A Survey on Security of Cloud Computing

Ruchi Dubey
Samrat Ashok
Technology Institute
Vidisha (M.P)

Nirmal Gaud
Samrat Ashok
Technology Institute
Vidisha (M.P)

ABSTRACT
Cloud computing is a derive technology that is still uncertain to many security troubles. The security problem becomes difficult under the cloud model as new scope enter into the problem extent related to the architecture, multi lease, layer dependency, and flexibility. On the other hand, these new dimensions create new vulnerabilities and possible attacks on a cloud system. This survey paper introduces a detailed analysis about attacks that are exacerbated by exploitation of the cloud system along with possible solutions.

Keywords
Cloud computing, Assets Analysis, Security issues

1. INTRODUCTION
Cloud computing has recently emerged as new pattern for hosting and delivering services over internet. It is a form of model that's suitable for, on-demand network access to a mutual cluster of configurable assets which will be quickly provisioned and free with least of organization effort or service supplier communication [1, 2].

This model attracts the eye of cluster of individuals as a result of its having a possible to supply unbelievable edges to the business and also the society. The shoppers (persons and business organizations) not ought to invest heaps within the data infrastructure technology (IT). Therefore users use assets provided by the cloud and pay in step with the employment. During this approach, there are a various major problems concerning organization that the cloud

facilitates for the protection. The two main cloud computing services are Amazon and Google that had major interruption. These interruption wasn't because of a security issue, solely showed simply however computing has become as the interruption for gather media expertise that enclosed international attention. But once organization moves to the cloud, most of the price of dysfunction is going to be economic and money. So they are seeing the possibility of health and questions of safety relating to cloud-based systems that support utility and medical infrastructure and this possibility has probably very severe price. Therefore in table1 defines the cloud model.

Table 1: Cloud Model

Five Essential Characteristics	1. On demand self-service
	2.Broad network access
	3.Resource pooling
	4.Rapid elasticity
	5.Measured Services
Three Service Models	1. Software as Service (Saas)
	2. Platform as service (Paas)
	3.Infrastructure as service (Iaas)
Deployment Models	1. Public Cloud
	2. Private Cloud
	3. Hybrid Cloud

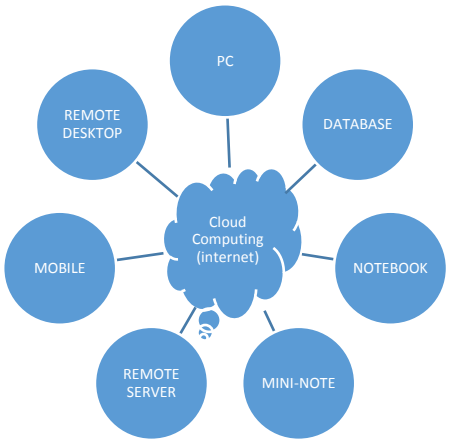

Figure 1: Cloud Computing Diagram

In cloud there are various security considerations relate to risk areas like external knowledge storage, dependency on the "public" web, lack of management, multi-tenancy and addition with internal security [3,4]. Not solely on existing issues, however these considerations have their origin directly heritable from the adopted technologies, save for this they're additionally regarding new problems derived from the composition of essential cloud computing options like measurability, resources sharing and virtualization (e.g., knowledge discharge and hypervisor vulnerabilities).

Traditional security mechanisms included various approaches such as identity; authentication and authorization are no longer enough for clouds in their existing form [5]. Moving to the essential application and sensitive data to public cloud environments is of great concern for those corporation that are moving beyond their data center's network under their control. A threat is a potential attack that may lead to a abuse of information or

resources, and the term vulnerability refers to the flaw in a system that allows an attack to be successful [3,4]. In this there is a list of vulnerabilities and threats, and they also indicate what cloud service models can be affect by them.

In this survey paper, various threats, assets and vulnerabilities for the security of cloud computing have been discussed with their some countermeasures or solution.

