Int. j. inf. tecnol. (2019) 11:683–690
https://doi.org/10.1007/s41870-018-0108-1

ORIGINAL RESEARCH

Security concerns and countermeasures in cloud computing: a qualitative analysis

Anjana[1] · **Ajit Singh**[1]

Received: 23 June 2017 / Accepted: 8 February 2018 / Published online: 28 February 2018

Abstract Nowadays, cloud computing is considered as most cost-effective platform which provides business and consumer services in IT over the Internet. But security is recognized as the main stammer block for wider adoption due to outsourcing of services from third party. Keeping in view the same, security issues in three service models of cloud computing namely SaaS, PaaS, and IaaS have been discussed. The present paper provides a qualitative analysis of all vulnerabilities and related threats corresponding to each service model. In last section countermeasures have been proposed to enhance the security in Cloud computing.

Keywords Cloud computing · Security · Threats · Vulnerabilities · SaaS · PaaS · IaaS · Virtual machine · Countermeasures

1 Introduction

Security is a major requirement for cloud computing as a reliable and feasible multi-purpose solution. Many academia researchers, business decision makers, government organization and IT firms have indicated a severe concern on crucial security and legal obstacles for cloud computing, that cover service availability, data confidentiality, service providers and reputation fate sharing. These concerns are not only derived from existing problems but also related to new compositions of need of cloud computing features like scalability, resource sharing and virtualization. These can be differentiated on the basis of model of services like Saas, PaaS, and IaaS and deployment method like private, public, community and hybrid [1].

ENISA (European Network and Information Security Agency) has enlists all risks and vulnerabilities along with related work and research recommendations [2]. Also, CSA (Cloud Security Alliance) has provided the security guidance which defines security domains functional aspects, from governance and compliance to virtualization and identity management [3]. Both documents present a plenty of security concerns, best practices and recommendations regarding all types of services and possible problems in cloud computing.

A threat is a possible attack on confidential information or critical resources for intended misuse, and vulnerability may be defined as a weakness which allows attacker to reduce a system's security assurance. There is difference between vulnerability and threats but various articles have used them interchangeably [4].

Security-related concerns in cloud computing are different from traditional IT solutions, as Cloud computing is itself a combination of existing techniques such as SOA (Service Oriented Architecture), Web 2.0, virtualization, grid computing and other technologies with dependency on the Internet, facilitating common business applications. Traditional security mechanism like identity, authentication and authorization are no more sufficient for cloud computing.

As compare to traditional technologies, cloud computing has various distinct features such as its scalability at large level, resource distribution at large scale which are totally heterogeneous and virtualized.

✉ Anjana
saroha.anjana@gmail.com

✉ Ajit Singh
ghanghas_ajit@rediffmail.com

[1] Department of CSE & IT, Bhagat Phool Singh Mahila Vishwavidyalaya, Khanpur Kalan, Sonipat, Haryana, India

Going forward towards public cloud environment having critical data and applications for various corporations is on a big risk which are losing control of their data centres. Customers should be ensured that they will keep same security and privacy level for their applications and services along with evidences which meet their service-level agreements with compliance to auditors by a cloud solution provider [5].

The main aim of this article is to identify, classify, organize and quantify the main security concerns and solutions related to cloud computing. This article provides an extended review of cloud computing security taxonomy and a deeper analysis of the security frameworks currently available.

In the Sect. 2, on the basis of service models, all related threats have been identified. Then in next Sect. 3, study of vulnerabilities and threats have been categorized into tabular form. Section 4 contains the countermeasures related to corresponding threats with proposed solutions.

2 Cloud service models and their security issues

Existing literature have been reviewed to analyse and categorize the existing vulnerabilities and threats which makes an outline to study current security issues in a systematic way [6–8].

Security in SPI models: Cloud service model decides the responsibilities of CSP (Cloud Service Provider) and CSC (Cloud Service Consumer) which have been categorized as follows:

2.1 PaaS (platform as a service)

In PaaS, deployment of consumer's application can be done on cloud environment without any platform or tool's installation on their local machines. Operating system support, platform layer resources and software development framework are provided in PaaS which can be used to develop high-level services.

PaaS security issues: In PaaS, there is not any cost of purchasing and maintenance of software and hardware layers [9]. There are two software layers where security is required: one is runtime engine (i.e. PaaS platform itself), and second consumer's application deployed on it [10]. Following challenges are being faced in PaaS, discussed as below.

