Cloud security issues and challenges: a survey

1 Introduction

1.1 Context

Our article is written in the framework of: "Cloud security issues and challenges: a survey", edited by: Ashish Singh, Kakali Chatterjee in 2016 whose link is http://dx.doi.org/10.1016/j.jnca. 2016.11.027. It is always in the perspective of finding or improving the solutions relating to the security of the cloud that this article has been drafted. This document discusses the basic characteristics of cloud computing, security issues, threats and their solutions. Additionally, the paper describes several key topics related to the cloud, namely cloud architecture framework, service and deployment model, cloud technologies, cloud security concepts, threats, and attacks.

1.2 Background

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand.
Computer **security**, also known as cybersecurity or **IT security**, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide.
Cloud computing security or, more simply, **cloud security** refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security computer security, network security, and, more broadly, information security.

Research questions
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.

Comparison of the related work with the survey based on the cloud overview, cloud automation, security requirements, cloud trust, Cloud security (abstraction, threats & attacks), Cloud security issues, Security solutions, and Open issues.

Survey paper	Year	Topic discussed	Cloud overview	Cloud automation	Security requirments	Cloud trust	Cloud security	Cloud security issues	Security solutions	Opens issues
Takabi et al. [159]	2010	Virtualization, trust management, secure service management, security & privacy	-	X	X	O	-	-	X	X
Zhou et al. [196]	2010	Security requirements (availability, confidentiality, integrity, control, and audit), privacy	-	X	O	X	X	X	X	X
Grobauer et al. [59]	2011	Cloud specific vulnerability, cloud risk, authentication, authorization, and access control	-	-	X	X	-	-	X	X
Vaquero et al.[171]	2011	IaaS cloud security, cloud threats and attacks, VMM security	X	X	X	-	O	-	-	X
Behl [24]	2011	Cloud security issues, cloud security challenges	-	X	X	X	X	-	X	O
Zissis et al. [198]	2012	Cloud trust, cryptographic method for security, security requirements, trusted third party authentication, certification based authorization	-	X	O	O	-	X	X	X
Modi et al. [107]	2013	Cloud threats and attacks, security issues at different layer, authentication and virtualization security issues	X	X	O	O	O	-	-	O
Oktay et al. [115]	2013	Cloud security attacks, Intrusion detection system, intrusion prevention system	O	X	X	X	O	X	X	X

Fernandes et al. [49]	2014	Cloud concept and technologies, cloud security issues	O	O	O	O	X	O	X	O
Abbas et al. [1]	2014	Cloud security requirements, privacy persevering approaches, open research issues in E-health cloud	X	X	O	X	X	X	X	O
Ali et al. [6]	2015	Cloud computing overview, cloud security issues, cloud security solutions, security issues in mobile cloud computing	O	X	X	-	-	-	-	O
Tari et al. [163]	2015	Security issues present in public and private clouds, service availability, access control, multi-tenant services, identity and data protection	X	X	X	X	-	-	-	X
This survey		Cloud overview, cloud technologies, cloud security requirements, cloud trust, Cloud security (abstraction, threats & attacks), cloud security issues and their solutions, future research directions	O	O	O	O	O	O	O	O

The "-" symbol denote the less discussion on respective aspect. The " O" and "X" symbol denote the specific domain is covered and domain is not covered with respect to given aspect respectively.

3. Methodology employed

The methodology employed in this article is presented as we will give below:

- **Title of article**: That present the domain study by author who is survey in cloud security issues and challenges.

- **Abstract**: he present what is the cloud computing and of what this article speak (the basic

features of the cloud computing, security issues, threats and their solutions), additionally, the paper describes several key topics related to the cloud, namely cloud architecture framework, service and deployment model, cloud technologies, cloud security concepts, threats, and attacks.

- **Introduction:** the introduction explain the evolution of computer science: the begin for arrive to nowadays with introduction the cloud computing concepts in present above two well known components for a distributed system are clusters and grids. At the end we have the work plan.

- **Presentation of the related work and elaborates the contribution of many other papers**: In this part, the author present the related work in the table and specify problems related to the different areas of cloud computing that each author points out.

