UNDERSTANDING THE SECURITY CONCERNS SURROUNDING CLOUD COMPUTING: A REVIEW

Tummapudi Sunil
Research Scholar
Department of Computer Science and Engineering
OPJS University, Churu Rajasthan

Dr. Vijay Pal Singh
Research Guide
Department of Computer Science and Engineering
OPJS University, Churu Rajasthan

Abstract

A proved, adaptable, and economical delivery model, cloud computing enables the provision of enterprise or consumer IT services via the Internet. Nevertheless, cloud computing introduces an additional degree of vulnerability due to the frequent delegation of critical services to external entities. This practice complicates the task of ensuring data security and privacy, ensuring the availability of data and services, and substantiating compliance. Cloud Computing utilizes numerous technologies (SOA, virtualization, Web 2.0); consequently, it inherits their security concerns, which are examined in this article. Our objective is to identify and correlate potential solutions to the most significant threats and vulnerabilities discovered in the literature pertaining to Cloud Computing and its environment.

Keywords: *Cloud Computing, Security Issues, Cyber security, Data Privacy.*

Introduction

Cloud computing is gaining popularity in science and industry. Cloud computing is the first of the ten most important technologies, and its adoption by companies and organizations is improving, according to Gartner [1].

Cloud computing provides simple, wherever, and anytime network connection to customizable computer resources including servers, storage, apps, and services. Service providers and management may easily provide and cancel these resources.

Cloud computing is a distribution architecture and computational paradigm that provides safe, efficient, and easy computing and data storage. This context treats all computer resources as Internet-delivered services [2,3]. Improved cooperation, agility, scalability, availability, demand adaptability, expedited development work, and cost savings via effective and optimal computing are all advantages of the cloud [4–7].

Cloud computing combines SOA, Web 2.0, virtualization, and more. It provides web-based business applications via web browsers. Software and data are stored on servers to meet user computing needs [5]. Cloud computing is a marketing phrase for technological advancements and services [6]. In this way, cloud computing matures these technologies. Cloud Computing has many benefits, but it faces several barriers to adoption. Compliance, privacy, and legal difficulties are major adoption barriers, followed by security [8]. The novelty of Cloud Computing raises questions about the possibility of establishing security measures across all tiers (e.g., network, host, application, and data) and migrating application security to Cloud Computing [9]. Information executives have consistently cited cloud computing security as their top issue due to uncertainty [10].

Vulnerabilities include external data storage, "public" internet use, lack of control, multi-tenancy, and internal security integration. The cloud's wide breadth and completely dispersed, heterogeneous, and virtualized resources set it apart from traditional technology. Traditional cloud security measures including identity verification, authentication, and permission are insufficient [11]. Most cloud computing security policies are similar to those in traditional IT settings. Cloud computing may bring different risks than traditional IT solutions owing to its operational structures, cloud service models, and supporting technologies. Unfortunately, security often makes these solutions more inflexible [4].

Organizations growing outside their data center worry about migrating key apps and sensitive data to public cloud environments. To address these concerns, a cloud solution provider must ensure that clients retain the same security and privacy controls across their services and applications, provide customers with proof that their organizations are secure and can meet service-level agreements, and allow auditors to verify compliance [12].

The SPI model (SaaS, PaaS, and IaaS) is used to classify Cloud Computing security threats in this article. We highlight the main system flaws and highest-level dangers in Cloud Computing and its surrounds literature. A threat is a potential attack that might misuse resources or information, whereas a vulnerability is a system flaw that allows an attack. Some polls focus on a specific service type, while others discuss cloud security risks without distinguishing vulnerabilities and attacks. This paper lists vulnerabilities, threats, and cloud service models that may be affected. We also explain the relationship between these vulnerabilities and threats, explain how these vulnerabilities can be used to launch an attack, and suggest countermeasures to fix or improve the identified issues.

Systematic Review of Security Issues for Cloud Computing

A systematic review [13-15] was conducted to examine the extant literature on security in Cloud Computing. The primary objectives of this review were to identify and analyze the prevailing security issues and threats pertaining to Cloud Computing, as well as to provide a comprehensive summary of the current state of security in this domain.

Selection of Sources

The authors of this work determined the selection criteria for study sources based on their research experience. Certain constraints were taken into account during the source selection process: studies included in the sources had to be written in English and were accessible via the internet. The sources that were taken into consideration include ScienceDirect, the ACM digital library, the IEEE digital library, Scholar Google, and DBLP. Subsequently, the outcomes shall be refined by the specialists, who shall incorporate significant works that were not recovered from these sources and revise them to account for additional limitations including impact factor, received citations, prestigious journals, authors, and so forth.