2.1.1 Third-party relationships

PaaS provides traditional programming language as well as third-party web services components. For example, mashups which is a single integrated unit formed when one or more source elements are combined, this is called mashups. Integrated unit also inherits security issues such as data and network security from their sources [11]. So third-party services and tools available for developments both play an important role in security of PaaS model.

2.1.2 Development of life cycle

Development of the application which may be hosted in the cloud is more complex than a normal application development. The frequency of changes done during development will reduce security as well as speed of the development process [5, 12]. Security of the applications along with their data is dependent on the changes done in PaaS module because data may be stored at various places with different legal regimes which cannot be easily traced.

2.1.3 Underlying infrastructure security

In PaaS, it is the provider's responsibility for maintaining the security of underlying components and services because developers cannot access underlying layers [13].

2.2 SaaS (software as a service)

The consumer can use the third party provider's host applications available on a cloud environment which can be accessed using different client devices via an interface like web browser.

SaaS security issues: Applications like email, software and packages like ERP, CRM and SCM are provided on demand by consumer in SaaS service model [14]. Users have less control over security in SaaS service model. SaaS applications have following security concerns.

2.2.1 Application security

SaaS applications are vulnerable in nature because the source via which they are delivered to consumer is Internet (using a Web browser). Internet is the main source for intruders to perform malicious activities and break the security e.g. steal the sensitive data. We need new approaches and new security solutions for cloud applications because security concerns are different from the traditional web applications.

2.2.2 Multi-tenancy

Multi-tenancy is another feature unique to clouds, especially in public clouds. Essentially, it allows cloud providers to manage resource utilization more efficiently by portioning a virtualized, shared infrastructure among various customers. From a customer's perspective, the notion

of using a shared infrastructure could be a huge concern. However, the level of resource sharing and available protection mechanisms can make a big difference. For example, to isolate multiple tenant's data, Salesforce.com employs a query rewriter at the database level, whereas Amazon uses hypervisors at the hardware level. Providers must account for issues such as access policies, application deployment, and data access and protection to provide a secure, multi-tenant environment [15].

2.2.3 Data security

Data security is major concern for any technology. In SaaS, it is a vital challenge because being processing and storage of data black box to consumers, only provider can manage security of the data stored [16]. Another critical task is to take data backup and provide it to consumer in case of any disaster, but again more security concerns are introduced with it [9]. The provider should also take care of regulatory compliance issues like data security, segregation and its privacy because complete data is stored in provider's data centre only.

2.2.4 Accessibility

In modern era of internet, accessing of applications via web browser makes so easy that it exposes the service to additional security risks. Top threats in this area are stealing information, insecure networks, insecure marketplaces and proximity-based hacking.

2.3 IaaS (infrastructure as a service)

The consumer can deploy and run various software including operating system and applications with help of provisioning of various infrastructure like networks, storage, processing and other basic computing resources. IaaS has following security issues given below.

2.3.1 Virtualization

Virtualization is an important enabling technology that helps abstract infrastructure and resources to be made available to clients as isolated Virtual Machines [17] but this technology increases the vulnerabilities and may cause threats.

2.3.2 Virtual machine monitor or hypervisor

Virtual machine monitor should not be compromised because it is responsible for virtual machine isolation [4]. Thus if VMM is not secure then virtual machines are also not secure.

2.3.3 Shared resources

Sharing of resources like input/output, memory and CPU among VMs can reduce security of each VM.

2.3.4 Public VM image repository

All the configuration files which are used to create VMs are saved as a pre-packaged template called VM Image which are globally accessed on cloud. Either VM image can be made from scratch or it can be used already available on cloud. So malicious users can store the malicious image having malicious code. Also, if some confidential information is stored with image then it can be exposed and may be available to intruders.

2.3.5 Virtual machine rollback

VMs can be roll backed to their previous states if required but it can re-expose them to security threats by enabling previous accounts and password.

2.3.6 Virtual machine life cycle

VMs can be in different states like On, Off and Suspended. It is very important that VMs and their states changes should be understood when they move throughout the environment. VMs can be vulnerable if it is in Offline state.

2.3.7 Virtual networks

Resource pooling is main feature which allows attackers cross-tenant attacks. Virtual network enhance the VMs interconnectivity but introduces a major security challenge as well. To avoid this, each VM should be hooked with its host by giving dedicated physical channels. Also, the probability of attacks like spoofing and sniffing is increased due to the ways of configuration of virtual networks.

