IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONSAND TECHNOLOGY

Cloud Computing – Security issue analyses

Prof. Vinit A. Sinha
vinit.sinha84@gmail.com

Department of Master in Computer Application
Prof Ram Meghe Institute of Technology & Research , Badnera Amravati

Abstract

Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Cloud Computing leverages many technologies (SOA, virtualization, Web 2.0); it also inherits their security issues, which we discuss here, identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment as well as to identify and relate vulnerabilities and threats with possible solutions.

Keywords: *Cloud computing, Security, SPI model, Vulnerabilities, Threats, Countermeasures*

1. Introduction

The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and
industrial communities. A study by Gartner [1] considered Cloud Computing as the first among the top 10 most
important technologies and with a better prospect in successive years by companies and organizations. Cloud Computing enables 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. Cloud Computing appears as a computational paradigm as well as a distribution architecture and its main objective is to provide secure, quick, convenient data
storage and net computing service, with all computing resources visualized as services and delivered over the Internet [2,3]. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [4-7].Cloud Computing combines a number of computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while
their software and data are stored on the servers [5]. In some respects, Cloud Computing represents the maturing
of these technologies and is a marketing term to represent that maturity and the services they provide [6]. Although there are many benefits to adopting Cloud Computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security, followed by issues regarding compliance, privacy and legal matters [8]. Because Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing [9]. That uncertainty has

consistently led information executives to state that security is their number one concern with Cloud Computing [10]. Security concerns relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many specific features, such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form [11]. Security controls in Cloud Computing are, for the most part, no
different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, Cloud Computing may present different risks to an organization than traditional IT solutions. Unfortunately, integrating security into these solutions is
often perceived as making them more rigid [4]. Moving critical applications and sensitive data to public cloud environments is of great concern for those corporations that are moving beyond their data center's network under their control. To alleviate these concerns, a cloud solution provider must ensure that customers will continue to have the same security and privacy controls over their applications and services, provide evidence to customers that their organization are secure and they can meet their service-level agreements, and that they can prove compliance to auditors [12]. We present here a categorization of security issues for Cloud Computing focused in the so-called SPI model (SaaS, PaaS and IaaS), identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment. A threat is a potential attack that may lead to a misuse of information or resources, and the term vulnerability refers to the flaws in a system that Allows an attack to be successful. There are some surveys where they focus on one service model, or they focus on listing cloud security issues in general without distinguishing among vulnerabilities and threats. Here, we present a list of vulnerabilities and threats, and we also indicate what cloud service models can be affected by them. Furthermore, we describe the relationship between these vulnerabilities and threats; how these vulnerabilities can be xploited in order to perform an attack, and also present some countermeasures related to these threats which try to solve or improve the identified problems. The remainder of the paper is organized as follows: Section 2 presents the results obtained from our systematic review. Next, in Section 3 we define in depth the most important security Aspects for each layer of the Cloud model. Later, we will analyze the security issues in Cloud Computing Identifying the main vulnerabilities for clouds, the most important threats in clouds, and all available countermeasures for these threats and vulnerabilities. Finally, we provide some conclusions.

1.1 Systematic review of security issues for cloud computing

We have carried out a systematic review [13-15] of the existing literature regarding security in Cloud Computing, not only in order to summarize the existing vulnerabilities and threats concerning this topic but also to identify and analyze the current state and the most important security issues for Cloud Computing.

1.2 Question formalization

The question focus was to identify the most relevant issues in Cloud Computing which consider Vulnerabilities, threats, risks, requirements and solutions of security for Cloud Computing. This question had to be related with the aim of this work; that is to identify and relate vulnerabilities and threats with possible solutions. Therefore, the research question addressed by our research was the following: What security vulnerabilities and threats are the most important in Cloud Computing which have to be studied in depth with the purpose of handling them? The keywords and related concepts that make up this question and that were used during the review execution are: secure Cloud systems, Cloud security, delivery models security, SPI security, SaaS security, Paas security, IaaS security, Cloud threats, Cloud vulnerabilities, Cloud recommendations, best practices in Cloud.

