STUDENT PERSONAL WORK

Topic: Cloud security issues and challenges

ABDOUL AZIZ HAMAYADJI	M1SLED	15A773FS
KANMOGNE WABO LEOENL	M1SLED	13A042FS

Teacher: Dr-ing Tchakounte Franklin

University of NGAOUNDERE
Systems and Networks security

1 – INTRODUCTION

The document is a survey that was made by **Ashish Singh** and **Kakali Chatterjee** exactly on cloud security issues and challenges. The last manuscript of this work was accepted the 27 November 2016 and appear in *Journal of Network and Computer Applications*.

Context: The scientific computing in the 21st century has evolved from the centralized infrastructure to distributed environment, where the two well-known components are clusters and grids both are different approaches. Nowadays the current trend of cloud computing allows accessing business applications and services from anywhere just by connecting to the internet. Day by day cloud computing is in growth as many organizations and industry adopted the cloud technology, but parallel several security issues are raised. These security issues come with challenges that are not generally known by the end users or organizations which request cloud' services. Cloud computing provides on demand services over the internet with the help of a large amount of virtual storage. The cloud used virtual environment to attain multi-tenancy. The cloud computing paradigms aimed is providing a huge amount of computing power in a completely virtualized manner, by combining all computing resources and services in a single system. Also, when data is stored in the remote storage, user looses the control over the data, at this time consumers may not be conscious the details security policies, vulnerability and malware information. Therefore, user has no idea about where its data is stored and if someone else can access those data; this situation lead to security issues and challenges in the cloud computing. In this purpose, the National Institute of Standards and Technology (NIST) has identify that security, portability and interoperability are the major obstacle to adoption of cloud computing. And according to the survey made in 2009, many firm give their opinions most about security issues; the International Data Corporation (IDC) analyzed firm's gives and the survey results clearly say that **87,5%** of the survey notice that **the security field as a top priority**.

Background: for this work, it is needed to have notions about some concepts like cloud computing; security that describes set of policies, technology, and control that is helpful to protect the data and services; virtualization; network; web protocols; cloud framework; web technologies, cloud role and boundaries.

Problem and question research: The main features of the cloud computing is that the user does not have any setup of expensive computing infrastructures and **the cost of its services is less**. To achieve the high level security and privacy of related data and services, cloud service provider settles a Service Level Agreement (SLA) to the cloud consumers. The problem is that many cloud providers as **Google, Amazon**, and **SalesForce** does not give full Service Level Agreement to guarantee that its user data is fully secure and it hides many others parameters related to the service. The research question are: what is the different basic components of cloud computing? Which kind of technology is needed in cloud computing? What are the different threats which emerge according to those technology and services provided?

The survey on Cloud Security issues and Challenges provide a comprehensive study of different security issues and its solutions. And also extend discussion to cloud security threats, the attacks after, propose some solutions.

2 – RLATED WORK

For produce this survey, the authors use not least than 198 various documents. But this table present the main and the comparison of the related work with the survey based on the cloud overview, cloud automation, security requirements, cloud trust, cloud security (attacks, threats and abstraction), cloud security issues, security solution and open issues.

Survey paper	**Year**	**Topic discussed**	**Cloud overview**	**Cloud automation**	**Security Requirements**	**Cloud trust**	**Cloud security (abstraction, Threats and attacks)**	**Cloud security issues**	**Security solutions**	**Open issues**
Takabi et al. [159]	2010	Virtualization, trust management, secure service management, security & privacy	less	no	no	yes	less	less	no	no
Zhou et al. [196]	2010	Security requirements (availability, confidentiality, integrity, control, and audit), privacy	less	no	yes	no	no	no	no	no
Grobauer et al. [59]	2011	Cloud specific vulnerability, cloud risk, authentication, authorization, and access control	less	less	less	no	no	less	no	no
Vaquero et al. [171]	2011	IaaS cloud security, cloud threats and attacks, VMM security	no	no	no	less	yes	less	less	no
Behl [24]	2011	Cloud security issues, cloud security challenges	less	no	no	no	no	less	no	yes
Zissis et al. [198]	2012	Cloud trust, cryptographic method for security, security requirements, trusted third party authentication, certification based authorization	less	no	yes	yes	less	no	no	no