3 Categorization of threats in cloud computing

In this section, all existing vulnerabilities and threats have been presented along with their countermeasures in a systematic way. In Table 1, each vulnerability has been represented with brief description of it and related cloud service model affected by them.

Going forward to Table 2 which represents corresponding countermeasures related to possible threats in cloud computing.

Following Table 2 represents an overview of threats in Cloud Computing including few defined by the Cloud Security Alliance [12, 18]. It also describes the

Table 1 Vulnerabilities in cloud computing (Source: [4])

ID	Vulnerabilities	Description
1	Less secure interfaces and APIs	APIs are the main medium to access cloud service so weak APIs can be vulnerable to attacker. Following are the concerns:
		a. Not too strong credentials Like credentials are not mixture of Alphanumeric, special character and related to any hint or clue which can be easily guessed
		b. Lack of checking of authorization
		c. No proper data validation
2	An indefinite number of allocation of resources	Server will not be able to recognize reliable and authorized resources when there is unlimited allocation of resources and network will be vulnerable to attacker
3	Data-related vulnerabilities	a. Competitors and Intruders can modify the data with minor changes and misuse it
		b. Different locations have different jurisdictions laws
		c. Data available on Internet can never be completely removed
		d. No Trust management for data backup providers
		e. No responsibility and authority taken for any data available, even location cannot be traced
		f. No encryption and decryption techniques used during data processing, transfer and its storage
4	VMs vulnerabilities	a. Virtual machine may introduce covert channels
		b. No restriction on allocation and de-allocation of resources
		c. No control on migration of VMs
		d. No control on imaging and copying of one VM to another
		e. In case of rollback, no control on the patches applied before restoration
		f. Cloud cartography where attacker knows direct IP address of VMs
5	Vulnerabilities in hypervisors	Hypervisor configuration and VMs are easy to break and can be attacked easily
6	Vulnerabilities in virtual networks	Several virtual machines share virtual bridges which are vulnerable in nature

countermeasures related to each threat corresponding to each cloud service models based on the related technology used in cloud environments.

In the above table, each threat has been provided with countermeasure which are explained in next section.

4 Countermeasures

In this section, countermeasures have been discussed related to each threat mentioned in above table.

4.1 Account or service hijacking (T01)

An account hijacking can be done by different methods such as weak credentials and other social engineering. If any attacker gains the access to any user's credentials, then he can access any sensitive data, modify it and deviate any transaction. Following are the ways defined as countermeasure for threat T01:

4.1.1 Identity and Access Management (IAM) guidance

IAM is used to manage access to group of people, resources, systems and processes by assuring that a particular identity is verified and on the basis of requirement, a level of access is granted to each identity. Cloud Security Alliance (CSA) has provided Guidance [19] which not only provides a list of recommended best practices to assure security but also includes different services related to user's role, their access and control and Identity Management services.

4.1.2 Dynamic/random credentials

It is an algorithm which creates dynamic login details for mobile cloud computing systems. Credentials are dynamically changed once either user switch from one location to other or number of data packets exchanged has reached a limit [16].

4.2 Data loss or leakage (T02)

Data security includes three features: confidentiality, Integrity and availability. Researchers have started to devise the solutions for ensuring data integrity and confidentiality.

Following are the methods defined as countermeasure for threat T02:

Table 2 Threats in cloud computing (Source: [4, 17, 29])