2. ASSETS TO BE ANALYZED

Basically, quality means that to that incorporates a worth or we are saying that object having some worth like; client knowledge or service. An asset that incorporates a worth, which must be shielded from threats in cloud security. Thus during this analysis varied kinds of assets square measure thought-about as follows: individuals, Activities, and Operation, info, Facilities and instrumentality, and Materials [6]. it's attractive to notice that within the cloud computing area, most of the vulnerabilities have an effect on that square measure individuals, Activities Operations, [7] and informational quality's of the organization however all the asset categories affects solely by the physical security vulnerability. In table1 they discuss that that quality worth is be a part of with that vulnerability as a result of their square measure varied single vulnerabilities that square measure enclosed with several assets worth in table 2.

Table2: Description of assets of value [8, 9, 10]

Assets of value	Vulnerabilities
People, Activities and Operations, Information, Facilities and Equipment, and Materials	Physical Security
People, Activities and Operations, Information,	Data Lockout
People, Activities and Operations, Information,	Loss of Data
People, Activities and Operations, Information,	Common Stack vulnerabilities
People, Activities and Operations, Information,	Execution Control
People, Activities and Operations, Information,	Multiparty Cloud Config
People, Activities and Operations, Information,	Authorization Issues
People, Activities and Operations, Information,	Real Time Access Issues
People, Activities and Operations, Information,	Identity Management
People, Activities and Operations, Information,	Security of Virtual App
People, Activities and Operations, Information,	Int and Ext Cloud App Interation
People, Activities and Operations, Information,	Trusted APIs
People, Information	Privacy of Data

Insistence could be a terribly difficult issue to live within the cloud computing area because the assets area unit pooled. These create transitive risks throughout the cloud structure that area unit merely not gift in normal systems wherever there's a non-shared assortment of assets. Thus it's having a possible to make distinctive and novel cascading impacts which will cause a number effect on the quality that's to be attacked. Once cloud computing becomes everyplace these drop the consequences have serious implications. So finally, once the mixture of vertically integrated impacts and cascading effects will cause feedback loops within the attack which will intensely increase its effect.

3. VARIABLES IN THREAT MODEL

Security can be broken into three main aspects which cover it fig2, namely:

1. Availability, which means data is available when needed.
2. Integrity, which means the data, is not modified without being detected.
3. Confidentiality, for the disclosure of data to un-authorized parties.

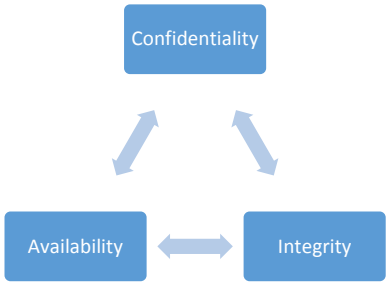

Figure 2: Security Triangle

4. LITERATURE SURVEY

In paper [11]; authors told that for users cloud computing offers high-end and scalable infrastructure at a coffee worth. Virtualization is that the key to detachment of cloud computing. This investigates that creating use of compromised virtual machines to execute large-scale Distributed Denial-of-Service (DDoS) attacks. For this they establish two main methods: initial, the intrusion is conceived to compromise VMs to launch a DDoS attack against a target that's external to the cloud. Second, develop security mechanisms for the additional ancient cloud intrusion, wherever the target of the attack is that the cloud or a component at intervals the cloud itself.

In paper [12]; authors mentioned a security risk methodology approach to assess the things which may risk the protection of the Cloud system and also the actors concerned within the Cloud. this enables work to be

categorize in terms of the foremost vital initial once assessing advanced ecosystems suggestive of Cloud environments that have too several parts that may fail throughout the service preparation or operation phases.

In paper [13]; authors told that the attacks will occur within the public clouds are common between the Cloud and ancient systems, however are exacerbated within the Cloud because of exploitation of multi-tenancy. These enclosed distributed denial of service, keystroke temporal arrangement, and side-channel attacks. What is more, some attacks that are specific to the Cloud paradigm are mentioned. These attacks exploit vulnerabilities in hypervisors and are ready to do malicious actions appreciate obstruction the Cloud resources for shoppers, eavesdropping on consumers' activities, and escaping fair proportion programming.