Modi et al. [107]	2013	Cloud threats and attacks, security issues at different layer, authentication and virtualization security issues	no	no	yes	yes	yes	less	less	yes
Oktay et al. [115]	2013	Cloud security attacks, Intrusion detection system, intrusion prevention system	yes	no	no	no	yes	no	no	no
Fernandes et al. [49]	2014	Cloud concept and technologies, cloud security issues	yes	yes	yes	yes	no	yes	no	yes
Abbas et al. [1]	2014	Cloud security requirements, privacy persevering approaches, open research issues in E-health cloud	no	no	yes	no	no	no	no	yes
Ali et al. [6]	2015	Cloud computing overview, cloud security issues, cloud security solutions, security issues in mobile cloud computing	yes	no	no	less	less	less	less	yes
Tari et al. [163]	2015	Security issues present in public and private clouds, service availability, access control, multitenant services, identity and data protection	no	no	no	no	less	less	less	no
This survey	2016	Cloud overview, cloud technologies, cloud security requirements, cloud trust, Cloud security (abstraction, threats & attacks), cloud security issues and their solutions, future research directions	yes	yes	yes	yes	yes	yes	yes	yes

3 – METHOLOGY EMPLOYED

The authors of“*cloud security issues and challenges: A survey*”. At the first time present the **cloud computing architectural framework**; in this part they present all essential characteristics of cloud computing as *On-demand self service, Broad network access, Resource pooling, Rapid elasticity and Measured service*; through *Service models*. After that authors move to Deployment model where we have *Private cloud, Public cloud, Community cloud* and *Hybrid cloud;* after they present different Storage models. The figure1 bellows resume the cloud computing architectural framework.

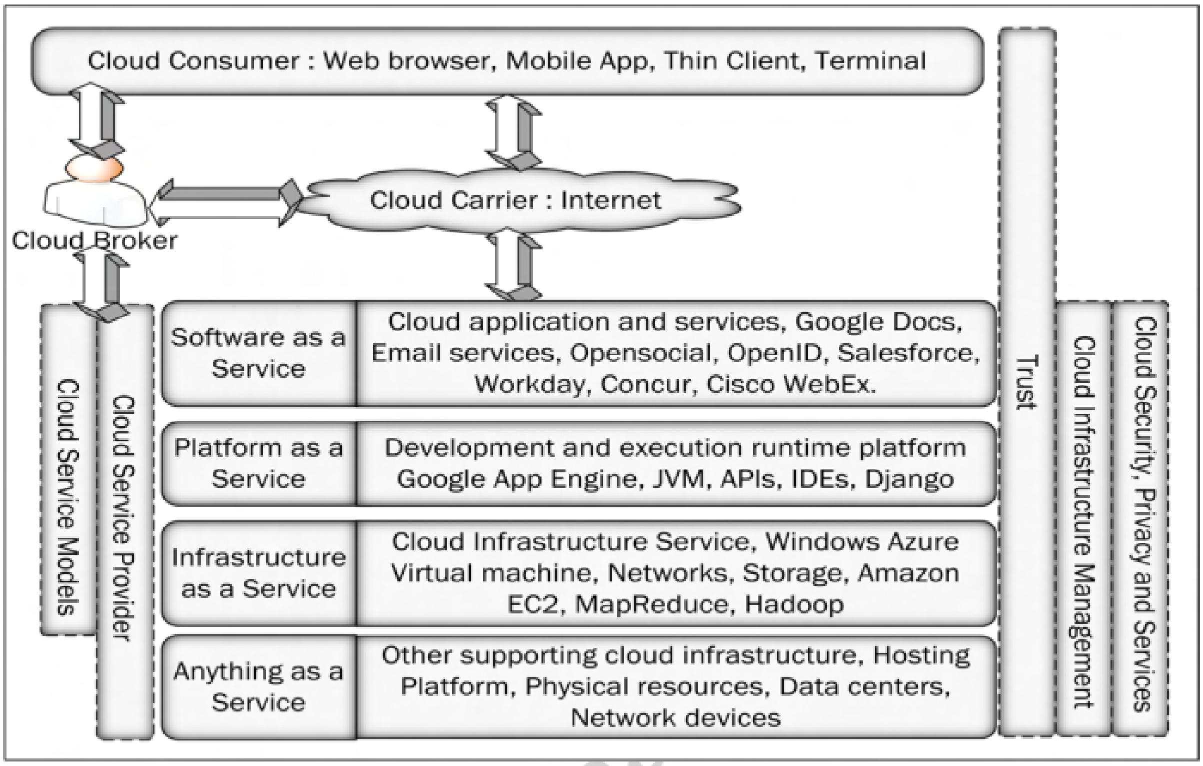
Cloud Consumer : Web browser, Mobile App, Thin Client, Terminal
Cloud Carrier : Internet
Cloud Broker
Cloud Service Models
Cloud Service Provider
Software as a Service
Cloud application and services, Google Docs, Email services, Opensocial, OpenID, Salesforce, Workday, Concur, Cisco WebEx.
Platform as a Service
Development and execution runtime platform Google App Engine, JVM, APIs, IDEs, Django
Infrastructure as a Service
Cloud Infrastructure Service, Windows Azure Virtual machine, Networks, Storage, Amazon EC2, MapReduce, Hadoop
Anything as a Service
Other supporting cloud infrastructure, Hosting Platform, Physical resources, Data centers, Network devices
Trust
Cloud Infrastructure Management
Cloud Security, Privacy and Services

