An Empirical Analysis of Security Issues in Cloud Environment

Rajesh Kumar Pandey, Dr. Amit Chaturvedi

[1]Ph.D. Scholar, Bhagwant University Ajmer, Rajasthan ,India
[2]Assistant Professor, MCA Department, Govt. Engineering College, Ajmer ,India

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, Security Issues, SAAS , PAAS, IAAS , Multi-tenancy , Data Security , Accessibility, Virtualization, Virtual networks

I. 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 exploited in order to perform an attack, and also present some countermeasures related to these threats which try to solve or improve the identified problems.

II. SECUITY IN THE CLOUD ARCHITECTURE [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 and dependencies 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.

III. SECUITY ISSUES IN SOFTWARE-AS-SERVICE (SAAS)

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

•**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.

•**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.

• **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.

•**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.

IV. SECUITY ISSUES IN PLATFORM-AS-SERVICE (PAAS)

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:

•**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.

• **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 processes are flexible enough to keep up with changes [19]. However, developers also have to understand that any changes in PaaS components can compromise the security of their applications. Besides secure development techniques, developers need to be educated about data legal issues as well, so that data is not stored in inappropriate locations. Data may be stored on different places with different legal regimes that can compromise its privacy and security.

• **Underlying infrastructure security**

In PaaS, developers do not usually have access to the underlying layers, so providers are responsible for securing the underlying infrastructure as well as the applications services[40]. Even when developers are in control of the security of their applications, they do not have the assurance that the development environment tools provided by a PaaS provider are secure.

In conclusion, there is less material in the literature about security issues in PaaS. SaaS provides software delivered over the web while PaaS offers development tools to create SaaS applications. However, both of them may use multi-tenant architecture so multiple concurrent users utilize the same software. Also, PaaS applications and user's data are also stored in cloud servers which can be a security concern as discussed on the previous section. In both SaaS and PaaS, data is associated with an application running in the cloud. The security of this data while it is being processed, transferred, and stored depends on the provider.

V. SECUITY ISSUES IN INFRASTRUCTURE-AS-SERVICE (IAAS)

IaaS provides a pool of resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet[24]. Users are entitled to run any software with full control and management on the resources allocated to them [18]. With IaaS, cloud users have better control over the security compared to the other models as long there is no security hole in the virtual machine monitor [21]. They control the software running in their virtual machines, and they are responsible to configure security policies correctly [41]. However, the underlying compute, network, and storage infrastructure is controlled by cloud providers. IaaS providers must undertake a substantial effort to secure their systems in order to minimize these threats that result from creation, communication, monitoring, modification, and mobility [42]. Here are some of the security issues associated to IaaS.

• **Virtualization**

Virtualization allows users to create, copy, share, migrate, and roll back virtual machines, which may allow them to run a variety of applications [43,44]. However, it also introduces new opportunities for attackers because of the extra layer that must be secured [31]. Virtual machine security becomes as important as physical machine security, and any flaw in either one may affect the other [19]. Virtualized environments are vulnerable to all types of attacks for normal infrastructures; however, security is a greater challenge as virtualization adds more points of entry and more interconnection complexity [45]. Unlike physical servers, VMs have two boundaries: physical and virtual [24].

• **Virtual machine monitor**

The Virtual Machine Monitor (VMM) or hypervisor is responsible for virtual machines isolation; therefore, if the VMM is compromised, its virtual machines may potentially be compromised as well. The VMM is a low-level software that controls and monitors its virtual machines, so as any traditional software it entails security flaws [45]. Keeping the VMM as simple and small as possible reduces the risk of security vulnerabilities, since it will be easier to find and fix any vulnerability.

Moreover, virtualization introduces the ability to migrate virtual machines between physical servers for fault tolerance, load balancing or maintenance [16,46]. This useful feature can also raise security problems [42,43,47]. An attacker can compromise the migration module in the VMM and transfer a victim virtual machine to a malicious server. Also, it is clear that VM migration exposes the content of the VM to the network, which can compromise its data integrity and confidentiality. A malicious virtual machine can be migrated to another host (with another VMM) compromising it.

• **Shared resource**

VMs located on the same server can share CPU, memory, I/O, and others. Sharing resources between VMs may decrease the security of each VM. For example, a malicious VM can infer some information about other VMs through shared memory or other shared resources without need of compromising the hypervisor [46]. Using covert channels, two VMs can communicate bypassing all the rules defined by the security module of the VMM [48]. Thus, a malicious Virtual Machine can monitor shared resources without being noticed by its VMM, so the attacker can infer some information about other virtual machines.