After establishing the sources, it became imperative to delineate the procedure and the standards by which the studies were chosen and assessed. In this investigation, the criteria for inclusion and exclusion were determined by the research query. As a result, it was determined that the research must encompass subjects and issues that pertain to the security of cloud computing, as well as provide descriptions of potential threats, vulnerabilities, countermeasures, and risks.

Review Execution

During this stage, it is necessary to conduct a search in the specified sources and assess the acquired studies based on the predetermined criteria. We obtained approximately 120 results after executing the search chain on the chosen sources; these results were then filtered using the inclusion criteria to yield forty studies that met the criteria for relevance. Once more, the exclusion criteria were applied to this set of pertinent studies, resulting in a subset of studies that aligns with fifteen primary proposals [4, 6, 10, 16-27].

Results and Discussion

The findings of the systematic review are succinctly presented in Table 1, which provides an overview of the concepts and subjects that were examined for each methodology.

As shown in Table 1, the majority of the discussed approaches identify, categorize, assess, and enumerate a variety of Cloud Computing-specific vulnerabilities and hazards. The studies conduct an analysis of risks and threats, frequently providing recommendations on how to prevent or mitigate them. As a consequence, there is a direct correlation between vulnerabilities or threats and potential solutions and mechanisms to address them. Furthermore, our investigation reveals that numerous approaches address not only threats and vulnerabilities but also other security-related concerns such as trust, data security, and security recommendations and mechanisms for addressing any of the challenges encountered in cloud environments.

Security in the SPI Model

Three kinds of services are offered by the cloud model [21,28,29]:SaaS refers to software as a service. The consumer is granted the ability to utilize the applications developed by the provider, which are operating on a cloud infrastructure. The applications are accessible via a thin client interface (e.g., web browser for web-based email) from a variety of client devices.

As a Service Platform (PaaS). The user is granted the ability to deploy their own applications onto the cloud infrastructure without the need to install any platforms or tools on their local devices. PaaS denotes the provision of resources at the platform layer, such as software development frameworks and operating system support, which are utilized in the construction of higher-level services.

SaaS places the responsibility for security squarely on the cloud provider. This is partially attributable to the SaaS model's high degree of integrated functionality and minimal customer control or extensibility requirements, which is a result of the degree of abstraction. In contrast, the PaaS model provides increased consumer control and extensibility. As a result of the comparatively reduced level of abstraction, IaaS affords customers or tenants enhanced authority over security in comparison to PaaS and SaaS [10].

Prior to examining security challenges in cloud computing, it is imperative to comprehend the interconnections and reliances that exist among these models of cloud services [4]. Since both PaaS and SaaS are hosted on top of IaaS, any security incident in IaaS will affect the security of those services. However, the inverse may also hold true. Nonetheless, it is crucial to consider that PaaS provides a foundation for developing and deploying SaaS applications, thereby augmenting the security interdependence among them. Due to the profound interdependencies present, any assault targeting a cloud service tier has the potential to compromise the higher layers. While every cloud service model has its own set of inherent security vulnerabilities, there are also certain challenges that are universally applicable to all of them. The interdependencies and associations among cloud models could potentially give rise to security vulnerabilities as well. A development environment may be rented by a SaaS provider from a PaaS provider, which in turn may rent an infrastructure from an IaaS provider. Due to the fact that individual service providers are tasked with securing their own offerings, the combination of security models may be inconsistent. It also complicates the determination of which service provider is liable in the event of an attack.

Application Security

Typically, these applications are distributed via the Web via a web browser [12,22]. Nevertheless, weaknesses present in web applications could give rise to susceptibilities for SaaS applications. Cybercriminals have been exploiting the internet to compromise the devices of users and carry out malicious tasks, including the theft of sensitive data [31]. SaaS applications face the same security challenges as any other web application technology; however, conventional security solutions are insufficient to defend them from assaults, necessitating the development of novel approaches [21]. The ten most critical hazards to the security of web applications have been identified by the Open Web Application Security Project (OWASP) [32]. While there remain further security concerns, this constitutes a commendable initial effort towards fortifying web applications.