1.3 Selection of sources

The selection criteria through which we evaluated study sources was based on the research experience of the authors of this work, and in order to select these sources we have considered certain constraints: studies included in the selected sources must be written in English and these sources must be web-available. The following list of sources has been considered: ScienceDirect, ACM digital library, IEEE digital library, Scholar Google and DBLP.
Later, the experts will refine the results and will include important works that had not been recovered in these sources and will update these work taking

into account other constraints such as impact factor, received cites,
important journals, renowned authors, etc. Once the sources had been defined, it was necessary to describe the process and the criteria for study selection and evaluation. The inclusion and exclusion criteria of this study were based on the research question. We therefore established that the studies must contain issues and topics which consider security on Cloud Computing, and that these studies must describe threats, vulnerabilities,
countermeasures, and risks.

1.4 Review execution

During this phase, the search in the defined sources must be executed and the obtained studies must be Evaluated according to the established criteria. After executing the search chain on the selected sources we obtained a set of about 120 results which were filtered with the inclusion criteria to give a set of about 40 relevant studies. This set of relevant studies was again filtered with the exclusion criteria to give a set of studies which corresponds with 15 primary proposals [4,6,10,16-27].

2. Results and discussion

The results of the systematic review are summarized in Table 1 which shows a summary of the topics and concepts considered for each approach. As it is shown in Table 1, most of the approaches discussed identify, classify, analyze, and list a number of vulnerabilities and threats focused on Cloud Computing. The studies analyze the risks and threats, often give recommendations on how they can be avoided or covered, resulting in a direct relationship between vulnerability or threats and possible solutions and mechanisms to solve them. In addition, we can see that in our search, many of the approaches, in addition to speaking about threats and vulnerabilities, also discuss other issues related to security in the Cloud such as the data security, trust, or security recommendations and mechanisms for any of the problems encountered in these environments.

2.1 Security in the SPI model

The cloud model provides three types of services [21,28,29]: _ Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).

_ Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services. _ Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to
deploy and run arbitrary software, which can include operating systems and applications. With SaaS, the burden of security lies with the cloud provider. In part, this is because of the degree of abstraction, the SaaS model is based on a high degree of integrated functionality with minimal customer control or extensibility. By contrast, the PaaS model offers greater extensibility and greater customer control. Largely because of the relatively lower degree of abstraction, IaaS offers greater tenant or customer control over security than do PaaS or SaaS [10]. Before analyzing security challenges in Cloud Computing, we need to understand the relationships anddependencies between these cloud service models [4]. PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and SaaS services, but also it may be true on the other way around. However, we have to take into account that PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between them. As a consequence of these deep dependencies,any attack to any cloud service layer can compromise the upper layers. Each cloud service model comprises its own inherent security flaws; however, they also share some challenges that affect all of them. These relationships and dependencies between cloud models may also be a source of security risks. A SaaS provider may rent a development environment from a PaaS provider, Which might also rent an infrastructure from an IaaS provider. Each provider is responsible for securing his own services, which may result in an inconsistent combination of security models. It also creates confusion over which
service provider is responsible once an attack happens.

2.2 Software-as-a-service (SaaS) security issues

SaaS provides application services on demand such as email, conferencing software, and business applications such as ERP, CRM, and SCM [30]. SaaS users have less control over security among the three fundamental

Table 1 Summary of the topics considered in each approach

Topics/References	[4]	[6]	[10]	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]
Vulnerabilities		X		X	X	X	X	X	X			X			X
Threats		X		X	X	X	X	X	X	X	X	X	X	X	X
Mechanisms/Recommendations	X			X		X		X				X	X	X	X
Security Standards							X			X					
Data Security	X		X				X		X		X		X		X
Trust			X								X		X	X	X
Security Requirements	X		X						X		X			X	X
SaaS, PaaS, IaaS Security					X				X			X			

delivery models in the cloud. The adoption of SaaS applications may raise some security concerns.

