pp. 1–8.

[37] Y. Jarraya, A. Eghtesadi, S. Sadri, M. Debbabi, and M. Pourzandi, "Verification of firewall reconfiguration for virtual machines migrations in the cloud," *Computer Networks*, vol. 93, pp. 480–491, 2015.

[38] X. Liu, J. Huai, Q. Li, and T. Wo, "Network state consistency of virtual machine in live migration," in *Proceedings of the 2010 ACM Symposium on Applied Computing*, ACM, 2010, pp. 727–728.

[39] B. Danev, R. J. Masti, G. O. Karame, and S. Capkun, "Enabling secure vm-vtpm migration in private clouds," in *Proceedings of the 27th Annual Computer Security Applications Conference*, ACM, 2011, pp. 187–196.

[40] P. A. Boampong and L. A. Wahsheh, "Different facets of security in the cloud," in *Proceedings of the 15th communications and networking simulation symposium*, Society for Computer Simulation International, 2012, p. 5.

[41] W. Paim de Jesus, D. Alves da Silva, R. T. de Sousa, and F. V. Lopes Da Frota, "Analysis of sdn contributions for cloud computing security," in *Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on*, IEEE, 2014, pp. 922–927.

[42] J. Cropper, J. Ullrich, P. Fruhwirt, and E. Weippl, "The role and security of firewalls in iaas cloud computing," in *Availability, Reliability and Security (ARES), 2015 10th International Conference on*, IEEE, 2015, pp. 70–79.

[43] R. Li, D. Abendroth, X. Lin, Y. Guo, H.-W. Baek, E. Eide, R. Ricci, and J. Van der Merwe, "P otassium: Penetration testing as a service," in *Proceedings of the Sixth ACM Symposium on Cloud Computing*, ACM, 2015, pp. 30–42.

[44] G. Liyanage and S. Fernando, "Firewall model for cloud computing," in *Industrial and Information Systems (ICIIS), 2013 8th IEEE International Conference on*, IEEE, 2013, pp. 86–91.

[45] M. Moshref, M. Yu, A. Sharma, and R. Govindan, "Vcrib: Virtualized rule management in the cloud," in *Presented as part of the*, 2012.

[46] H. Hu, G.-J. Ahn, and K. Kulkarni, "Detecting and resolving firewall policy anomalies," *Dependable and Secure Computing, IEEE Transactions on*, vol. 9, no. 3, pp. 318–331, 2012.

[47] F. B. Ftima, K. Karoui, and H. B. Ghzela, "A secure mobile agents approach for anomalies detection on firewalls," in *Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services*, ACM, 2008, pp. 689–693.

[48] R. Potharaju and N. Jain, “Demystifying the dark side of the middle: A field study of middlebox failures in datacenters,” in *Proceedings of the 2013 conference on Internet measurement conference*, ACM, 2013, pp. 9–22.

[49] A. S. Sairam, R. Kumar, and P. Biswas, “Implementation of an adaptive traffic-aware firewall,” in *Proceedings of the 7th International Conference on Security of Information and Networks*, ACM, 2014, p. 385.

[50] Q. Duan and E. Al-Shaer, “Traffic-aware dynamic firewall policy management: Techniques and applications,” *Communications Magazine, IEEE*, vol. 51, no. 7, pp. 73–79, 2013.

[51] H.-C. Li, P.-H. Liang, J.-M. Yang, and S.-J. Chen, “Analysis on cloud-based security vulnerability assessment,” in *E-Business Engineering (ICEBE), 2010 IEEE 7th International Conference on*, IEEE, 2010, pp. 490–494.

[52] X. He, T. Chomsiri, P. Nanda, and Z. Tan, “Improving cloud network security using the tree-rule firewall,” *Future generation computer systems*, vol. 30, pp. 116–126, 2014.

[53] D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, and P. R. Inácio, “Security issues in cloud environments: A survey,” *International Journal of Information Security*, vol. 13, no. 2, pp. 113–170, 2014.

[54] J. Wiebelitz, M. Brenner, C. Kunz, and M. Smith, “Early defense: Enabling attribute-based authorization in grid firewalls,” in *Proceedings of the 19th ACM International Symposium on High Performance Distributed Computing*, ACM, 2010, pp. 336–339.

[55] J. Nielsen and T. Hacker, “Using virtual private networks for reliable vm based hpc systems,” in *High Performance Computing, Networking, Storage and Analysis (SCC), 2012 SC Companion:*, IEEE, 2012, pp. 1226–1233.