Multi-Tenancy

Maturity models for SaaS applications are established on the basis of the subsequent attributes: scalability, metadata configurability, and multi-tenancy [30,33]. In the initial maturity model, every client is provided with an individualized instance of the software. Although this model does have some limitations, security concerns are not as severe as those of other models. In the second model, while the vendor does offer unique application instances to each client, the application code remains consistent across all instances. Customers can modify certain configuration options in this model to suit their requirements. Multitenancy is incorporated into the third maturation paradigm so that a solitary instance can cater to all clients [34]. Although this method increases resource utilization efficiency, its scalability is restricted. Due to the likelihood that data from multiple tenants will be stored in the same database, there is a significant risk of data leakage between these tenants. Security policies are essential for the purpose of segregating customer data from that of other consumers [35]. In order to increase the scalability of applications for the final model, they may be relocated to a more potent server if necessary.

Data Security

Data security is an issue that affects all technologies, but it presents a significant obstacle for SaaS users who depend on their providers to ensure adequate protection [12,21,36]. Frequently, organizational data is processed and stored in the cloud in raw text within SaaS. It is the responsibility of the SaaS provider to ensure the security of the data during processing and storage [30]. Furthermore, while data storage is an essential component for facilitating recovery in the event of a catastrophe, it also presents security risks [21]. Additionally, cloud service providers may subcontract backup and other services to third-party service providers, which may cause concern. Furthermore, in the realm of cloud computing, compliance with regulations is not anticipated by the majority of compliance standards [12]. Compliance in the SaaS industry is a complex process due to the fact that data is stored in the datacenters of the provider. This may give rise to regulatory compliance concerns, including but not limited to data privacy, segregation, and security, which the provider is obligated to enforce.

Platform as a Service (PAAS) Security Issues

PAAS enables the installation of cloud-based applications without incurring the expenses associated with procuring and managing the underlying software and hardware layers [21]. Similar to SAAS and IAAS, PAAS requires a dependable and secure web browser and network. Security of customer applications deployed on a PAAS platform comprises two software layers: security of the runtime engine of the PAAS platform and security of the customer applications themselves [10]. It is the responsibility of PAAS providers to ensure the security of the platform software architecture, which comprises the runtime engine utilized to execute customer applications. In the same way that SAAS introduces data security concerns and additional obstacles, PAAS presents the following:

Third-Party Relationships

In addition to conventional programming languages, PAAS also provides components of third-party web services, including mashups [10,38]. Mashups integrate multiple source components into a unified entity. Consequently, PAAS models also acquire security concerns associated with mashups, including those pertaining to data and networks [39]. Additionally, PAAS consumers must rely on third-party services and web-hosted development tools for security.

Development Life Cycle

From an application development standpoint, the construction of secure applications that may be hosted in the cloud presents a formidable challenge. The rate of application evolution in the cloud will have an impact on both the security and System Development Life Cycle (SDLC) [12,24]. In light of the fact that PaaS applications should be routinely upgraded, it is the responsibility of developers to ensure that their application development processes are adaptable [19]. Nevertheless, it is crucial for developers to comprehend that tampering with PaaS components could potentially undermine the security of their applications. In addition to understanding secure development techniques, developers must also be informed about data law in order to prevent data from being stored in inappropriate locations. Data may be stored in various locations governed by distinct legal systems, which may compromise its security and privacy.

Infrastructure as a Service (IAAS) Security Issues

IAAS offers a repository of computational resources, including storage, networks, servers, and storage, in the form of virtualized systems that can be accessed via the Internet [24]. Users are granted complete authority and administration over the resources allocated to them in order to execute any software [18]. IAAS grants cloud users enhanced security control in comparison to alternative models, provided that the virtual machine monitor remains devoid of any security vulnerabilities [21]. They have authority over the software that operates within their virtual machines and are tasked with the accurate configuration of security policies [41]. The compute, network, and storage infrastructure, nevertheless, are under the control of cloud service providers. IaaS providers are obligated to implement robust security measures for their systems to mitigate the risks associated with creation, communication, monitoring, modification, and mobility [42]. Presented below are several security concerns that are linked to IaaS.

Virtual Machine Monitor

The Virtual Machine Monitor (VMM) or hypervisor isolates virtual machines, thus if it's compromised, so may its virtual machines. Low-level VMM software manages and monitors virtual machines, hence it has security weaknesses like any other program [45]. Since vulnerabilities are simpler to identify and correct, keeping the VMM simple and small minimizes security risks.

Virtualization allows virtual machine migration between physical servers for fault tolerance, load balancing, and maintenance [16,46]. This handy feature might cause security issues [42,43,47]. An attacker may exploit the VMM migration module and move a victim virtual machine to a hostile server. Since VM migration exposes VM material to the network, data integrity and confidentiality may be compromised. Migrating a malicious virtual machine to another host (with another VMM) compromises it.