2.3 Application security

These applications are typically delivered via the Internet through a Web browser [12,22]. However, flaws in web
applications may create vulnerabilities for the SaaS applications. Attackers have been using the web to compromise
user's computers and perform malicious activities such as steal sensitive data [31]. Security challenges in SaaS
applications are not different from any web application technology, but traditional security solutions do not effectively protect it from attacks, so new approaches are necessary [21]. The Open Web Application Security
Project (OWASP) has identified the ten most critical web applications security threats [32]. There are more
security issues, but it is a good start for securing web applications.

2.4 Multi-tenancy

SaaS applications can be grouped into maturity models that are determined by the following characteristics: scalability, configurability via metadata, and multi-tenancy [30,33]. In the first maturity model, each customer has his own customized instance of the software. This model has drawbacks, but security issues are not so bad compared
with the other models. In the second model, the vendor also provides different instances of the applications for each customer, but all instances use the same application code. In this model, customers can change some configuration
options to meet their needs. In the third maturity model multi-tenancy is added, so a single instance serves all customers [34]. This approach enables more efficient use of the resources but scalability is limited. Since data from multiple tenants is likely to be stored in the same database, the risk of data leakage between these tenants is high. Security policies are needed to ensure that customer's data are kept separate from other customers [35]. For the final model, applications can be scaled up by moving the application to a more powerful server if needed.

2.5 Data security

Data security is a common concern for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security [12,21,36]. In SaaS, organizational data is often processed in plaintext and stored in the cloud. The SaaS provider is the one responsible for the security of the data while is being processed and stored [30]. Also, data backup is a critical aspect in order to facilitate recovery in case of disaster, but it introduces security concerns as well [21]. Also cloud providers can subcontract other services such as backup from third-party service providers, which may raise concerns. Moreover, most compliance standards do not envision compliance with regulations in a world of Cloud Computing [12]. In the world of SaaS, the process of compliance is complex because data is located in the provider's datacenters, which may introduce regulatory compliance issues such as data privacy, segregation, and security, that must be enforced by the provider.

2.6 Accessibility

Accessing applications over the internet via web browser makes access from any network device easier, including public computers and mobile devices. However, it also exposes the service to additional security risks. The Cloud

Security Alliance [37] has released a document that describes the current state of mobile computing and the top threats in this area such as information stealing mobile malware, insecure networks (WiFi), vulnerabilities found
in the device OS and official applications, insecure marketplaces, and proximity-based hacking.

2.7 Platform-as-a-service (PaaS) security issues

PaaS facilitates deployment of cloud-based applications without the cost of buying and maintaining the underlying
hardware and software layers [21]. As with SaaS and IaaS, PaaS depends on a secure and reliable network and secure web browser. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform [10]. PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications. Same as SaaS, PaaS also brings data security issues and other challenges that are described as follows:

2.7.1 Third-party relationships

Moreover, PaaS does not only provide traditional programming languages, but also does it offer third-party web services components such as mashups [10,38]. Mashups combine more than one source element into a single integrated unit. Thus, PaaS models also inherit security issues related to mashups such as data and network
security [39]. Also, PaaS users have to depend on both the security of web-hosted development tools and third-party services.

