Applied Computing and Informatics (2017) 13, 57–65

Saudi Computer Society, King Saud University

Applied Computing and Informatics

(http://computer.org.sa)
www.ksu.edu.sa
www.sciencedirect.com

ORIGINAL ARTICLE

Multilevel classification of security concerns in cloud computing

Syed Asad Hussain [a,*], Mehwish Fatima [a], Atif Saeed [b], Imran Raza [a], Raja Khurram Shahzad [c]

[a] Department of Computer Science, COMSATS Institute of Information Technology Lahore, Pakistan
[b] School of Computing and Communications, Lancaster University, Lancaster, United Kingdom
[c] School of Computing, Blekinge Institute of Technology, Sweden

Received 11 May 2015; revised 11 March 2016; accepted 20 March 2016
Available online 8 April 2016

KEYWORDS

Cloud computing;
Security;
Virtualization;
SaaS;
PaaS;
IaaS

Abstract Threats jeopardize some basic security requirements in a cloud. These threats generally constitute privacy breach, data leakage and unauthorized data access at different cloud layers. This paper presents a novel multilevel classification model of different security attacks across different cloud services at each layer. It also identifies attack types and risk levels associated with different cloud services at these layers. The risks are ranked as low, medium and high. The intensity of these risk levels depends upon the position of cloud layers. The attacks get more severe for lower layers where infrastructure and platform are involved. The intensity of these risk levels is also associated with security requirements of data encryption, multi-tenancy, data privacy, authentication and authorization for different cloud services. The multilevel classification model leads to the provision of dynamic security contract for each cloud layer that dynamically decides about security requirements for cloud consumer and provider.

1. Introduction

Cloud computing is a broad paradigm based on models for providing services of storage and platform software. Cloud computing concept has emerged from distributed and grid computing domains that are already in use for mail servers, web storage and hosting services. Cloud computing, as defined by NIST, is referred to as: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].

* Corresponding author.
E-mail addresses: asadhussain@ciitlahore.edu.pk (S.A. Hussain), mehwish.fatima@ciitlahore.edu.pk (M. Fatima), a.saeed2@lancs.ac.uk (A. Saeed), iraza@ciitlahore.edu.pk (I. Raza), khurram.shahzad@bth.se (R.K. Shahzad).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.aci.2016.03.001

01
Wimalasekera

In cloud computing, clouds can be described at different layers, i.e., SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). Although applications for clouds are in development phase, however security requirements for the data and services on the clouds are getting attention of researchers and it has become necessary to consider each layer of a cloud for possible attacks. It is worth noting that cloud computing systems have many advantages; however, large organizations are still hesitant to shift their setups on the cloud mainly due to security issues and risks. Thus, it is important to address the security issues and problems in cloud systems, and to find a solution for the widespread acceptance of these solutions. However, being a new domain, the research on the requirements and issues regarding security of clouds is still in its early stages.

In the literature, there are different classifications of cloud security attacks [2–7] targeting a specific cloud service or a particular kind of the cloud system. Thus there is a need for a more comprehensive classification of security attacks across versatile cloud services at each layer. This paper proposes a multilevel classification of security attacks for different cloud services and their associated risks at cloud layers. It also discusses provision of dynamic security contract for each cloud layer that dynamically decides about security requirements for cloud consumer and provider.

2-3
2 notes:

The rest of paper is structured as follows: Section 2 consists of related work. Section 3 presents the proposed multilevel classification of security concerns in cloud computing. Section 4 is based on the dynamic security contract concept. Section 5 concludes the paper.

4-5
2 notes:

2. Related work

The application softwares at SaaS are provided with a specific license based subscription, pay-as-go [8]. Platform as a Service (PaaS) caters services for operating system, network capacity, storage and multi-tenancy via the Internet. Infrastructure as a service (IaaS) provides utility computing, automation of administrative tasks, dynamic scaling, desktop virtualization, policy-based services, and Internet connectivity. IaaS provides virtual servers with unique IP address and storage pool as required by customers. The concept of infrastructure and hardware layer is mentioned by different researchers. Some authors have suggested that the infrastructure layer offers system software services and hardware layer provides hardware-based services. Infrastructure and hardware layers may be combined due to intrinsic relationship between hardware and software.

In [9], security aspects of one of the popular cloud Amazon Elastic Compute Cloud (EC2) have been discussed. It consists of systematic analysis of various crucial vulnerabilities in publicly available Amazon Machine Images (AMIs) and mechanisms to eliminate them. The proposed tool referred to as Amazon Image Attacks (AmazonIA) uses only publicly available interfaces regardless of the underlying cloud infrastructure. As a result of exploiting vulnerabilities and successful attacks, authors are able to extract sensitive information including passwords, and credentials from AMIs. The extracted information can be used to initiate botnets, or create back doors to launch impersonate attacks or access source code of a web service available on AMI. The authors have discussed effects of successful attacks and also the methods to mitigate those attacks. Some research groups have worked on the interfaces of both public and private clouds [10]. The public cloud under their consideration is Amazon, while the private cloud is Eucalyptus.