The same server may host shared resource VMs that share CPU, memory, I/O, and more. Sharing resources may reduce VM security. A rogue VM may infer information about other VMs from shared memory or other resources without compromising the hypervisor [46]. Using covert channels, two VMs may evade all VMM security module restrictions [48]. Thus, a malicious Virtual Machine may monitor shared resources without its VMM noticing, allowing the attacker to deduce information about other virtual machines.

Public VM Image Repository

In IAAS setups, VM images are prepackaged software templates with VM configuration files. Thus, these photos are crucial to cloud security [46,49]. One may make her own VM image or utilize one from the provider's repository. For instance, Amazon provides a public repository for lawful users to download or publish VM images. malevolent people may store photos with malicious code in public repositories, compromising other users or the cloud [20,24,25]. An attacker with a legitimate account may generate a Trojan horse picture. This picture will infect another customer's virtual computer with concealed spyware. Additionally, VM replication might mistakenly disclose data [20]. Passwords and cryptographic keys may be recorded during picture creation. If the picture is not "cleaned," other users might see sensitive information. Dormant VM images are challenging to fix offline [50].

Virtual Machine Rollback

In addition, in the event of an error, virtual machines can be reverted back to their prior configurations. However, reverting to a previous version of virtual machines may re-establish access to corrected security flaws or re-establish previously disabled accounts or credentials. To facilitate rollbacks, a "copy" (snapshot) of the virtual machine must be created; this process may lead to the propagation of configuration errors and other susceptibilities [12,44].

Virtual Machine Life Cycle

Furthermore, it is critical to comprehend the lifecycle of the virtual machines (VMs) and the manner in which their states evolve while traversing the environment. The fact that VMs may be powered on, off, or suspended complicates the detection of malware. Furthermore, virtual machines remain susceptible to vulnerabilities even when they are not operational [24]. For instance, a virtual machine could be initiated using an image that harbors malicious code. These malevolent images have the potential to initiate the spread of malware through the injection of malicious code into other virtual machines during their construction.

Virtual Networks

A result of resource aggregation, various tenants utilize the same network components. As previously stated, resource sharing enables adversaries to conduct cross-tenant assaults [20]. The increased interconnectivity of VMs made possible by virtual networks poses a significant security challenge for cloud computing [51]. Connecting each virtual machine to its host via dedicated physical channels is the most secure method. However, the majority of hypervisors connect VMs via virtual networks so that they can communicate more efficiently and directly. For example, the majority of virtualization platforms, including Xen, offer two configuration options for virtual networks: routed and bridged. However, employing these methods increases the vulnerability to certain attacks, such as spoofing and monitoring virtual networks [45,52].

Analysis of Security Issues in Cloud Computing

Researching Cloud Computing security threats. The vulnerabilities and dangers that influence cloud service models are identified. Examining cloud vulnerabilities. This article briefly discusses cloud service model flaws and insecurity. Our analysis focuses on technology-based risks, although business issues may affect cloud and platform security. The following are weaknesses:

Some cloud companies don't vet vendors or staff [16]. Data access is typically limitless for cloud administrators. Many cloud services allow anybody with a credit card and email to sign up. Fraudulent accounts help thieves get away with anything [16]. People are information security vulnerabilities without security education [53]. This is true in any business, but cloud providers, third-party providers, suppliers, organizational customers, and end-users use it more.

Cloud ecosystems evolve via internet, browsers, and virtualization. A failure in these technologies might dramatically impact the cloud.

Conclusions

Cloud computing is innovative and beneficial, but security concerns may limit its use. Firms may go to the Cloud by understanding Cloud Computing vulnerabilities. Because Cloud Computing employs several technologies, it inherits security risks. Some solutions for web applications, data hosting, and virtualization are immature or nonexistent. IaaS, PaaS, and IaaS cloud models have different security problems. This paper says Cloud Computing's biggest security vulnerabilities are storage, virtualization, and networks. Virtualization worries cloud users because it enables several users share a server. Another difficulty is that virtualization platforms approach security differently. Some assaults target virtual networks, especially when connecting to remote virtual machines.

Some cloud security surveys ignored vulnerabilities and dangers. We explored this distinction to understand these issues. In addition to listing security problems, we linked threats and vulnerabilities to identify their execution shortcomings and strengthen the system. Some known therapies reduced these risks. The cloud architecture necessitates new security methodologies and revised solutions. Traditional security methods may fail in cloud environments owing to their complexity and mix of technology. Table 4 presents 3 use patterns [46]. We'll complete them.