In paper [14]; authors planned numerous options that encourage the organizations and individual users to shift their applications and services to the cloud they're straightforward to manage, elastic, powerful resources on the fly, over the net. During this they elaborate the safety problems that arise thanks to the shared, virtualized and public nature of the cloud computing paradigm. The tabular analysis of the conferred techniques highlighted the scope of security provided by the reviewed techniques. Tabulated analysis can greatly facilitate the readers to check and analyze the professionals and cons of the analysis endeavors.

In paper [15]; authors analysis that however to look at accuracy for establishing a stronger security transparency between a cloud service provider(CSP) and a cloud service consumer(CSC) author projected some routes towards it. For this they take novel coding mechanisms, SLA and virtual machines watching are amongst the one. Through this they unmarked the importance of mutual trust concerns and also they would like the mutual audit ability within the cloud. So that they square measure having nice considerations concerning its security and privacy.

In paper [16]; authors planned a trust model that measures the protection strength and computes a trust price. A trust price consists of assorted parameters that square measure obligatory dimensions on that security of cloud services are measured. Trust model acts as a customary and ranking service to live security in a very cloud computing criterion. During this trust price is diagrammatic the output of the trust model that measures the protection strength. Trust model is integrated with the cloud services and their descriptions as a cloud service manager. Cloud service manager stores trust price store of registered cloud suppliers and their services. The trust price measures is accustomed choose a service globally by the users.

In paper [17]; authors discuss a baseline security analysis of the Cloud Computing Operational setting in terms of threats, vulnerabilities and impacts. The analysis is that the foremost serious threats area unit non-technical and may be resolved via management processes instead of technical countermeasures. In table 3 they describe three issues problems with their countermeasures area unit mentioned however they're not advanced with problems and answer in table 3.

Table 3: Countermeasures [18]

Issue	Countermeasures
Conflicts between customer procedures and cloud provider procedures.	Thoroughly researches and staffed, Service Level Agreement Contracts
Physical Theft	Standard FISMA, Physical Security Procedures
Malicious Insider	Standard FISMA, Personnel Security Procedures.

In paper [19]; authors told that valuable quality may be information it's a good considerations once moving towards the cloud. Information may be of varied varieties and degree of protection needed for all the info is additionally varies. Its security may be provided supported the extent and also the needed protection. Therefore author planned a classification technique that defines numerous parameters. All the weather that are hold on in cloud storage may be classified initial supported the content and access management parameters. Supported that, classification requirements may be given for storage and communication coding, integrity and access management mechanisms.

5. VARIOUS SECURITY ISSUES IN CLOUD COMPUTING

The cloud model provides three types of services that they called its SPI model. Each SPI model having its own security issues with their some countermeasures that are as follows:

5.1 Software-as-a-service (SaaS)

SaaS provides application services on demand admire email, [20] conferencing software system and business applications admire ERP, CRM, and SCM. The adoption of SaaS applications could raise some security issues. They're follows as:

5.1.1 Application security

These applications square measure usually delivered via the web through an internet browser. But, here were varied flaw in internet application which will produce vulnerabilities for the SaaS applications. To perform malicious activities attackers are mistreatment the net to compromise user's computers. That why security challenges in SaaS applications don't seem to be totally different from any internet application technology [21], however ancient security solutions don't effectively defend it from attacks, thus new approaches square measure necessary [22,23]. There square measure a lot of security problems, however it's a decent begin for securing internet applications.

5.1.2 Multi-tenancy

SaaS applications may be sorted into development models that square measure determined by the subsequent characteristics: measurability, configurability via information, and multi-tenancy. These approaches change additional capable use of the resources however measurability is restricted. Since knowledge from multiple tenants is probably going to be keep within the same info, the chance of information outflow between these tenants is high [20, 24]. Security policies square measure needed to

confirm that customer's knowledge square measure unbroken cut loose different customers.