Authors in [11] consider security as a service for cloud-based applications. The architecture considers the existing services at different levels. It considers user-centric security i.e., users have control over their security permitting them to use security solutions across different clouds. They can subscribe to any security solution provided by any cloud provider and use that particular security solution for their cloud and may also have multiple security solutions for a particular service depending upon its criticality. The multiple security solutions can also be used at different levels.

Authors in [9] address the security and privacy aspects of real-life cloud deployments, while ignoring the malicious cloud providers or customers. Here authors' focus is Amazon Elastic Compute Cloud (EC2). They have analyzed the crucial vulnerabilities of Amazon Machine Images (AMIs) through an automated tool and as a result of attack information regarding API Keys, private keys and credentials of publishers were extracted [9]. Vulnerabilities were discovered in Secure Shell. The extracted information can be further used to create multiple security threats resulting in botnet instances, access of backend services or code of the Web sites through back-door content.

In [12] authors suggest that security should be provided as a service and propose a model for security as service. Security as a service implies that the security applications and services can be provided by a cloud vendor, or cloud consumer or even by a third trust-worthy party. The security service can be in the form of a cloud-based infrastructure or software. The authors have proposed a component based software model in which authorization components can be developed by any party regardless of being a service provider. An eXtensible access control markup language (XACML) decision engine that is composed of a context handler, a policy decision point and a policy administration point, can be furnished by reusable components to augment the security service. By XACML standard attributes of subjects, resources and environments and authorization rules can be defined as Boolean expressions. Thus, these types of security services, which can be managed and altered by cloud customers, are helpful to build trust of cloud customers on cloud systems.

In [3] Cloud Computing Open Architecture (CCOA) concept is discussed for clouds in virtual environments. The role and functions of the architecture are discussed according to different infrastructures for IT and business systems. Different types of architectures complicate security management for cloud systems. This architecture provides a solution for different security aspects regarding virtual environments. The authors suggest physical and logical isolation of data instances for each customer to enhance the data privacy and expeditious replication and recovery system. Authorized users based on the role-based access control can access the sensitive data on platforms. To prevent intrusion attacks, cloud service provider blocks the malicious and un-trusted codes enabling digital forensic applications.

Research in [14] suggests a trusted computing and attestation system for virtual environments. In virtual environments systems are more prone to threats due to the poor computer communication architectures and hidden network channels. These hidden channels can be a risk since many virtualized network channels can be easily observed and hacked.

3. A multilevel classification of security concerns in cloud computing

Cloud systems have a layered architecture of different services and control levels for users. Fig. 1 illustrates the classification model of security problems at each layer of the cloud system. SaaS, PaaS and IaaS layers are considered for associated security risks and problems.

3.1. Security concerns for Software as a Service (SaaS)

SaaS is exposed by attacks on API's, publishers, web portals and interfaces. The attacks on the SaaS are categorized into two broad groups: attacks on development tools and attacks on management tools. Most popular services on SaaS are web services, web portals and APIs. Intruders' attempt unauthorized access and gain of services by attacking web portals and APIs. These attacks affect data privacy. Intruders try to extract the sensitive information of API Keys, private keys, and credentials of publishers via different kinds of attacks and automated tools. Another possibility of attack on this layer is exposure of secure shell for extracting key credentials.

3.1.1. Data protection

In cloud computing applications are deployed in shared resource environments; therefore, data privacy is an important aspect. Data privacy has three major challenges: integrity, authorized access and availability (backup/ replication). Data integrity ensures that the data are not corrupted or tampered during communication. Authorized access prevents data from intrusion attacks while backups and replicas allow data access efficiently even in case of a technical fault or disaster at some cloud location. Data are shared and communicated at the common network backbone. Hence malicious attackers or intruders can deploy hidden proxy applications between the cloud provider and consumer to scavenge information of login credentials and session details [4]. An intruder can also perform packet sniffing or IP-spoofing as a middle-party and can access and/or alter the restricted or sensitive information. One possible solution for the data privacy in cloud computing is Cisco Secure Data Center Framework that provides multilayer security mechanism [4].

3.1.2. Attacks on interfaces

A successful attack on the cloud interfaces can result in a root level access of a machine without initiating a direct attack on the cloud infrastructure. Two different kinds of attacks are launched on authentication mechanism of clouds. The control interfaces are vulnerable to signature wrapping and advanced cross site scripting (XSS) techniques. First kind of attack is referred to as signature wrapping attack or XML Signature Wrapping attacks. Single signed SOAP message or X.509 certificate can be used to compromise security of customers? accounts through operations on virtual machines or resetting of passwords. Second type of attacks exploits the vulnerability in XSS. The particular vulnerability attack steals username and password pair information.