- **A general view of cloud computing and some general models related to cloud:** The author present several essential characteristics, service models, deployment models, storage models and cloud rôle and boundaries:
    - Essential characteristics
    - Service models
    - Deployment models
    - Storage models
    - Cloud rôle and boundaries

- P**resentation of detail study of cloud technologies:** In this section, the author define technologies that help to understand how these technologies are deployed over cloud infrastructure. We have as technologies:
    - Broadband network and Internet technology.explore several security
    - concepts, which will help to better understand the cloud security issues.b
    - Data center technology;
    - Virtualization technology;
    - Web technology;
    - Multi-tenant technology;
    - Service technology;

- **Presentation of cloud security (** *concepts, requirements, threats, attacks, data center*): exploration several security concepts, which will help to better understand the cloud security issues. Here he explain different concepts,

- **Presentation of cloud security issues (***Data storage and computing security issues, Virtualization security issues, Internet and services related security issues, Network security issues, Access control issues, Software security issues, Trust management issues and Compliance and legal security issues***):**In this section, work is mainly focusing on several categorized security issues and their solutions. First, the work presents a brief introduction about security issue in cloud computing then presents their solutions. Each step is well developped and have equaly one table that regroup all the problems and solutions.

- **Presentation of Discussion and open issues:** Author give different problems present at the beginning of cloud computing and propose the solutions.

- **Conclusion:** In this part author show the important of cloud computing and shows also that using the cloud requires much more vigilance to preserve important data.

- **Refrence:** All refrences of documents used by author for write this article.

3.Results found and perspectives

➔ Results found

Data is very important in cloud computing. The principle of cloud computing is that the data owner does not aware the locality of the cloud storage center, security services and security mechanisms used for securing the cloud data, it's why their data are exposed and vulnerable. But we can have many solutions for evade these threats or attacks. We can underligned these solutions for resolve the threats and attacks problems. We have as solutions:

A comprehensive study on data storage and computing security issues and solutions

Security topic	Security issues	Studies/survey	Security solutions
Data storage	Remote data storage Loss of control Data pooling, data locality Multi-location Complex model for integrity checking	[155] [185] [144] [185] [196] [153]	better security scheme for resident data [150] File Assured Deletion (FADE) scheme for data security [162] SecCloud protocol for secure storage [182]
Un-trusted computing	Top down SLAs Malicious users, downtimes, slowdowns Dishonest computing, root level error in backups, migration and restoring problem Weak security solutions for computing models	[66] [189] [185] [138]	A non-interactive solution [53] A lightweight and low-cost solution for e-banking [96]
Data and service availability	Counterfeit resource usage Cloud interruption Hardware availability issue (hardware fault)	- [3] [14] [133]	A solution for data availability [173] Proxy re-encryption scheme based on time-based [98]
Cryptography	Insecure cryptography mechanism, poor key management faulty cryptography algorithms Brute force and Dictionary attack	[59] [193] [150] [167]	Order-preserving encryption [27] Cryptography in cloud computing [75]

A comprehensive study on virtualization security issues and solutions

Security topic	Security issues	Studies/survey	Security solutions
VMs image management	Cryptographic overhead due to large size images VMs theft and malicious code injection Overlooked image repository Virtual machine transience, infected VMs Virtual machine sprawl	[171] [7] [181] [181] [100]	A VM image management system [181] VM image privacy and integrity [86]
Virtual machine monitor	Hypervisor failure, single point od failure, untrusted VMM components, transparency of VMM, lack of monitor GUI, VMM separation, inspection, and interposition VM escape VM diversity , Load balancing in VMM VMM zero day vulnerabilities	[124] [153] [59] [171] [161]	HyperCheck [175] DeHype [183] HyperLock [179] SplitVisor [122] NoHype [158]
Network virtualization	Twofold traffic, limited network access, inapplicability of standard security mechanisms Effectiveness of network security devices in virtual network Dynamic network property Packet sniffing and spoofing Virtual devices software exposure Virtualized communication medium	[59] [59] [171] [174] [124] [7] [127]	Virtual network security [99] [93] [184] [68]

A comprehensive study on Internet and service related security issues and solutions