Fig. 1. A complete cloud computing architectural framework

At the end with cloud computing architectural framework part, the authors present the cloud role and boundaries, where each participant role, responsibilities and how their interact; then we have: *cloud provider, cloud consumer, cloud service owner, cloud resource administrator, organizational boundary, trust boundary, cloud auditor, cloud broker*, and *cloud carrier*. After this first section on cloud computing architectural framework, the authors move to cloud technology.

The second point is **cloud technology**, within this part, authors present some technology as: *Broadband network and internet technology* which reveal the dependency on internet; we have also in this level: *data center technology, web technology, multi-tenant technology* among other, and the biggest technology which is **virtualization** that make cloud computing possible. The virtualization is a conversion process that translates physical IT resources into a virtual IT resources. The IT resources include servers, storage, network and power. Also, the virtualization is created by two types: operating system based virtualization and hardware based virtualization.

The third point in the authors' methodology is **cloud security**, with the next section which threats the cloud security issues represent the heart of survey.

Concerning the cloud security, which is a part of computer security, it describes set of policies, technology, and control that is helpful to protect the data and services. Within this section, the authors present some security concepts as **threats agent** that is an entity that creates a threat called the threat agents, capable to tackle an attack; **Security controls** are countermeasure used to reduce or avoid risk; **Security policy** is a mechanism to establish set of security rules and regulations and the cloud security service is a complex service, technique, regulation and behavior that is composed to protect IT assets. Inside this part of the survey, after cloud security concepts authors also deal with: *treats, requirements, attacks and Data center security*.

The next point was **cloud security issues**, where authors threat all different issues as: Data storage and computing security issues with concepts like *Data storage, Cryptography, Data and Service availability, and Data backup* among other. After that we have **Virtualization security issues** which is the reason of wide adoption of cloud computing in industry, concepts like: *virtual machine monitor, Virtual machines image management and network virtualization*; the authors move from there to **internet and service related security issues**, **network security issues**, **Access control issues**, **Software security issues**, and **Trust management issues** which is a non-measurable parameter in cloud computing. Because trust plays an important role for any system. The end point in this part is **Compliance and legal security issues**, within the SLA is a document plays an important role in the cloud business model. It contains an agreement between the two communicating parties, all service related information, and terms and conditions of the service.

The last step in the methodology way **Discussion and Open research issues**, where authors give some ideas and topics for future survey.

4 – RESULT FOUND AND PERSPECTIVES

These two tables show the results found about cloud security issues and challenges according to the survey.

Table A: A comprehensive study on cloud threats described by the CSA in 2013 and its solutions

Threats	**Effects**	**Affected cloud services**	**Solutions**
Different service delivery/receiving model	Loss of control over the infrastructure of the cloud	PaaS, SaaS, and IaaS	Offered services under the control and monitored
Abusive use of cloud Computing	Loss of validation, service fraud, stronger attack due to unidentified signup	PaaS and IaaS	Observe the network status, provide robust registration and authentication technique
Insecure interface and API	Improper authentication and authorization, wrong	PaaS, SaaS, and IaaS	Data transmission is in encrypted form, strong access control and authentication mechanism.

	transmission of the content		
Malicious insiders	Penetrate organizations resources, damage assets, loss of productivity, affect an operation	PaaS, SaaS, and IaaS	Use agreement reporting and breach notifications, security and management process is transparent
Shared technology Issues	Interfere one user services to other user services by compromising hypervisor	IaaS	Audit configuration and vulnerability, for administrative task use strong authentication and access control mechanisms
Data loss and leakage	Personal sensitive data can be deleted, destructed, corrupted or modified	PaaS, SaaS, and IaaS	Provide data storage and backup mechanisms
Service/Account Hijacking	Stolen user account credentials, access the critical area of the cloud, allowing the attacker to compromise the security of the services	PaaS, SaaS, and IaaS	Adoption of strong authentication mechanisms, security policies, and secure communication channel
Risk profiling	Internal security operations, security policies, configuration breach, patching, auditing and logging	PaaS, SaaS, and IaaS	Acknowledge partial logs, data and infrastructure aspect, to secure data use monitoring and altering system
Identity theft	An aggressor can get identity of a valid user to access that user resources and take credits or other benefits in that user name	PaaS, SaaS, and IaaS	Use strong multi-tier passwords and authentication mechanisms