3.1.3. Attacks on SSH (Secure Shell)

Attacks on Secure Shell (SSH), the basic mechanism used to establish trust and connection with cloud services, are the most alarming threat that compromises control trust. According to Ponemon 2014 SSH security Vulnerability Report [15], 74 percent organizations have no control to provision, rotate, track and remove SSH keys. Cybercriminals take full advantage of these vulnerabilities and use cloud computing to launch different attacks. An organizations cloud workload can be used host botnets if SSH access has been compromised. Attackers have hosted the Zeus botnet and control infrastructure on Amazon EC2 instances [16]. The different types of attack on SSH

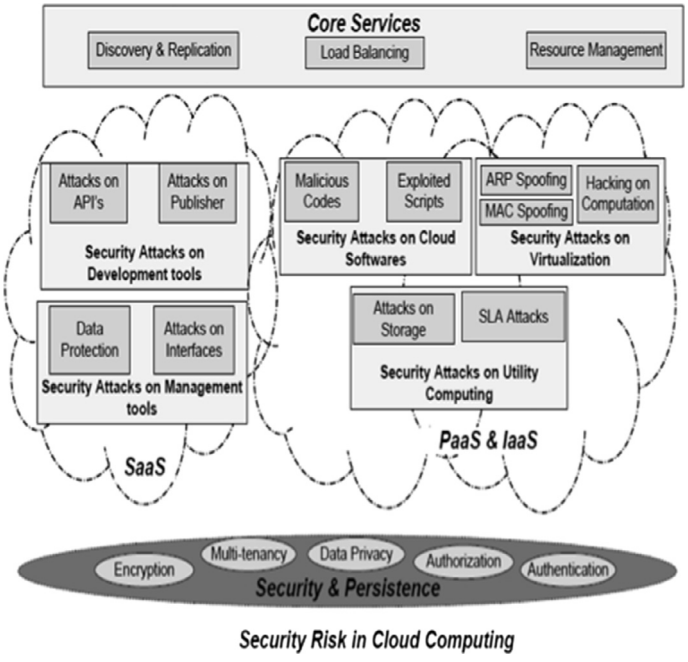

Figure 1 Classification model of attacks at each layer of the cloud system.

include attacks on API keys, attacks on user credentials, and attacks on publisher credentials.

3.2. Security concerns for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)

IaaS and PaaS layers are overlapped in the model due to their interdependency on each other. The attacks on these layers are grouped into three types: attacks on cloud services, attacks on virtualization, and attacks on utility computing. The security concerns for IaaS and PaaS are discussed below.

3.2.1. Hardware virtualization

The VMs interconnectivity is the biggest security concern in the designing of cloud computing platform. VMs are linked using bridge and route virtual network configuration modes. The bridge mode works as a virtual hub shared among all the VMs, which may result in sniffing the virtual network by a compromised VM. In the route mode, where route works as a virtual switch, each VM is connected using a dedicated virtual interface. Any network intruder in a LAN segment of a network can access virtual environments by address resolution protocol (ARP) spoofing and MAC spoofing. ARP spoofing alters the ARP tables and management interfaces and systems. On the other hand, an intruder can mimic another host through MAC spoofing and also change address of host or guest Virtual Machine (VM) to gain access of restricted resources [13]. The attacks and exploitation of virtual environments are very diversified and they will increase in future since platforms are growing in number and complexity. Therefore, a mechanism for detecting attacks along with preventions is necessary.

3.2.2. Software virtualization

A software virtualization attack may examine the VM images to launch an attack or steal of information, especially targeting development images, which are accidentally released [21]. It is also possible to provide a VM image having malware to cloud computing system resulting in theft and corruption of data. For example, cloud consumers are enticed to run tainted VM images contributed to image repository manipulating the registration process for first page listing.

3.2.3. Cloud softwares

Multi-tenancy in clouding computing requires multiplexing the execution of VMs from different consumer on the same physical server [17]. Softwares deployed on guest VM remain susceptible to attack and compromise. A malicious code in VM may interfere with the hypervisor or other VMs. Shortcomings in programming interfaces and processing of instructions are the main targets to uncover vulnerabilities [18]. This security concern also includes indirect attacks such as man-in-the-middle during a live VM migration; insertion VM based rootkit during memory modification; a zero-day exploit in HyperVM; side-channel attack to gain information.

3.2.4. Utility computing

Utility computing is the concept that emerged from grid computing, and it combines computation, storage and bandwidth to provide services on the demand through payment by the customer. It also provides two basic advantages of cost reduction and scalability. Security risk associated with utility computing is access by attackers who want to utilize resources without paying [8]. Majority of hackers and crackers use the computing power or storage for the illegal use. The common use of public cloud includes e-commerce, web-application and Web site hosting making these services vulnerable to variety of attacks on possession, authenticity, integrity and utility. A compromised client may perform a Fraudulent Resource Consumption (FRC) attack by using the metered bandwidth of web-based service that results in a financial burden on the cloud consumer [19].