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-future- kpmgs-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 Security 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/risk-management/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 and research 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

32. OWASP (2010) The Ten most critical Web application Security risks. Available: https://www.owasp.org/index.php/Category: OWASP_Top_Ten_Project

33. Zhang Y, Liu S, Meng X (2009) Towards high level SaaS maturity model: methods and case study. In: Services Computing conference. APSCC, IEEE Asia-Pacific, pp 273–278

34. Chong F, Carraro G, Wolter R (2006) Multi-tenant data architecture. Online. Available: http://msdn.microsoft.com/en-us/library/aa479086.aspx. Accessed: 05-Jun-201

35. Bezemer C-P, Zaidman A (2010) Multi-tenant SaaS applications: maintenance dream or nightmare? In: Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE), Antwerp, Belgium. ACM New York, NY, USA, pp 88–92

36. Viega J (2009) Cloud Computing and the common Man. Computer 42 (8):106–108

37. Cloud Security Alliance (2012) Security guidance for critical areas of Mobile Computing. Available: https://downloads.cloudsecurityalliance.org/initiatives/ mobile/Mobile_Guidance_v1.pdf

38. Keene C (2009) The Keene View on Cloud Computing. Online. Available: http://www.keeneview.com/2009/03/what-is-platform-as-service-paas.html. Accessed: 16-Jul-

2011

39. 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, DC, USA, pp 1–4

40. Chandramouli R, Mell P (2010) State of Security readiness. Crossroads 16 (3):23–25

41. Jaeger T, Schiffman J (2010) Outlook: cloudy with a chance of Security challenges and improvements. IEEE Security Privacy 8(1):77–80

42. Dawoud W, Takouna I, Meinel C (2010) Infrastructure as a service security: Challenges and solutions. In: the 7th International Conference on Informatics and Systems (INFOS), Potsdam, Germany. IEEE Computer Society, Washington, DC, USA, pp 1–8

43. Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, Washington, DC, USA, pp 35–41

44. Garfinkel T, Rosenblum M (2005) When virtual is harder than real: Security challenges in virtual machine based computing environments. In: Proceedings of the 10th conference on Hot Topics in Operating Systems, Santa Fe, NM. volume 10. USENIX Association Berkeley, CA, USA, pp 227–229

45. Reuben JS (2007) A survey on virtual machine Security. Seminar on Network Security. http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdf. Technical report, Helsinki University of Technology, October 2007

46. Hashizume K, Yoshioka N, Fernandez EB (2013) Three misuse patterns for Cloud Computing. In: Rosado DG, Mellado D, Fernandez-Medina E, Piattini M (ed) Security engineering for Cloud Computing: approaches and Tools. IGI Global, Pennsylvania, United States, pp 36–53

47. Venkatesha S, Sadhu S, Kintali S (2009) Survey of virtual machine migration techniques., Technical report, Dept. of Computer Science, University of California, Santa Barbara. http://www.academia.edu/760613/ Survey_of_Virtual_Machine_Migration_Techniques

48. Ranjith P, Chandran P, Kaleeswaran S (2012) On covert channels between virtual machines. Journal in Computer Virology Springer 8:85–97

49. 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, NY, USA, pp 91–96

50. Owens K Securing virtual compute infrastructure in the Cloud. SAVVIS. Available: http://www.savvis.com/en-us/info_center/documents/hos- whitepaper-securingvirutalcomputeinfrastructureinthecloud.pdf

51. 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, DC, USA, pp 18–21

52. 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 DC, USA, pp 395–398

53. Popovic K, Hocenski Z (2010) Cloud Computing Security issues and challenges. In: Proceedings of the 33rd International convention MIPRO. IEEE Computer Society Washington DC, USA, pp 344–349

54. Carlin S, Curran K (2011) Cloud Computing Security. International Journal of Ambient Computing and Intelligence 3(1):38–46

55. Bisong A, Rahman S (2011) An overview of the Security concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications (IJNSA) 3(1):30–45

56. Townsend M (2009) Managing a security program in a cloud computing environment. In: Information Security Curriculum Development Conference, Kennesaw, Georgia. ACM New York, NY, USA, pp 128–133

57. Winkler V (2011) Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier Inc, Waltham, MA

58. Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA. ACM New York, NY, USA, pp 199–212

59. Zhang Y, Juels A, Reiter MK, Ristenpart T (2012) Cross-VM side channels and their use to *extract private keys. In: Proceedings of the 2012 ACM conference on Computer and communications security, New York, NY, USA. ACM New York, NY, USA, pp 305–316*

60. 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, USA, pp 380–395