5.1.3 Data Security

Data security may be a common concern for any technology; however it becomes a serious challenge once SaaS users ought to admit their suppliers for correct security [20, 25]. In SaaS, structure information is usually processed in plaintext and hold on within the cloud. The SaaS supplier is that the one liable for the safety of the information whereas is being processed and hold on. within the world of SaaS, the method of observance is complicated as a result of information is found within the provider's datacenters, which can introduce restrictive conformity problems adore information privacy, separation, and security, that has to be enforced by the supplier.

5.1.4 Accessibility

Accessing applications over the web via applications programmed makes access from any network device easier, as well as public computers and mobile devices [26]. The Cloud Security Alliance has free a document that describes this state of mobile computing and also the high threats during this space admire info stealing mobile malware, insecure networks (Wi-Fi), vulnerabilities found within the device OS and official applications, insecure marketplaces, and proximity-based hacking.

5.2 Platform-as-a-service (Paas)

As with SaaS and Iaas, Paas depends on a secure and reliable network and secure browser [25]. Paas application security contains 2 computer code layers: Security of the Paas platform itself (i.e., runtime engine), and Security of client applications deployed on a Paas platform. Paas supplier's area unit answerable for securing the platform computer code stack that has the runtime engine that runs the client applications. Same as SaaS, Paas additionally brings knowledge security problems and different challenges that area unit represented as follows:

5.2.1 Third-party Relationships

Third-party offers web services components such as mashups [27, 28]. 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 improvement of tools and third-party services.

5.2.2 Development Life Cycle

From the angle of the appliance development, developers face the complexness of building secure applications which will be hosted within the cloud [20]. However, developers even have to know that any changes in Paas parts will compromise the protection of their applications. Besides secure development techniques, developers have to be compelled to be educated regarding information legal problems further, in order that information isn't hold on in unsuitable locations. Information is also hold on completely different places with different legal regimes that may compromise its privacy and security.

5.2.3 Underlying Infrastructure Security

Developers don't sometimes have access to the underlying layers, therefore suppliers are answerable for securing the underlying infrastructure similarly because the applications services [29]. Therefore finally there's less material within the text regarding security problems in PaaS. SaaS provides computer code delivered over the net whereas PaaS offers development tools to form SaaS applications. However, each of them might use multi-tenant design therefore multiple synchronous users utilize identical computer code.

5.3 Infrastructure-as-a-Service (Iaas)

Iaas provides a pool of resources cherish servers, storage, networks, and different computing resources within the style of virtualized systems, that area unit accessed through the web [25,30]. With IaaS, cloud users have higher management over the safety compared to the opposite models as long there's no security hole within the virtual machine monitor. The management of software package running in their virtual machines, and that they area unit accountable to tack together security policies properly. Here is a unit that having number of the safety problems associated to IaaS.

5.3.1 Virtualization

It permits users to make, copy, share, migrate, and roll back virtual machines, which can enable them to run a range of applications [22, 31]. Virtualized environments square measure susceptible to every kind of attacks for traditional infrastructures; but, security could be a larger challenge as virtualization adds additional points of entry and additional interconnection complexness. In contrast to physical servers, VMs have two boundaries: physical and virtual.

5.3.2 Virtual Machine Monitor

The Virtual Machine Monitor (VMM) or hypervisor is to blame for virtual machines isolation; so, if the VMM is compromised, its virtual machines might doubtless be compromised similarly. The VMM is low-level software system that controls and monitors its virtual machines, thus as any ancient software system it entails security flaws [30]. Associate in attention of attacker will compromise the migration module within the VMM and transfer a victim virtual machine to a malicious server. Also, it's clear that VM migration exposes the content of the VM to the network, which might compromise its knowledge integrity and confidentiality.

5.3.3 Shared Resource

Sharing resources between VMs could decrease the safety of every VM [32, 33]. As an example, a malicious VM will infer some info regarding alternative VMs through shared memory or alternative shared resources while not would like of compromising the hypervisor. Thus, a malicious Virtual Machine will monitor shared resources while not being detected by its VMM, therefore the aggressor will infer some info regarding alternative virtual machines.