3.2.5. Service Level Agreement (SLA)

SLA is an optimal way for ensuring security and trust. The implementation of SLA results in a well-designed contract of responsibilities between parties that can enhance security level. In cloud environment, SLA can be combined with the web service level agreement (WSLA) for mitigating security risks [8]. SLA defines the different levels of security and their complexity based on the services for the better understanding of the security policies to a cloud consumer. The existing cloud storage systems do not provide security guarantees in their SLAs effecting the adaptation of cloud services. A cloud storage service may leak private data, return inconsistent data or modify the data due to bugs, hacking, crashes, or misconfigurations. This security concerns require proper SLA guarantee models such as CloudProof [20].

Table 1 shows multilevel classification for the three cloud layers in terms of cloud service, types of attack, cloud type and risk levels. Cloud layers are considered as first level followed by cloud services as second level and types of attacks for these services as third. A risk is associated with each level of this classification. SaaS has low to medium risk level if it is under attack. However attacks on publisher service at this layer may adversely affect the services. Services at PaaS and IaaS layers are associated with medium to high risks.

The classification identifies the risk levels as low (less vulnerable), medium, and high (more vulnerable) depending on the exposure of cloud security requirements. Data encryption, multi-tenancy, data privacy, authentication, and authorization are the security requirements for cloud services. The exposure of these security requirements constitutes different risk levels. For example exposure of multi-tenancy and data privacy for hardware virtualization represents high risk. These levels indicate control of a customer given by a service over the cloud system. The attacks on software layer are generally considered less severe and if the attack effects infrastructure or platform layers it has medium to high severity. However it is observed that certain attacks such as attacks on SSH for publisher credentials on software layer are highly adverse. A cloud service offered at PaaS or IaaS provides multiple ways for the exposure of cloud system. From this, it may be inferred that major attacks and threats exist on the underlying layers of a cloud system.

At second level available services on PaaS and IaaS constitute hardware virtualization, software virtualization, utility computing and development services. Some attacks on these services may be severe up to the extent that even the real machines can be affected. Most of intruders try to hack these layers with the help of ARP spoofing, MAC spoofing or executing malicious codes on cloud platforms.

Table 1 A multi-level classification of security and privacy risk in cloud computing.

Cloud layer	Cloud service	Security concerns	Attack type	Cloud type	Risk
SAAS	Web service	Data protection	Privacy	All clouds	Medium
	Web portal	Attack on interfaces	Attack on signature	AMI/EC2	Low
			Attacks on credentials	AMI/EC3	Medium
	API	Attack on SSH	Attack on API Keys	AMI/EC4	Medium
			Attack on user credentials	AMI/EC5	Medium
			Attack on publisher credentials	AMI/EC6	High
PAAS and IAAS	Platform virtualization	Hardware virtualization	ARP Spoofing on virtual switching	All	High
			MAC spoogin on virtual switching	All	Medium
		Software virtualization	Hacking on computations	All	Low
Development services	Cloud softwares	Malicious code	script	All	High
	Computation services	Utility computing	Unpaid client attacks	All	Low
		SLA	Hacking	All	High

Table 2 A mapping of cloud service and security requirements.

	Data encryption	Multi-tenancy	Data privacy	Authentication	Authorization
Security requirements					
Data protection	Yes	No	Yes	No	No
API's	No	No	No	Yes	Yes
Web portals	No	No	No	Yes	Yes
Cloud software	Yes	No	Yes	No	Yes
HardWare virtualization	No	Yes	Yes	No	No
Software virtualization	No	Yes	No	No	Yes
Virtualization	No	Yes	No	No	Yes
Utility computing	No	Yes	No	No	Yes

Web services and web portals are attacked to break encryption or to get signatures and user credentials. Attacks on SSH (Secure SHell) extract API keys, user credentials and publisher credentials. Attacks for breaking encryption, extracting signatures, keys, and credentials are associated with low to medium level risks. However attack on publisher credentials has high-level risk. Hardware virtualization is attacked through ARP spoofing and MAC spoofing. Risk level associated with hardware virtualization is medium to high. Software virtualization is threatened by hacking with automated tools and has a high level of risk. Malicious codes and scripts can be executed with development services and these may adversely affect the whole cloud system, and hence risk associated with development services is high. Utility computing is associated with high risk level and can be attacked by hacking or for SLA.