• **Public VM image repository**

In IaaS environments, a VM image is a prepackaged software template containing the configurations files that are used to create VMs. Thus, these images are fundamental for the the overall security of the cloud [46,49]. One can either create her own VM image from scratch, or one can use any image stored in the provider's repository. For example, Amazon offers a public image repository where legitimate users can download or upload a VM image. Malicious users can store images containing malicious code into public repositories compromising other users or even the cloud system [20,24,25]. For example, an attacker with a valid account can create an image containing malicious code such as a Trojan horse. If another customer uses this image, the virtual machine that this customer creates will be infected

with the hidden malware. Moreover, unintentionally data leakage can be introduced by VM replication [20]. Some confidential information such as passwords or cryptographic keys can be recorded while an image is being created. If the image is not "cleaned", this sensitive information can be exposed to other users. VM images are dormant artifacts that are hard to patch while they are offline [50].

• **Virtual machine rollback**

Furthermore, virtual machines are able to be rolled back to their previous states if an error happens. But rolling back virtual machines can re-expose them to security vulnerabilities that were patched or re-enable previously disabled accounts or passwords. In order to provide rollbacks, we need to make a "copy" (snapshot) of the virtual machine, which can result in the propagation of configuration errors and other vulnerabilities[12,44].

• **Virtual machine life cycle**

Additionally, it is important to understand the lifecycle of the VMs and their changes in states as they move through the environment. VMs can be on, off, or suspended which makes it harder to detect malware. Also, even when virtual machines are offline, they can be vulnerable [24]; that is, a virtual machine can be instantiated using an image that may contain malicious code. These malicious images can be the starting point of the proliferation of malware by injecting malicious code within other virtual machines in the creation process.

• **Virtual networks**

Network components are shared by different tenants due to resource pooling. As mentioned before, sharing resources allows attackers to launch cross-tenant attacks [20]. Virtual Networks increase the VMs interconnectivity, an important security challenge in Cloud Computing [51]. The most secure way is to hook each VM with its host by using dedicated physical channels. However, most hypervisors use virtual networks to link VMs to communicate more directly and efficiently. For instance, most virtualization platforms such as Xen provide two ways to configure virtual networks: bridged and routed, but these techniques increase the possibility to perform some attacks such as sniffing and spoofing virtual network [45,52].

VI. SECUITY ISSUES IN PLATFORM-AS-SERVICE (PAAS)

We systematically analyze now existing security vulnerabilities and threats of Cloud Computing. For each vulnerability and threat, we identify what cloud service model or models are affected by these security problems.

•**Lack of employee screening and poor hiring practices** [16] – some cloud providers may not perform background screening of their employees or providers. Privileged users such as cloud administrators usually have unlimited access to the cloud data.

•**Lack of customer background checks** – most cloud providers do not check their customer's background, and almost anyone can open an account with a valid credit card and email. Apocryphal accounts can let attackers perform any malicious activity without being identified [16].

•**Lack of security education** – people continue to be a weak point in information security [53]. This is true in any type of organization; however, in the cloud, it has a bigger impact because there are more people that interact with the cloud: cloud providers, third-party providers, suppliers, organizational customers, and end-users.

VII. CONCLUSION

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.

REFERENCES

[1] J. Linn, "Generic Security Service Application Program Interface", RFC-2743, RSA Laboratories, January 2000.

[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.

[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.

[4] Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0..

[5] Available:https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdfwebcite
[6] Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China.
[7] Centre for the Protection of National Infrastructure (2010) Information Security Briefing 01/2010 Cloud Computing.
[8] Available:http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf webcite
[9] Khalid A (2010) Cloud Computing: applying issues in Small Business. International Conference on Signal Acquisition and Processing (ICSAP'10).
[10] KPMG (2010) From hype to future: KPMG's 2010 Cloud Computing survey..
[11] Available:http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291webcite
[12] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):
[13] Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. Sebastopol, CA
[14] 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. Beijing, China
[15] Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation
[16] Kitchenham B (2004) Procedures for perfoming systematic review, software engineering group. Australia: Department of Computer Scinece Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd.
[17] 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.
[18] Brereton P, Kitchenham BA, Budgen D, Turner M, Khalil M (2007) Lessons from applying the systematic literature review process within the software engineering domain.
[19] Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0.
[20] Available: https://cloudsecurityalliance.org/research/top-threats website.
[21] ENISA (2009) Cloud Computing: benefits, risks and recommendations for information Security.
[22] Available: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment webcite
[23] 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.
[24] 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.
[25] Grobauer B, Walloschek T, Stocker E (2011) Understanding Cloud Computing vulnerabilities.
[26] Subashini S, Kavitha V (2011) A survey on Security issues in service delivery models of Cloud Computing.
[27] 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).
[28] Onwubiko C (2010) Security issues to Cloud Computing. In: Antonopoulos N, Gillam L (eds) Cloud Computing: principles, systems & applications, Springer-Verlag:
[29] Morsy MA, Grundy J, Müller I (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop.
[30] 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.
[31] Zissis D, Lekkas D (2012) Addressing Cloud Computing Security issues.
[32] Jansen W, Grance T (2011) Guidelines on Security and privacy in public Cloud Computing.
[33] Mell P, Grance T (2011) The NIST definition of Cloud Computing. Gaithersburg, MD: NIST, Special Publication 800–145.
[34] Zhang Q, Cheng L, Boutaba R (2010) Cloud Computing: state-of-the-art and research challenges. Journal of Internet Services Applications 1(1):7-18Publisher
[35] 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. Washington, DC, USA: IEEE Computer Society. pp 384-387
[36] Owens D (2010) Securing elasticity in the Cloud. Commun ACM 53(6):46-51