5.3.4 Virtual Machine Rollback

Virtual machines are able to be rolled back to their previous states if an error happens [20]. But rolling back virtual machines can re-expose them to security vulnerabilities that were patched or re-enable earlier disable 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 [39].

5.3.5 Virtual Networks

Virtual Networks increase the VMs interconnectivity, a vital security challenge in Cloud Computing. The foremost secure manner is to hook every VM with its host by victimization dedicated physical channels. However, most hypervisors use virtual networks to link VMs to speak additional directly and with efficiency. Let's say, most virtualization platforms love Xen offer 2 ways in which to set up virtual networks: bridged and routed, however these techniques increase the likelihood to perform some attacks love sniffing and spoofing virtual network.

6. ANALYSIS OF SECURITY ISSUES IN CLOUD COMPUTING

In associate degree organized manner they analyze the prevailing security in vulnerabilities and threats of the cloud computing [34,35]. Within the table three they outline every vulnerability and threat by explaining what cloud service model or model area unit plagued by this security downside [36,37]. The association between these two describes that however a threat will benefit of some vulnerability to regulate the system.

6.1 Threat

A threat may be a potential explanation for associate unwanted incident. In cloud computing threat analysis reveals distinctive challenges.

6.2 Vulnerabilities

Vulnerabilities are a spot or weakness in security that may be exploited by threats to achieve unauthorized access to associate in nursing quality [38]. So, by the top of definition of threat and vulnerabilities they conclude that ideally, potential threats poised to use the vulnerabilities. To illustrate, identity thieves can be a threat poised to use the vulnerability of poor coaching, and thereby cause a failure of confidentiality.

6.3 Relation between Threats and Vulnerabilities

In table4, the connection between threats and vulnerabilities describes however threat will cash in of some vulnerability to compromise the system. The most aim of this analysis is additionally to spot some existing defenses that may defeat these threats. They additionally offer temporary description of every threat measure.

Table4: Relationship between threats, vulnerabilities, and countermeasure

Threats	**Vulnerabilities**	**Incidents**	**Countermeasures**
Account or service Hijacking	Insecure interface and APIs	Get access target resources	Identity and Access Management Guidance
Data scavenging	Data related vulnerabilities	Data not removed completely from hard drive.	Specify destruction strategies on service-level agreement (SLA)
Data leakage	Data related vulnerabilities	To gain confidential information	FRS techniques/digital signatures
Denial of service	Insecure interface and APIs/ unlimited allocation of resources	An attacker request more computational resources	Cloud providers can force policies to offer limited computational resources
Malicious VM creation	Virtual Machine Images	Create a VM image containing malware	Mirage
Insecure VM migration	Virtual Machine	Showed attack against the migration functionality	PALM, TCC, VNSS
VM escape	Hypervisor	A zero-day exploit in the hyperVM virtualization application	Hypersafe TCCP (Trusted Cloud Computing Platform)

7. CONCLUSION

Security is an important fact for bold a reliable setting so the utilization of applications within the cloud and for business processes to virtualized infrastructures. This paper provides an intuition of varied threats and vulnerabilities in cloud computing. However these security problems don't seem to be enough that is why we have a tendency to create a relationship between threats and vulnerabilities. Thus from the threat analysis, we've got shown that the knowledge security principles of integrity, confidentiality and usefulness square measure most relevant to the cloud connected situations. The knowledge risk ratings performed shows the loss of confidentiality is rated because the highest level of risk followed by usefulness and integrity.

8. REFERENCES

[1] Lim, C., Superman, and A.: Risk analysis and comparative study of the different cloud computing providers in Indonesia. In: 2012 International Conference on Cloud Computing and Social Networking (ICCCSN). IEEE (2012).

[2] Mell, P., Grance, T.: The NIST Definition of Cloud Computing. National Institute of Standards and Technology, Information Technology Laboratory (2011).

[3] Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud ComputingV3.0 guidance/csaguide.v3.0.pdf.

[4] 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

[5] Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press.