Table 2 presents a mapping of cloud services and cloud security requirements. The mentioned security requirements are mandatory to achieve the integrity and coherence in the cloud system. These security requirements are data encryption, multi-tenancy, data privacy, authentication, and authorization. Data encryption and hashing techniques are used to protect the data over the distributed system. Thus, the data protection service depends on encryption techniques and privacy policies. If data protection services or web services are attacked, the data encryption and data privacy will be compromised because intruder will try to break encryption and hashing policies. However physical data storage is not threatened so risk factor associated is medium. On the other hand, if API's and web portals are intruded, authentication and authorization requirements will be violated. API's and web portals provide a gateway to access cloud systems, thus by attacking these gateways, attackers can easily expose cloud systems. However these credentials and signatures are expired after the session so risk factor associated with these services is low to medium. Development services provide a way to create other cloud services by customers. By accessing this service, malicious scripts and codes can be executed. Attacks on development services can expose the data encryption, multi-tenancy and authentication. So this service has a high risk factor. Virtualization offers many advantages but these advantages are associated with the possibility of some threats e.g., multiple numbers of customers on a single resource can access data in an un-authorized manner. Intrusion on hardware virtualization may violate multi-tenancy requirement and data privacy and has a high risk factor. If software virtualization and utility computing are attacked, multi-tenancy and authorization are threatened. Attacks on multi-tenancy jeopardize the logical separation of multiple customers on a single resource, and hence risk factor is high.

4. Dynamic security provisioning

Dynamic Security Contract (DSC) between a cloud consumer and a provider is implemented across the layers according to consumer and provider requirements for services and security. Security gets more stringent for the services offered at cloud provider layers (PaaS and IaaS). The risk levels associated with these two layers are in the medium to high range since the attacks on the services of these layers may affect the whole cloud system. Hence level of security is determined dynami-

cally for cloud consumer and cloud provider through DSC as shown in Fig. 2.

Fig. 2 shows that the service X_1 and X_2 at SaaS layer has a specific risks R, such as attacks on APIs, attacks on interfaces, attacks on publisher, and data protection, having severity levels such as low, medium and high. DSC takes this information as input to prepare the security services at PaaS and IaaS. The service, X_1 and X_2, requested by a cloud consumer in forwarded to PaaS to allocate platform service PS_1 along with the necessary security services is defined by DSC. IaaS layer provides suitable infrastructure service IS_1 for PS_1 along with the required security services.

DSC defines the risk levels associated with each service. The DSC is constituted by X, S, A where X is the service, S is security expected/required, and A is the type of attack. In symbolic form DSA can be written as

$$DSC(X, S, A) \rightarrow R \tag{1}$$

where R is the risk level associated with a particular DSC. DSC is provisioned when a cloud service is requested by a consumer. The DSC for this request will identify security requirements for this particular service and classify the risk levels associated with the service demanded by the consumer. The risk levels change dynamically depending on the type of the service and possible attacks associated with that service. The outcome of this dynamic security assessment is decision regarding the level and type of security required for the risk. Eq. (1) for multiple services and different attack types becomes:

$$DSC\left(X, \sum S, \sum A\right) \rightarrow R \tag{2}$$

Following example illustrates the concept behind Eqs. (1) and (2). The example shows subset of web portal services and hardware virtualization consisting of possibilities of attacks and security services of authentication, authorization, multi-tenancy and data privacy. It is important to observe that risk level changes to high as cloud service changes to hardware virtualization from web portal. Hence security service dynamically switches over to multi-tenancy and data privacy.

Example:

Possible Subset for Web Portal

X = Web portal, S = Authentication, A = Attacks on Signatures, R = Low

X = Web portal, S = Authentication, A = Attacks on credentials, R = Medium

X = Web portal, S_1 = Authentication, S_2 = Authorization, A = Attacks on credentials, R = Medium

X = Web portal, S_1 = Authentication, S_2 = Authorization, A_1 = Attacks on Signatures, A_2 = Attacks on credentials, R = Medium