2.7.2 Development Life Cycle

From the perspective of the application development, developers face the complexity of building secure applications
that may be hosted in the cloud. The speed at which applications will change in the cloud will affect both the System Development Life Cycle (SDLC) and security [12,24]. Developers have to keep in mind that PaaS applications should be upgraded frequently, so they have to ensure that their application development

Table 2 Vulnerabilities in cloud computing

ID	Vulnerabilities	Description	Layer
V01	Insecure interfaces and APIs	Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON) [42]. The security of the cloud depends upon the security of these interfaces [16]. Some problems are:	SPI
		a) Weak credential	
		b) Insufficient authorization checks	
		c) Insufficient input-data validation	
		Also, cloud APIs are still immature which means that are frequently updated. A fixed bug can introduce another security hole in the application [54].	
V02	Unlimited allocation of resources	Inaccurate modeling of resource usage can lead to overbooking or over-provisioning [17].	SPI
V03	Data-related vulnerabilities	a) Data can be colocated with the data of unknown owners (competitors, or intruders) with a weak separation [36]	SPI
		b) Data may be located in different jurisdictions which have different laws [19,54,55]	
		c) Incomplete data deletion – data cannot be completely removed [19,20,25,56]	
		d) Data backup done by untrusted third-party providers [56,57]	
		e) Information about the location of the data usually is unavailable or not disclosed to users [25]	
		f) Data is often stored, processed, and transferred in clear plain text	
V04	Vulnerabilities in Virtual Machines	a) Possible covert channels in the colocation of VMs [48,58,59]	I
		b) Unrestricted allocation and deallocation of resources with VMs [57]	
		c) Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance [42,44]	
		d) Uncontrolled snapshots – VMs can be copied in order to provide flexibility [12], which may lead to data leakage	
		e) Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration [44], but patches applied after the previous state disappear	
		f) VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud (Cloud cartography [58])	
V05	Vulnerabilities in Virtual Machine Images	a) Uncontrolled placement of VM images in public repositories [24]	I
		b) VM images are not able to be patched since they are dormant artifacts [44]	
V06	Vulnerabilities in Hypervisors	a) Complex hypervisor code [60]	I
		b) Flexible configuration of VMs or hypervisors to meet organization needs can be exploited	
V07	Vulnerabilities in Virtual Networks	Sharing of virtual bridges by several virtual machines [51]	I

Table 3 Threats in cloud computing

ID	Threats	Description	Layer
T01	Account or service hijacking	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction [16].	SPI
T02	Data scavenging	Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data [10,17,25].	SPI
T03	Data leakage	Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed [16,17,20,58].	SPI
T04	Denial of Service	It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.	SPI
T05	Customer-data manipulation	Users attack web applications by manipulating data sent from their application component to the server's application [20,32]. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.	S
T06	VM escape	It is designed to exploit the hypervisor in order to take control of the underlying infrastructure [24,61].	I
T07	VM hopping	It happens when a VM is able to gain access to another VM (i.e. by exploting some hypervisor vulnerability) [17,43]	I
T08	Malicious VM creation	An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository [20].	I
T09	Insecure VM migration	Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions: a) Access data illegally during migration [42] b) Transfer a VM to an untrusted host [44] c) Create and migrate several VM causing disruptions or DoS	I
T10	Sniffing/Spoofing virtual networks	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs [45,51].	I

Furthermore, web services are the largest implementation technology in cloud environments. However, web services
also lead to several challenges that need to be addressed. Security web services standards describe how to secure communication between applications through integrity, confidentiality, authentication and authorization. There are several security standard specifications [79] such as Security Assertion Markup Language (SAML), WSSecurity,
Extensible Access Control Markup (XACML), XML Digital Signature, XML Encryption, Key Management Specification (XKMS), WS-Federation, WS-Secure Conversation, WS-Security Policy and WS-Trust. The NIST Cloud Computing Standards Roadmap Working Group has gathered high level standards that are relevant for Cloud
Computing.

3 Conclusions

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines. Some surveys have discussed security issues about clouds without making any difference between vulnerabilities and threats. We have focused on this distinction, where we consider important to understand these issues. Enumerating these security issues was not enough; that is why we made a relationship between threats and vulnerabilities, so we can identify what vulnerabilities contribute to the execution of these threats and make the system more robust. Also, some current solutions were listed in order to mitigate these threats. However, new security techniques are needed as well as redesigned

traditional solutions that can work with cloud architectures.

Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies. We have expressed three of the items in Table 4 as misuse patterns [46]. We intend to complete all the others in the future.

References

1. Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15-Jul-2011
2. Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp 347–358
3. Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. IEEE Computer Society, Washington, DC, USA, pp 93–97
4. Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: Https://cloudsecurityalliance.org/ guidance/csaguide.v3.0.pdf
5. Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Springer-Verlag Berlin, Heidelberg
6. Centre for the Protection of National Infrastructure (2010) Information Security Briefing 01/2010 Cloud Computing. Available: http://www.cpni.gov. uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf
7. Khalid A (2010) Cloud Computing: applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP'10), pp 278–281
8. KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey.. Available: http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs- 2010-cloud-computing-survey/2384291
9. Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469–487
10. Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA
11. Li W, Ping L (2009) Trust model to enhance Security and interoperability of Cloud environment. In: Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg, Beijing, China, pp 69–79
12. Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press
13. Kitchenham B (2004) Procedures for perfoming systematic review, software engineering group. Department of Computer Scinece Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd, Australia. TR/SE-0401
14. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering. Version 2.3 University of keele (software engineering group, school of computer science and mathematics) and Durham. Department of Conputer Science, UK
15. Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M (2007) Lessons from applying the systematic literature review process within the software engineering domain. J Syst Softw 80(4):571–583
16. Cloud Se curity Alliance (2010) Top Threats to Cloud Computing V1.0.Available: https://cloudsecurityalliance.org/research/top-threats
17. ENISA (2009) Cloud Computing: benefits, risks and recommendations for information Security. Available: http://www.enisa.europa.eu/activities/riskmanagement/ files/deliverables/cloud-computing-risk-assessment
18. Dahbur K, Mohammad B, Tarakji AB (2011) A survey of risks, threats and vulnerabilities in Cloud Computing. In: Proceedings of the 2011 International conference on intelligent semantic Web-services and applications. Amman, Jordan, pp 1–6
19. Ertaul L, Singhal S, Gökay S (2010) Security challenges in Cloud Computing. In: Proceedings of the 2010 International conference on Security and Management SAM'10. CSREA Press, Las Vegas, US, pp 36–42
20. Grobauer B, Walloschek T, Stocker E (2011) Understanding Cloud Computing vulnerabilities. IEEE Security Privacy 9(2):50–57
21. Subashini S, Kavitha V (2011) A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1–11
22. Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) On technical Security issues in Cloud Computing. In: IEEE International conference on Cloud Computing (CLOUD'09). 116, 116, pp 109–116
23. Onwubiko C (2010) Security issues to Cloud Computing. In: Antonopoulos N, Gillam L (ed) Cloud Computing: principles, systems & applications. 2010, Springer-Verlag

24. Morsy MA, Grundy J, Müller I (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia
25. Jansen WA (2011) Cloud Hooks: Security and Privacy Issues in Cloud Computing. In: Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, Kauai, HI. IEEE Computer Society, Washington, DC,
USA, pp 1–10
26. Zissis D, Lekkas D (2012) Addressing Cloud Computing Security issues. Futur Gener Comput Syst 28(3):583–592
27. Jansen W, Grance T (2011) Guidelines on Security and privacy in public Cloud Computing. NIST, Special Publication 800–144, Gaithersburg, MD
28. Mell P, Grance T (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800–145, Gaithersburg, MD
29. Zhang Q, Cheng L, Boutaba R (2010) Cloud Computing: state-of-the-art andresearch challenges. Journal of Internet Services Applications 1(1):7–18
30. Ju J, Wang Y, Fu J, Wu J, Lin Z (2010) Research on Key Technology in SaaS .In: International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. IEEE Computer Society, Washington, DC, USA, pp 384–387
31. Owens D (2010) Securing elasticity in the Cloud. Commun ACM 53(6):46–51