[6] Kretzschmar, M., & Hanigk, S. (2010). Security Management Interoperability Challenges for Collaborative Clouds. Paper presented at 2010 4th International DMTF Academic Alliance Workshop on Systems and Virtualization Management, Ontario, Canada.

[7] Almorsy, M., Gundy, J., & Ibraham, A. (2011). Collaboration-based Cloud Computing Security Management Framework. Paper presented at 2011 IEEE 4th International Conference on Cloud Computing, Washington DC, USA.

[8] Wang, X., Huang, T., & Ren, Z. (2010). Research on the anti-virus system of military network based on cloud security. Paper presented at 2010 International Conference on Intelligent Computing and Integrated Systems (ICISS 2010), Guilin, China.

[9] Bayuk, J. (2011). Cloud Security Metrics. In Proc. of the 2011 6th International Conference on System of Systems Engineering, Albuquerque, New Mexico, USA - June 27-30, 2011 (pp. 341-345).

[10] Benkler, Y. (1997). Overcoming Agoraphobia: Building the Commons of the Digitally Networked Environment. Harvard Journal of Law and Technology, 11(2), 287-400.

[11] Andrew Carline , Mohammad Hammoudehb , Omar Aldabbasc" Defence for Distributed Denial of Service Attacks in Cloud Computing" vol 1877-0509 © 2015

[12] Mariam Kiran; "A Methodology for Cloud Security Risks Management". Springer International Publishing Switzerland 2014.

[13] Saeed Shafieian, Mohammad Zulkernine and Anwar Haque; "Attacks in Public Clouds: Can They Hinder the Rise of the Cloud"? Springer International Publishing Switzerland 2014.

[14] Mazhar Ali a,c,*, Samee U. Khan a, Athanasios V. Vasilakos b; "Security in cloud computing: Opportunities and challenges".

[15] Moussa Ouedraogo1*, Severine Mignon1, Herve Cholez1, Steven Furnell2 and Eric Dubois1 "Security transparency: the next frontier for security research in the cloud".

[16] Munir, K., Palaniappan, S.: Security threats/attacks present in cloud environment. IJCSNS 12(12) (2012).

[17] Frederick R. Carlson "Security Analysis of Cloud Computing" Frederick R, Carlson 352-586-2621.

[18] Cloud Security Alliance, (2011). Top threats to cloud computing v1.0.

[19] Rizwana Shaikha, Dr. M. Sasikumarb "Data Classification for achieving Security in cloud computing".

[20] 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.

[21] 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.

[22] Owens D (2010) Securing elasticity in the Cloud. Commune ACM 53(6):46–51.

[23] OWASP (2010) The Ten most critical Web application Security risks.

[24] 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.

[25] Subashini S, Kavitha V (2011) A survey on Security issues in service delivery models of Cloud Computing. J Newt Compute Apply 34(1):1–11.

[26] Cloud Security Alliance (2012) Security guidance for critical areas of Mobile Computing.

[27] Keene C (2009) The Keene View on Cloud Computing. Online Available: Accessed: 16-Jul-2011.

[28] Xen K, Zhang X, Song M, Song J (2009) Mobile Mashups: Architecture, Challenges and Suggestions. In: International Conference on Management and Service Science. MASS'09. IEEE Computer Society, Washington, DC, USA, pp 1–4.

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

[30] Jaeger T, Schiff man J (2010) Outlook: cloudy with a chance of Security challenges and improvements. IEEE Security Privacy 8(1):77–80.

[31] 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.

[32] 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.

[33] Hashizume K, Yoshioka N, Fernandez EB (013) 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.

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

[35] Wang Z, Jiang X (2010) Hyper Safe: 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.

[36] Tebaa M, El Hajji S, El Ghazi A (2012) Homomorphism encryption method applied to Cloud Computing. In: National Days of Network Security and Systems (JNS2). IEEE Computer Society, Washington, DC, USA, pp 86–89.

[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, USA, pp 9–18.

[38] Cloud Security Alliance (2012) Secaas implementation guidance, category 1: identity and Access management. initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf

[39] 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.