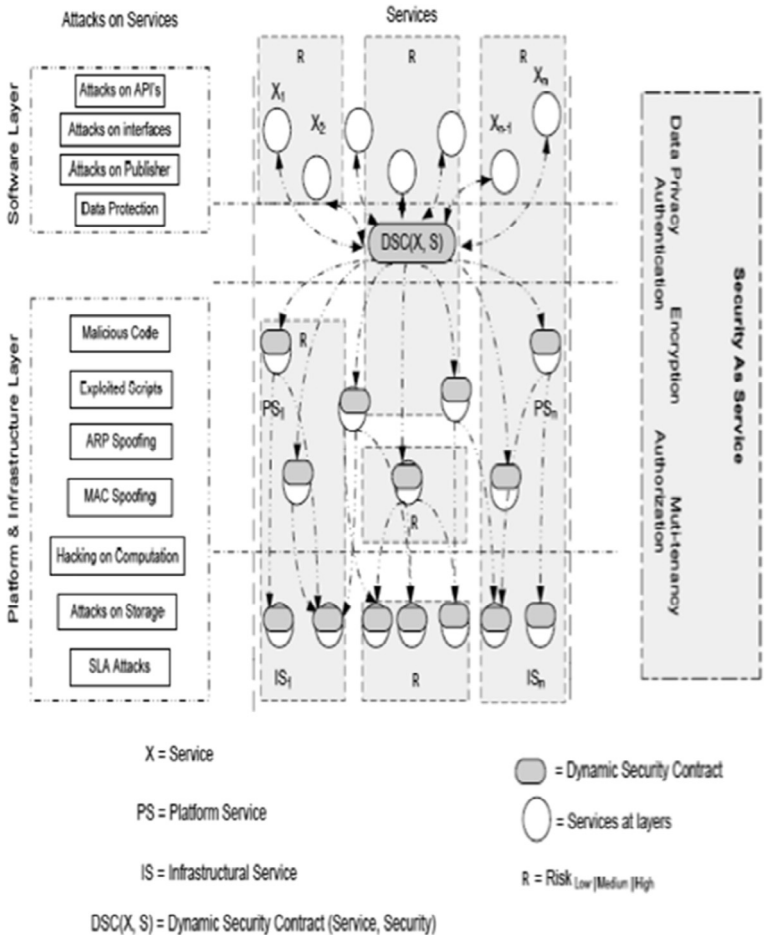

Figure 2 Dynamic security provision across layers of the cloud system.

Possible Subset for Hardware Virtualization

X = Hardware Virtualization, S_1 = Multi-tenancy, S_2 = Data Privacy, A_1 = ARP spoofing, R = High.
X = Hardware Virtualization, S_1 = Multi-tenancy, S_2 = Data Privacy, A_1 = MAC spoofing, R = High.
X = Hardware Virtualization, S_1 = Multi-tenancy, S_2 = Data Privacy, A_1 = ARP spoofing, A_2 = MAC spoofing, R = High.

4.1. Dynamic Security Contract (DSC) provisioning model

DSC is an approach for agreement between a consumer and a provider regarding cross layer security provisioning methods corresponding to the available services. Before establishing the security model, it is necessary to understand the different objectives and outcomes of DSC from consumer as well as provider perspective.

Fig. 3 shows the flow of our proposed Dynamic Security Contract (DSC) in which the consumer is offered a DSC after initial contact to the provider. The consumer can have three available options, accept the DSC as it is, negotiate the parameters as per his requirements or decline the DSC without giving any reason. The provider responds to either of the choices with its own viable set of corresponding options, i.e. Provision of security if accepted by consumer, alter the DSC keeping in view of its own parameters of cost and Return on investment (ROI) or decline any further contact. The consumer can now either accept or decline the new offer as there is only one available option for negotiation to simplify the model, and provider responds with provisioning security or declining the consumer choices. Consumer and provider have their own set of parameters to decide the viability of the contract and are discussed in further sections with the foremost discussion on measurement of security in a quantifiable manner.

4.1.1. Security measurement metrics

Each threat $t \in T$ is associated with a set of vulnerabilities and to represent attack we extend the notation of [22] to establish a Cloud Attack Graph (CAG). Each CAG is a tuple $CAG = (V, E)$ where $V = N_c \cup N_d \cup N_r$ and E is set of directed edges between any members of V. Each node $S_c \in N_c$ is defined as a tuple (Service, Vulnerability). Each node belonging to N_d is the outcome of exploiting vulnerability in the corresponding service. For each attack step node $S_c \in N_c$ the probability of vulnerability exploitation at any given time is denoted by $Pr[e]$, which can be assigned according to the Base Score (BS) calculated from CVSS [23]. The value of BS ranges from 0 to 10 and $Pr[e]$ can be derived as

$$Pr[e] = BS\left(\frac{S_c}{10}\right), \forall S_c \in N_c \tag{3}$$

In an attack graph the vulnerabilities are related to each other through their dependency conditions [24], and thus the probability of an exploit can be calculated according to its relation with its predecessor and their risk probabilities. Given a set of predecessor nodes ω as parents for node $S_c \in N_c$, the conditional risk probability can be given as

$$Pr(S_c|\omega) = Pr[e] \times \prod_{y \in \omega} Pr(y|\omega) \tag{4}$$

once the conditional probabilities are assigned, the cumulative risk probability for effective mitigation and remediation plan against each threat can be calculated as

$$Pr(S_c) = Pr(S_c|\omega) \times \prod_{y \in \omega} Pr(y) \tag{5}$$

4.1.2. DSC offering

The cumulative risk calculated in the previous section is used to effectively select the corresponding countermeasure from the set of mitigation plan pool. The mitigation plan is a set $MP = \{mp_1, mp_2, mp_3, \ldots, mp_n\}$ where each mp is a tuple $mp = (condition, effort, effectiveness, cost)$, where condition is the exploit that must hold a true value, effort is the struggle required to implement the mitigation plan, effectiveness is the probabilistic measure of guarantee in case of applying the specific plan and cost is the expense incurred in its implementation. The return on investment from provider perspective can be given by