Table B: A comprehensive study on cloud attacks and solutions

Attacks	**Attack surface/procedure**	**Affected cloud services**	**Effects**	**Solutions**
Zombie attack (DoS/DDoS attack)	Direct/indirect SYN packet flooding to host, attack on VM, attack on hypervisor, network based attack.	SaaS, PaaS, and IaaS	Service availability affected, may be create a fake service.	Strong authentication and authorization
Service injection attack	Distractive service entering through accessing service identification files, application and VM level attack.	PaaS	Service integrity distressed, Malicious service provided to users instead of valid service	Strong isolation mechanisms be-tween VMs, use hash function to check service integrity, Web service security, adopt secure web browsers and API
Attack on virtualization/hypervisor	Settlement with the hypervisor, breakout Virtual layer. VM and hypervisor level Attack.	IaaS	Access the credentials and control to another user	Need a hypervisor security solutions, monitor hypervisor

				activities, VM isolation required
User to root attacks	Accessing the whole resources of a valid user. User level attack.	SaaS	Affect the privacy of user's sensitive information and services	Use strong password, better authentication mechanism
Port scanning	Scan the open port and gain information about open port.	IaaS, SaaS, and PaaS	Abnormal behavior of the service, affect service availability	Required strong port security
Man-in-middle attack	Modify service information file such as WSDL. Service level attack two individual.	SaaS, PaaS, and IaaS	Penetrate the data privacy and security	Required a proper secure Secure Socket Layer (SSL) architecture
Metadata spoofing attack	Modify service information file such as WSDL. Service level attack.	SaaS and PaaS	Abnormal behavior of the service, affect privacy of the service	Service functionality and other details should be kept in encrypted form, to access the file required a strong authentication mechanism
Phishing attack	By accessing a fake web link.	SaaS, PaaS, and IaaS	Affect the privacy of the user credentials that should not be revealed	Use secure web link (HTTPS)
Backdoor channel attack	Settlement with the valid user VMs, VM and hypervisor level attack.	IaaS	Affect the service availability and data privacy, provides rights for gaining valid user's resources	Required strong authentication, authentication and isolation mechanisms

Many security vulnerabilities are present at the browser Application Program Interface (API) and in the network channel.

SOME PERSPECTIVES

In a cloud computing environment, several services and resources are available, but security level of the resources depends upon the sensitivity and value level of the resource. The first and more important open issue is to **design an extensive and integrated security solution** that may fulfill all major security requirements in the cloud. **The privacy of the computation** is another open issue in cloud computing. In these phenomena **identification of the insider attack in cloud computing** is an open area of research. Similarly, another open issue is to **identify who is the normal user and who is the malicious user**, still have a problem in a cloud environment.

5 – MOST IMPORTANT PUBLICATIONS FOR THIS WORK

[3] Ahuja SP, Komathukattil D. A survey of the state of cloud security. Network and Communication Technologies. 2012 Nov 20;1(2): pp.66-75.

[7] Almorsy M, Grundy J, Mller I. An analysis of the cloud computing security problem. InProceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010 Nov.

[47] ENISA: Cloud Computing: Benefits, Risks and Recommendations for Information Security. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computingrisk-assessment(2009). Accessed August 2015.

[59] Grobauer B, Walloschek T, Stcker E. Understanding cloud computing vulnerabilities. Security & privacy, IEEE. 2011 Mar;9(2): pp. 50-57

[153] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications. 2011 Jan 31;34(1): pp. 1-11.

[166] Taylor M, Haggerty J, Gresty D, Lamb D. Forensic investigation of cloud computing systems. Network Security. 2011 Mar 31;2011(3): pp. 4-10.

[169] Tripathi A, Mishra A. Cloud computing security considerations. InSignal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on 2011 Sep 14 (pp. 1-5). IEEE

[171] Vaquero LM, Rodero-Merino L, Morn D. Locking the sky: a survey on IaaS cloud security. Computing. 2011 Jan 1;91(1): pp. 93-118.

[196] Zhou M, Zhang R, Xie W, Qian W, Zhou A. Security and privacy in cloud computing: A survey. InSemantics Knowledge and Grid (SKG), 2010 Sixth International Conference on 2010 Nov 1 (pp. 105-112). IEEE.