ID	Threats	Incident	Countermeasures
T01	Hijacking of service or account	When an attacker gains access to a user's credential by any mean like social engineering or weak credentials, then he can use the access for performing malicious activities such as exposing confidential information, modification of data and wrong update in any transaction	Identity and Access Management Guidance Dynamic credential
T02	Data scavenging	When any device is destroyed having crucial data but attacker restore the data from it, so data is not removed permanently which is called data scavenging	Service-level agreements (SLAs) should be updated with destruction strategies
T03	Data leakage	Any activity related to data like processing, transfer and storage can cause leakage of data to attacker or intruders	FRS techniques Digital Signatures Encryption Homomorphic encryption
T04	Denial of service	Malicious user intentionally flood the resources requests to the server so that it cannot identify the genuine request from authorized user and cannot process the request due to unavailability of resources	Only limited computational resources should be offered
T05	Customer-data manipulation	The major techniques to access and modify the data available on cloud servers like SQL injection	Web application scanners
T06	VM escape	To take unauthorized control on underlying infrastructure on cloud environment	HyperSafe TCCP (Trusted Cloud Computing Platform) TVDc (Trusted Virtual Datacenter)
T07	VM image creation	A malicious VM image which may contain malicious code, can be created using a valid account	Mirage
T08	Insecure VM migration	Live migration of virtual machines can cause following possible attacks: a. Illegal access of data b. Transfer a VM to an untrusted host c. DoS	PALM TCCP (Trusted Cloud Computing Platforms VNSS
T09	Sniffing/spoofing virtual networks	To redirect packets from one VM to another by accessing virtual networks	Virtual network framework based on Xen
T10	Abuse and nefarious use of cloud computing	Malicious code authors, spammers and other criminals can abuse the relative anonymity behind some of current cloud services.	Customer CSC's network traffic introspection VM monitoring,
T11	Malicious insiders	The threat of malicious insider is amplified for cloud services due to the convergence of Information Technology (IT) services and customers under a single management domain.	Supply chain audit including human resource hiring procedure, Security certification, Audits, use of trusted Cloud computing platform (TCCP)
T12	Shared technology issues	CSPs deliver services in a scalable way. Some underlying component parts of the cloud infrastructure were not originally designed for that environment, and can potentially cause security problems. The main concern is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud.	VM monitoring and cloud audit, Access control, SLA enforcement for patching and vulnerability remediation
T13	Unknown security profile	The reduction of cost of ownership induced by the cloud also resulted in more complex analysis of a company's security posture. More tenants imply increased complexity in detecting who is using the infrastructure and how this is done.	Security certification, Audits, SLA monitoring

4.2.1 Fragmentation-redundancy-scattering (FRS)

Sensitive data is divided into many fragmentation which do not have any relevant information individually and then scattered to different servers of distributed systems so, this technique provides intrusion tolerance and a secure storage [20].

4.2.2 Digital signatures

Data is secured using RSA algorithm while sending on network. It is most efficient algorithm used to secure data in cloud computing [21].

4.2.3 Homomorphic encryption

Encryption techniques are used in cloud data transfer but during decryption process, it raises security and privacy concerns. So a new technique proposed named Homomorphic encryption, in which arbitrary computations are performed on cipher text such addition or multiplications without decryption [22]. But due to huge processing requirement it may lead to overheads like more response time and more power consumption [38].

4.2.4 Encryption

Encryption is the technique used since long time for securing the data [23]. Encrypted data on cloud is meant to be secure. There are many encryption algorithms which can be used to reduce side-channel attacks e.g. DES and AES but these techniques have their own limitations like exposing private keys.

4.3 Customer data manipulation (T03)

User attacks website data by sending its manipulative data from their component to the server component. So to avoid such attacks we can use various Web application firewalls, web applications scanners etc. [24]. Web application firewall inspects specific threats in all web traffic going through it. Web scanners are web programs which are used to scan web applications to identify security vulnerabilities.

4.4 VM escape (T04)

It exploits the hypervisor so to take control of the underlying infrastructure. Following are the ways for countermeasure for Threat T06:

4.4.1 HyperSafe

To protect hypervisor control flow integrity, HyperSafe is used [25]. It uses two techniques: (a) non-bypassable memory lockdown to protect write-protected memory pages from being edited and (b) prevents conversion of control data into pointer indexes. Following attacks have been conducted (i) modification of hypervisor code (ii) execution of injected code to check effectiveness of this approach.

4.4.2 Trusted cloud computing platform (TCCP)

TCCP [26] allow users to check before launching their virtual machines if the environment is secure enough. TCCP has two fundamental components: a) a trusted virtual machine monitor (TVMM) (b) a trusted coordinator (TC).TVMM is run by set of trusted nodes and these nodes are coordinated by TC. TC is maintained by trusted third party.TC either launch or migrates a VM, and also verifies that VM is running on a trusted platform. This whole process cause overload because each transaction is verified by TC [27]. Direct Anonymous Attestation (DAA) and Privacy CA scheme have been proposed to handle this concern.

Another initiative that uses the concept of trusted platform is Private Virtual Infrastructure (PVI) proposed by Krauthin [28]. This has suggested a mean to allow monitoring in the cloud by combining the trusted platform module (TPM) and a locator bot that pre-measures the cloud for security properties, securely provisions the data center in the cloud and provides situational awareness through continuous monitoring of the cloud security [29]. In this approach, security appears as a shared responsibility between the provider and the consumer.