Security topic	Security issues	Studies/survey	Security solutions
Advanced repeated threats and venomous outsiders	Information collection, scan publicly available information Doxing Data exfiltration, cyber activity	[149] [56] [101]	Property hidden Strong privacy laws
Internet protocols	Susceptible communication protocols, network-based cross-tenant attacks Session hijacking Mixed HTTP and HTTPS data streams Weak cryptographic key usages Cookie theft, cookie poisoning, impersonation attacks TLS attack, cookie theft	[7] [121] [59] [71] [71] [128] [67] [121] [5] [103]	Use Secure Flag for security of the cookies OpenSSL [190] Network Security Services (NSS) [146] Secure the server operators private keys Use secure HTTP protocol [28]
Web services	HTTP stateless protocol, API transaction support for integrity Metadata spoofing attacks, improper WSDL documents XML injection, SOAP wrapping attacks Incorrect inspection WSDL documents	[153] [77] [80] [136] [77] [43] [77]	Signed SAML assertions XML Encryption [141] XML Signature [141] Encoding of binary tokens [32]

A comprehensive study on network security issues and solutions

Security topic	Security issues	Studies/survey	Security solutions
Mobile platforms	Generation of mobile malware Extension of mobile vulnerabilities Rooting and jailbreaking, rootkits, openness of privilege Cloud syncing mobile applications vulnerabilities	[38] [69] [95] - [58]	Intrusion detection system to protect mobile platforms [191] Mobile security [95]
Circumference security	Immobile network infrastructure Open network perimeter DMZ assumption Firewalls limitation, limited mobile connection VMM network sniffing and spoofing Security threats in logging, insufficient monitoring system	- - [146] [130] [59]	Network security for virtual machine Cloud network security using tree-rule firewall [68] Security for dynamic cloud network [146]

A comprehensive study on access control issues and solutions

Security topic	Security issues	Studies/survey	Security solutions
Physical access	Malicious insiders Malicious system admin Cold boot attack, hardware tempering	[193] [197] [82] [140] [69]	Use eXtensible Access Control Markup Language (XACML) expressing access policies Secure data access [139]
User credentials	Load on IT management, LDAP and AD servers location Weak credential reset methods Phishing attack, key-logger attack, man-in-the-middle attack, replay attack, sessions hijacking, User to root attack	[153] [59] [24] [108]	Attribute based encryption [178] Use Heirarchical Attribute Set Based Encryption [178]
Entity authentication	Archaic static password Inapplicability of alternative password schemes SAML explosure XML SAML wrapping attacks QA explosure Account lockout	[64] [41] [20] [20] [148] [60] [59]	Hierarchy identity based cryptography ID management framework Decentralized access control for cloud storage SMS based password recovery

➔ Perspectives

The prospects are many in this area of security. Despite the number of solutions available, we are still wary of the security threats of our data. To this end, we have highlighted several points to be developed, namely:

- Design a comprehensive and integrated security solution that can meet all major security requirements in the cloud.
- A common and more integrated security solution is more secure and easier to implement in security tools than the use and arrangement of several security solutions.
- Ensure confidentiality during computation time.
- Insurance and verification tool to ensure better identity management and access control system.
- Confidentiality during the calculation time.
- For migration, it is necessary to have a standard protocol and standard formats that support the cloud format and help the client migrate its data and applications to other clouds.
- As part of the attacks initiated, it is necessary to develop an indicator that helps to find the internal attacks. This indicator will increase the security potential of the cloud system.

4. Most important publication for this work

- 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.
- Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M. A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing. 2013 Feb 1;63(2): pp. 561-592.
- Fernandes DA, Soares LF, Gomes JV, Freire MM, Incio PR. Security issues in cloud environments: a survey. International Journal of Information Security. 2014 Apr 1;13(2): pp. 113-170.
- Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information Sciences. 2015 Jun 1;305: pp.357-383
- Grobauer B, Walloschek T, Stcker E. Understanding cloud computing vulnerabilities. Security & privacy, IEEE. 2011 Mar; 9(2): pp. 50-57
- Takabi H., Joshi J. B., and Ahn G.-J. Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 2010; no. 6, pp. 24-31.
- Jensen M, Gruschka N, Herkenhner R. A survey of attacks on web services. Computer Science-Research and Development. 2009 Nov 1;24(4): pp. 185-197.
- Tang Y, Lee PP, Lui J, Perlman R. Secure overlay cloud storage with access control and assured deletion. Dependable and Secure Computing, IEEE Transactions on. 2012 Nov;9(6): pp. 903-916.

Refrences:

- Cloud Computing et Sécurité : Approches et Solutions. Al Haddad Zayed 1 , Hanoune Mostafa 2 , Mamouni Abdelaziz 3 *International Journal of Computer Trends and Technology (IJCTT) – volume 30 Number 1 – December 2015.*
- *https://en.wikipedia.org/wiki/Cloud_computing_security*