$$ROI[t, mp] = \frac{benefit[t, mp]}{mp.cost + mp.effort} \tag{6}$$

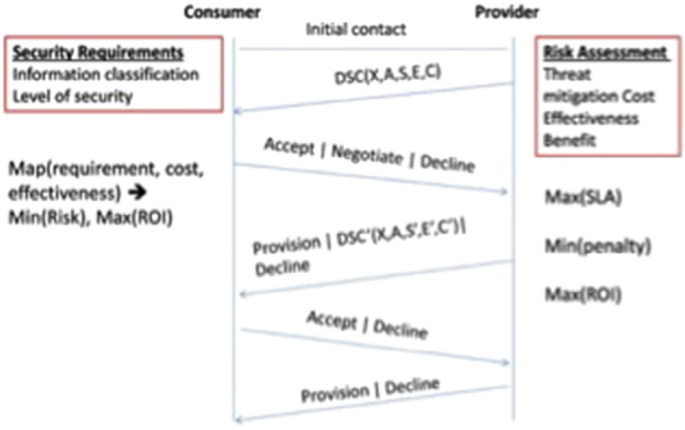

Figure 3 Dynamic security contract.

Table 3 DSC from consumer/provider perspective.

Consumer	Provider
Security of data as per information requirements (i.e. sensitivity) with minimum cost and maximum utilization – Demand sufficient security – Min (Risk) – Min (Cost) – Max (Utilization) – Max (ROI)	Provision of security at every layer of cloud – Risk assessment and countermeasure selection – Opt-able security choices – Meet dynamic SLAs – Avoid penalties – Max (ROI)

where benefit is the change in the probability of exploitation of the given node after applying a mitigation plan, given by

$$benefit[t, mp] = pr(e) = \Delta pr(e) \times (mp.effectiveness) \quad (7)$$

Possible choices for mitigation plan and their respective cost benefit analysis from the provider perspective are crucial in offering dynamic security contracts and their negotiations. The objective of /Volumes/Macintosh HD 2/Research/Multilevel security concerns cloud computing/LaTex/Multilevel security classification/Supplementary.texMAX (ROI), *MAX (SLA)* and *MIN (penalties)* for provider can be achieved once the maximum and minimum costs for countermeasure are known for each threat. Effectiveness and Cost are two parameters delivered to the consumer in the DSC. Optimal selection of mitigation plan and countermeasure selection is related to the information classification and definition of acceptable security at consumer end.

4.1.3. DSC selection

A consumer $c \in C$ opts to use at least one service $x \in X$ from the provider P at any layer of cloud with no limit on maximum number. Thus there exists a many-to-many relation between consumers and services. For simplicity, we will be considering each service independently in the context of a single consumer. Sufficient security is said to be achieved when the consumer data residing/ transiting cloud service is safe from threat or the risk has been accepted as inevitable by the consumer. We assume that the information is classified and the respective security level is translated into numeric values that scale from 0 to 10 with 0 as least restricted requiring no security and 10 as the most restricted information level requiring stringent security measures. Mapping of security requirements, effectiveness of countermeasure and cost leads to the decision of adopting, negotiating or declining a DSC. Given the information protection level, the return on investment (ROI) for adopting a DSC, for a service $x \in X$ with threat vector aA and offered security $s \in S$ with effectiveness e and cost c must be greater than or equal to 1 (see Table 3).

$$TOI[dsc, p] = \frac{p \times s.effectiveness}{s.cost} \quad (8)$$

$$DSC(x, a, s, e, c) = \begin{cases} accept, & ROI > 1 \\ negotiate, & ROI = 1 \\ decline, & ROI < 1 \end{cases}$$

5. Conclusion

A novel multilevel classification of security concerns in cloud computing highlighting the effect of different security attacks on each cloud layer is presented in this paper. This multilevel classification provides a new dimension to address security concerns on multiple levels and minimization of their effects. The level of severity of the attack is also assessed as low, medium and high across different security concerns. The security requirements for different cloud services are also outlined for the secure cloud computing. These security requirements include data encryption, multi-tenancy, data privacy, authentication and authorization. These security requirements are mapped to different cloud services to achieve integrity and coherence in the cloud system. The paper presents a novel concept of dynamic security contract to determine the risk level and type of security required for each service at different cloud layers for a cloud consumer and cloud provider.

Appendix A. Supplementary material

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.aci.2016.03.001.