[37] OWASP (2010) The Ten most critical Web application Security risks.
[38] Available:https://www.owasp.org/index.php/Category: OWASP_Top_Ten_Projectwebcite
[39] Zhang Y, Liu S, Meng X (2009) Towards high level SaaS maturity model: methods and case study. In: Services Computing conference. IEEE Asia-Pacific: APSCC. pp 273-278
[40] Chong F, Carraro G, Wolter R (2006) Multi-tenant data architecture.
[41] Online. Available: http://msdn.microsoft.com/en-us/library/aa479086.aspx webcite. Accessed: 05-Jun-2011
[42] 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. NY, USA: ACM New York. pp 88-92
[43] Viega J (2009) Cloud Computing and the common Man. Computer 42(8):106-108
[44] Cloud Security Alliance (2012) Security guidance for critical areas of Mobile Computing.
[45] Available:https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdfwebcite
[46] Keene C (2009) The Keene View on Cloud Computing.
[47] Online. Available:http://www.keeneview.com/2009/03/what-is-platform-as-service-paas.html website. Accessed: 16-Jul-2011
[48] 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. Washington, DC, USA: IEEE Computer Society. pp 1-4 PubMed Abstract | Publisher Full Text
[49] Chandramouli R, Mell P (2010) State of Security readiness. Crossroads 16(3):23-25
[50] Jaeger T, Schiffman J (2010) Outlook: cloudy with a chance of Security challenges and improvements. IEEE Security Privacy 8(1):77-80
[51] 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. Washington, DC, USA: IEEE Computer Society. pp 1-8
[52] 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. Washington, DC, USA: IEEE Computer Society. pp 35-41
[53] 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. CA, USA: USENIX Association Berkeley. pp 227-229
[54] Reuben JS (2007) A survey on virtual machine Security. Seminar on Network Security.
[55] http://www.tml.tkk.fi/Publications/C/25/papers/Reuben_final.pdfwebcite. Technical report, Helsinki University of Technology, October 2007
[56] Hashizume K, Yoshioka N, Fernandez EB (2013) Three misuse patterns for Cloud Computing. In: Rosado DG, Mellado D, Fernandez-Medina E, Piattini M (eds) Security engineering for Cloud Computing: approaches and Tools, Pennsylvania, United States: IGI Global. pp 36-53
[57] Venkatesha S, Sadhu S, Kintali S (2009) Survey of virtual machine migration techniques. Technical report, Dept. of Computer Science, University of California, Santa Barbara: .
[58] http://www.academia.edu/760613/Survey_of_Virtual_Machine_Migration_Techniqueswebcite
[59] Ranjith P, Chandran P, Kaleeswaran S (2012) On covert channels between virtual machines. Journal in Computer Virology Springer 8:85-97 Publisher Full Text
[60] 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. NY, USA: ACM New York. pp 91-96
[61] Owens K Securing virtual compute infrastructure in the Cloud. SAVVIS.
[62] Available: http://www.savvis.com/en-us/info_center/documents/hos-whitepaper-securing virutalcomputeinfrastructureinthecloud.pdf
[63] 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). DC, USA: IEEE Computer Society Washington. pp 18-21
[64] 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). Washington DC, USA: IEEE Computer Society. pp 395-398

[65] 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
[66] Carlin S, Curran K (2011) Cloud Computing Security. International Journal of Ambient Computing and Intelligence 3(1):38-46
[67] 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 PubMed Abstract | Publisher Full Text |PubMed Central Full Text
[68] Townsend M (2009) Managing a security program in a cloud computing environment. In: Information Security Curriculum Development Conference, Kennesaw, Georgia. NY, USA: ACM New York. pp 128-133
[69] Winkler V (2011) Securing the Cloud: Cloud computer Security techniques and tactics. Waltham, MA: Elsevier Inc.
[70] 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. NY, USA: ACM New York. pp 199-212
[71] 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. NY, USA: ACM New York. pp 305-316
[72] 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. Washington, DC, USA: IEEE Computer Society. pp 380-395
[73] Wang C, Wang Q, Ren K, Lou W (2009) Ensuring data Storage Security in Cloud Computing. In: The 17th International workshop on quality of service. Washington, DC, USA:IEEE Computer Society. pp 1-9
[74] Fernandez EB, Yoshioka N, Washizaki H (2009) Modeling Misuse Patterns. In: Proceedings of the 4th Int. Workshop on Dependability Aspects of Data Warehousing and Mining Applications (DAWAM 2009), in conjunction with the 4th Int.Conf. on Availability, Reliability, and Security (ARES 2009), Fukuoka, Japan. Washington, DC, USA: IEEE Computer Society. pp 566-571
[75] 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. CA, USA: USENIX Association Berkeley.