4.4.3 Trusted virtual datacenter

Trusted Virtual Domain (TVDc) enables isolation between workloads by grouping virtual machines having common objectives. It enforces MAC, Virtual LANs and Hypervisor to provide isolation. It also facilitates integrity by employing load-time attestation mechanism [30, 31].

4.5 Malicious virtual machine image creation (T05)

In [32], a virtual machine image management system is proposed which includes security features like image filtering, maintenance services, keeping tracking information and managing access control. But these filters may have their own concerns like content of the image may contain customer's confidential data so cannot scan and remove it completely.

4.6 Insecure virtual machine migration (T06)

Following are the ways for countermeasure for threat T06:

4.6.1 Protection aegis for live migration of VMs (PALM)

To preserve integrity and privacy of data, a live migration has been proposed [33]. But the results of pilot phase of the implementation shown that it took long time and created overhead due to encryption and decryption.

4.6.2 Virtual network security system (VNSS)

For each virtual machine, security policies are modified to provide continuous protection using VM live migration [34]. The prototype was based on firewall technology and authors revealed that the security policies are in place throughout the live migration.

4.7 Sniffing/spoofing (T07)

To make a secure communication between two VMs, Wu and et al. [35] proposed a virtual network security framework. It is composed of three layers: shared networks, firewalls and routing layers to prevent VMs from sniffing and spoofing.

4.8 Abuse and nefarious use of cloud computing (T08)

By using VM monitoring and Customer's CSC's network traffic introspection can be used to avoid nefarious use of cloud computing [29].

4.9 Malicious insiders (T09)

Security Certification, Audits, Use of TCCP and Supply chain audit including human resources can reduce the malicious insider's threat [29].

4.10 Shared technology issues (T10)

SLA enforcement for patching and vulnerabilities remediation, VM Monitoring and cloud audits can be helpful for shared technology issues [29].

4.11 Unknown security profile (T11)

Security certification, SLA monitoring and Audits can be helpful for such issues [29].

5 Conclusion

Cloud computing paradigm is gaining momentum but along with that security is a crucial aspect for providing a reliable environment. A systematic organization of vulnerabilities and related threats will make a better understanding for researchers to devise the possible solutions. Since Cloud computing has inherited many other technologies so possible threats are also inherited from their origin. We have represented security threats on the basis of service models in Cloud computing such as: SaaS, IaaS, and PaaS. Also, a categorization have been represented in the terms of vulnerabilities, respective threats and their possible countermeasure on the basis of various literature available regarding the security challenges and their solutions in cloud computing. Though major solutions are proposed and not in actual implementations so new techniques like Virtualization in Cloud Infrastructure, Cloud Identity Management [36] to enhance security, Cloud Security using Cryptofunctions can be designed for more robust cloud systems.

References

1. Gonzalez et al (2012) A quantitative analysis of current security concerns and solutions for cloud computing. J Cloud Comput Adv Syst Appl 1:11
2. Catteddu D, Hogben G (2009) Benefits, risks and recommendations for information security. Tech. rep., European Network and Information Security Agency, enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment
3. CSA (2009) Security guidance for critical areas of focus in cloud computing. Tech. rep., Cloud Security Alliance
4. Hashizume et al (2013) An analysis of security issues for cloud computing. J Int Serv Appl 4:5
5. Rittinghouse JW, Ransome JF (2009) Security in the cloud. In: Cloud computing. implementation, management, and security. CRC Press
6. Kitchenham B (2004) Procedures for performing systematic review, software engineering group. Department of Computer Science Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd, Australia. TR/SE-0401
7. 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 Computer Science, UK
8. 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
9. 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
10. Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media Inc, Sebastopol
11. Xu K, Zhang X, Song M, Song J (2009) Mobile mashup: architecture, challenges and suggestions. In: International conference on management and service science. MASS'09. IEEE Computer Society, Washington
12. Morsy MA, Grundy J, Müller I (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 cloud workshop. APSEC, Sydney
13. Chandramouli R, Mell P (2010) State of security readiness. Crossroads 16(3):23–25
14. 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
15. Takabi H, Joshi J.B.D, Ahn G.-J (2010), "Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing

Environments," Proc. 1st IEEE Int'l workshop emerging applications for cloud computing (CloudApp 2010). IEEE CS Press
16. Wylie J, Bakkaloglu M, Pandurangan V, Bigrigg M, Oguz S, Tew K, Williams C, Ganger G, Khosla P (2001) Selecting the right data distribution scheme for a survivable Storage system. CMU-CS-01-120, Pittsburgh
17. Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," http://www.cloudsecurityalliance.org/csaguide.pdf
18. Cloud Security Alliance (2010) Top Threats to Cloud Computing. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. Accessed 21 Mar 2014
19. Cloud Security Alliance (2012) SecaaS implementation guidance, category 1: identity and access management. https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf. Accessed 8 Oct 2012
20. Somani U, Lakhani K, Mundra M (2010) Implementing digital signature with RSA encryption algorithm to enhance the data Security of Cloud in Cloud Computing. In: 1st International conference on parallel distributed and grid Computing (PDGC). IEEE Computer Society Washington
21. Harnik D, Pinkas B, Shulman- Peleg A (2010) Side channels in cloud services: deduplication in cloud storage. IEEE Secur Priv 8(6):40–47
22. Fong E, Okun V (2007) Web application scanners: definitions and functions. In: Proceedings of the 40th annual Hawaii International conference on system sciences. IEEE Computer Society, Washington
23. Tebaa M, El Hajji S, El Ghazi A (2012) Homomorphic encryption method applied to cloud computing. In: National days of network security and systems (JNS2). IEEE Computer Society, Washington
24. Berger S, Cáceres R, Pendarakis D, Sailer R, Valdez E, Perez R, Schildhauer W, Srinivasan D (2008) TVDc: managing Security in the trusted virtual data center. SIGOPS Oper Syst Rev 42(1):40–47
25. Xiao S, Gong W (2010) Mobility can help: protect user identity with dynamic credential. In: Eleventh international conference on mobile data management (MDM). IEEE Computer Society, Washington
26. Wang Z, Jiang X (2010) HyperSafe: a lightweight approach to provide lifetime hypervisor control-flow integrity. In: Proceedings of the IEEE symposium on security and privacy. IEEE Computer Society, Washington, DC
27. Santos N, Gummadi KP, Rodrigues R (2009) Towards trusted cloud computing. In: Proceedings of the 2009 conference on hot topics in cloud computing, San Diego, California. USENIX Association Berkeley, CA
28. Krautheim FJ (2009) Private virtual infrastructure for cloud computing. In: Proceedings of the HOTCLOUD conference 2009. ACM, New York
29. Ouedraogo et al (2015) Security transparency: the next frontier for security research in the cloud. J Cloud Comput Adv Syst Appl 4:12
30. Berger S, Cáceres R, Goldman K, Pendarakis D, Perez R, Rao JR, Rom E, Sailer R, Schildhauer W, Srinivasan D, Tal S, Valdez E (2009) Security for the cloud infrastructure: trusted virtual data center implementation. IBM J Res Dev 53(4):6
31. Naehrig M, Lauter K, Vaikuntanathan V (2011) Can homomorphic encryption be practical? In: Proceedings of the 3rd ACM workshop on cloud computing security workshop. ACM, New York
32. Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing Security of virtual machine images in a Cloud environment. In: Proceedings of the 2009 ACM workshop on cloud computing security. ACM, New York
33. Han-zhang W, Liu-sheng H (2010) An improved trusted cloud computing platform model based on DAA and privacy CA scheme. In: International conference on computer application and system modeling (ICCASM), Vol. 13, V13–39. IEEE Computer, Society, Washington, DC
34. Xiaopeng G, Sumei W, Xianqin C (2010) VNSS: A network security sandbox for virtual computing environment. In: IEEE youth conference on information computing and telecommunications (YC-ICT). IEEE Computer Society, Washington
35. Wu H, Ding Y, Winer C, Yao L (2010) Network security for virtual machine in cloud computing. In: 5th International conference on computer sciences and convergence information technology (ICCIT). IEEE Computer Society, Washington
36. Habiba et al (2014) Cloud identity management security issues & solutions: a taxonomy. Complex Adapt Syst Model 2:5
37. Zhang F, Huang Y, Wang H, Chen H, Zang B (2008) PALM: security preserving VM live migration for systems with VMM-enforced protection. In: Trusted infrastructure technologies conference, 2008. APTC'08, Third Asia-Pacific. IEEE Computer Society, Washington, DC