References

[1] P. Mell, T. Grance, The NIST definition of cloud computing, in: National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, springer, 2011, pp. 1–7.
[2] R. Bhadauria, S. Sanyal, Survey on security issues in cloud computing and associated mitigation techniques, Int. J. Comput. Appl. 47 (18) (2012) 47–66.
[3] S.S. Yeo, J.H. Park, Security considerations in cloud computing virtualization environment, Grid Pervasive Comput. Lecture Notes Comput. Sci. 7861 (2013) 208–215.
[4] H. Yu, N. Powell, D. Stembridge, X. Yuan, Cloud computing and security challenges, in: Proc of the 50th Annual Southeast Regional Conference (ACM-SE12), ACM, New York, USA, 2013, pp. 298–302.
[5] H. Jay, M. Nicolett, Assessing the security risks of cloud computing http://www.studymode.com/essays/Assessing-The-Security-Risks-Of-Cloud-1009499.html2008.
[6] W. Jansen, T. Grance, et al, Guidelines on security and privacy in public cloud computing, NIST Special Publ. 800 (2011) 144.
[7] T. Mather, S. Kumaraswamy, S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, Inc., 2009.
[8] P. Arora, R.C. Wadhawan, E.S.P. Ahuja, Cloud computing security issues in infrastructure as a service, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 2 (1) (2012) 1–7.
[9] S. Bugiel, S. Nurnberger, T. Poppelmann, A.R. Sadeghi, T. Schneider, AmazonIA: when elasticity snaps back, in: Proc of the 18th ACM Conference on Computer and Communications Security (CCS11), ACM, 2011, pp. 389–400.
[10] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, L.L. Iacono, All your clouds are belong to us:

security analysis of cloud management interfaces, in: Proc. of the 3rd ACM workshop on Cloud Computing Security Workshop (CCSW11), ACM, 2011, pp. 3–14.
[11] M. Hussain, H. Abdulsalam, SECaaS: security as a service for cloud-based applications, in: Proc. of the Second Kuwait Conference on e-Services and e-Systems (KCESS11), ACM, 2011, pp. 1–4.
[12] R. Laborde, F. Barrère, A. Benzekri, Toward authorization as a service: a study of the XACML standard, in: Proceedings of the 16th Communications & Networking Symposium, Society for Computer Simulation International, 2013, pp. 1–7.
[13] G. Pek, L. Buttyan, B. Bencsath, A survey of security issues in hardware virtualization, ACM Comput. Surveys 45 (3) (2013) 1–34. ACM.
[14] M. Pearce, S. Zeadally, R. Hunt, Virtualization: issues, security threats, and solutions, ACM Comput. Surveys 45 (2) (2013) 1–39. ACM.
[15] L. Ponemon, Ponemon 2014 SSH security Vulnerability Report Retrieved from http://www.venafi.com/collateral/wp/ponemon-2014-ssh-security-vulnerability-report2014.
[16] Zeua, Zeus Botnet Controller Retrieved from http://aws.amazon.com/security/zeus-botnet-controller/2009.
[17] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Get off of my cloud: exploring information leakage in third-party compute clouds, in: ACM Conference on Computer and Communications Security, ACM, 2009.
[18] Zeua, Attacks on Virtual Machine Emulators, White Paper Symantec Corporation http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf2007.
[19] J. Idziorek, Exploiting Cloud Utility Models for Profit and Ruin Graduate Theses and Dissertations, Lowa State University, 2012.
[20] R.A. Popa, J.R. Lorch, D. Molnar, H.J. Wang, L. Zhuang, Enabling security in cloud storage SLAs with CloudProof, in: Proc. of the 2011 USENIX Conference on USENIX Annual Technical Conference, 2011, 31-31.
[21] J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning, Managing security of virtual machine images in a cloud environment, in: ACM Cloud Computing Security Workshop (CCSW?09), ACM, 2009.
[22] X. Ou, S. Govindavajhala, A.W. Appel, gMulVAL: a logic-based network security analyzer, in: Proc. 14th USENIX Security Symp., 2005, pp. 113–128.
[23] P. Mell, K. Scarfone, S. Romanosky, gCommon Vulnerability Scoring System (CVSS) http://www.first.org/cvss/cvss-guide.html2010, May.
[24] M. Frigault, L. Wang, gMeasuring network security using bayesian network-based attack graphs, in: Proc. IEEE 32nd Ann. Intfl Conf. Computer Software and Applications (COMPSAC f08), 2008, pp. 698–703. Aug.

Multilevel classification of security concerns in cloud computing

Hussain, Syed Asad; Fatima, Mehwish; Saeed, Atif; Raza, Imran; Shahzad, Raja Khurram

01 Dhananjaya Wimalasekera Page 2

17/2/2021 17:18

02 Dhananjaya Wimalasekera Page 2

17/2/2021 17:27

proposed model, security as a service

03 Dhananjaya Wimalasekera Page 2

17/2/2021 17:26

04 Dhananjaya Wimalasekera Page 2

17/2/2021 17:25

related work

05 Dhananjaya Wimalasekera Page 2

17/2/2021 17:24