[56] J. Long, L.-d. Wang, and Z.-d. Li, “Research and design of the firewall penetration technology serving to distributed cloud resource,” in *Proceedings of the 5th Asia-Pacific Symposium on Internetware*, ACM, 2013, p. 16.

[57] C. N. Modi, D. R. Patel, A. Patel, and M. Rajarajan, “Integrating signature apriori based network intrusion detection system (nids) in cloud computing,” *Procedia Technology*, vol. 6, pp. 905–912, 2012.

[58] S. Yu, R. Doss, W. Zhou, and S. Guo, “A general cloud firewall framework with dynamic resource allocation,” in *Communications (ICC), 2013 IEEE International Conference on*, IEEE, 2013, pp. 1941–1945.

[59] F. Guenane, H. Boujezza, M. Nogueira, and G. Pujolle, “An architecture to manage performance and reliability on hybrid cloud-based firewalling,” in *Network Operations and Management Symposium (NOMS), 2014 IEEE*, IEEE, 2014, pp. 1–5.

[60] R. Harrison, “Reducing complexity in securing heterogeneous networks,” *Network Security*, vol. 2015, no. 10, pp. 11–13, 2015.

[61] Z. Wang, Z. Lu, J. Wu, and K. Fan, “Cpfirewall: A novel parallel firewall scheme for fwaas in the cloud environment,” in *Advances in Services Computing*, Springer, 2015, pp. 121–136.

[62] M. Liu, W. Dou, S. Yu, and Z. Zhang, “A decentralized cloud firewall framework with resources provisioning cost optimization,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 26, no. 3, pp. 621–631, 2015.

[63] H. Hu, W. Han, G.-J. Ahn, and Z. Zhao, “Flowguard: Building robust firewalls for software-defined networks,” in *Proceedings of the third workshop on Hot topics in software defined networking*, ACM, 2014, pp. 97–102.

[64] M. T. Siponen and H. Oinas-Kukkonen, “A review of information security issues and respective research contributions,” *ACM Sigmis Database*, vol. 38, no. 1, pp. 60–80, 2007.

[65] C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu, “From security to assurance in the cloud: A survey,” *ACM Computing Surveys (CSUR)*, vol. 48, no. 1, p. 2, 2015.

[66] R. Sandhu and P. Samarati, “Authentication, access control, and audit,” *ACM Computing Surveys (CSUR)*, vol. 28, no. 1, pp. 241–243, 1996.

[67] A. N. Toosi, R. N. Calheiros, and R. Buyya, “Interconnected cloud computing environments: Challenges, taxonomy, and survey,” *ACM Computing Surveys (CSUR)*, vol. 47, no. 1, p. 7, 2014.

[68] S. Khamadja, K. Adi, and L. Logrippo, “Designing flexible access control models for the cloud,” in *Proceedings of the 6th International Conference on Security of Information and Networks*, ACM, 2013, pp. 225–232.

[69] R. Banyal, V. Jain, and P. Jain, “Dynamic trust based access control framework for securing multi-cloud environment,” in *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies*, ACM, 2014, p. 29.

[70] N. Miloslavskaya, M. Senatorov, A. Tolstoy, and S. Zapechnikov, “Big data information security maintenance,” in *Proceedings of the 7th International Conference on Security of Information and Networks*, ACM, 2014, p. 89.

[71] N. Meghanathan, “Review of access control models for cloud computing,” *Computer Science & Information Science*, vol. 3, no. 1, pp. 77–85, 2013.

[72] I. Iankoulova and M. Daneva, “Cloud computing security requirements: A systematic review,” in *Research Challenges in Information Science (RCIS), 2012 Sixth International Conference on*, IEEE, 2012, pp. 1–7.

[73] K. Yang, X. Jia, and K. Ren, “Attribute-based fine-grained access control with efficient revocation in cloud storage systems,” in *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, ACM, 2013, pp. 523–528.

[74] Y. Zhang, R. Krishnan, and R. Sandhu, “Secure information and resource sharing in cloud,” in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, ACM, 2015, pp. 131–133.

[75] C. Zhou and B. Li, “Ihac: A hybrid access control framework for iaas clouds,” in *Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, IEEE Computer Society, 2014, pp. 853–858.

[76] M. Auxilia and K. Raja, “Dynamic access control model for cloud computing,” in *Advanced Computing (ICoAC),*

2014 Sixth International Conference on, IEEE, 2014, pp. 47–56.

[77] R. Knights and E. Morris, “Move to intelligence-driven security,” *Network Security*, vol. 2015, no. 8, pp. 15–18, 2015.

[78] S. Cates, “The evolution of security intelligence,” *Network Security*, vol. 2015, no. 3, pp. 8–10, 2015.