Volume 5, Issue 4, April 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cloud Computing Security: An Issue of Concern

Prof. A. P. Bodkhe
Professor
Prof. Ram Meghe Instt. of Tech. & Research
Badnera- Amravati, Maharashtra, India

Dr. C. A. Dhote
System Manager
Prof. Ram Meghe Instt. of Tech. & Research
Badnera-Amravati, Maharashtra, India

Abstract: ***Cloud computing is an emerging technology exemplar that migrate current technological and computing concepts into utility-like solutions. Cloud computing as a ubiquitous on-demand model for accessing common resources over a network. The main idea of cloud computing is to deliver both software and hardware as services. Clouds bring out a wide range of benefits including configurable computing resources, economic savings, and service flexibility. However, security and privacy concerns are shown to be the issues of great concern to a wide adoption of clouds. The new concepts that clouds introduce, such as multi-tenancy, resource sharing and outsourcing, create new challenges to the security community. Addressing these challenges requires, in addition to the ability to grow and tune the security measures developed for traditional computing systems, proposing new security policies, models, and protocols to address the unique cloud security challenges. In this paper, we provide a comprehensive study of cloud computing security and privacy concerns. We identify cloud vulnerabilities, classify known security threats and attacks, and present the state-of-the-art practices to control the vulnerabilities, neutralize the threats, and calibrate the attacks. Additionally, we investigate and identify the limitations of the current solutions and provide insights of the future security perspectives.***

Keywords: cloud computing; cloud security; security vulnerabilities; threats; attacks.

I. INTRODUCTION

Cloud computing provides a centralized pool of configurable computing resources and computing outsourcing mechanisms that enable different computing services to different people in a way similar to utility-based systems. Cloud computing does not have a common accepted definition [1]. The National Institute of Standards and Technology (NIST) [2] defined five essential characteristics of cloud computing, namely: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. Also, cloud computing is described as a dynamic and often easily extended platform to provide transparent virtualized resources to users through the Internet [3]. Cloud computing architecture consists of three layers: (i) Software as a service (SaaS); (ii) Platform as a service (PaaS) and (iii) Infrastructure as a service (IaaS) [4]. The clouds are also viewed as five component architectures that comprise clients, applications, platforms, infrastructure and servers [5]. The current clouds are deployed in one of four deployment models: (a) public clouds in which the physical infrastructure is owned and managed by the service provider; (b) community clouds in which the physical infrastructure is owned and managed by a consortium of organizations; (c) private clouds in which the infrastructure is owned and managed by a specific organization and (d) hybrid clouds which include combinations of the previous three models [6].

Figure 1 shows cloud deployment models together with their internal infrastructure (IaaS, PaaS and SaaS). Cloud deployment models have similar internal infrastructure, but vary in their policies and user-access levels.

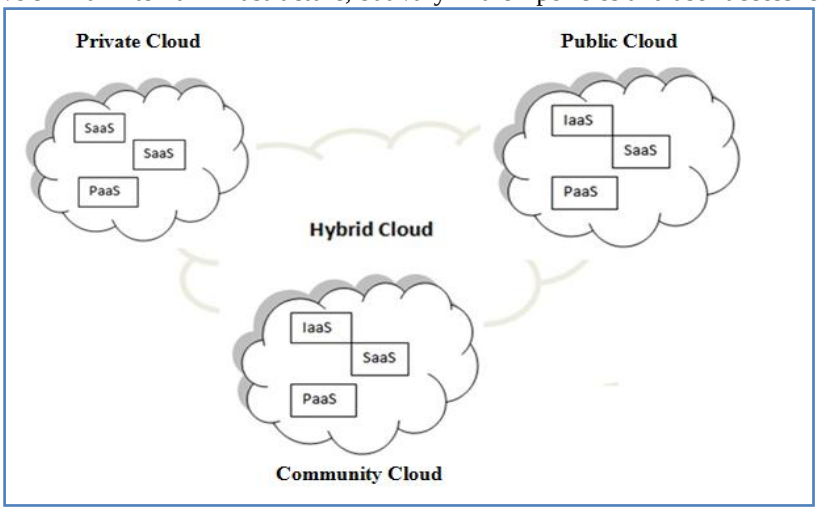

Figure1. Cloud deployment models and infrastructure

II. RELATED WORK

Many researchers and practitioners work on identifying cloud threats, vulnerabilities, attacks, and other security and privacy issues, in addition to providing countermeasures in the form of frameworks, strategies, recommendations, and service oriented architectures. Additionally, efforts in other domains such as ad hoc networks have been tuned to address the emerging security problems in the clouds [7-12]). Many researchers [13–19] have addressed single attributes of cloud computing security such as data integrity, authentication vulnerabilities, auditing, *etc*. Others provide surveys that cover specific areas of cloud security concerns and proposed solutions. The researchers briefly and broadly discuss cloud security issues involving data, applications and virtualization. The authors in [10] discuss similar cloud security issues but with deeper investigations. In [17, 19], the authors present surveys on cloud security requirements such as confidentiality, integrity, transparency, availability, accountability, and assurance. In [18], the authors present a survey on the different security issues of the service delivery models of the clouds. In [20], the authors discuss the security challenges specific to the public clouds. In [21], Hashizume *et al*. classify the security issues in the cloud based on the SPI (SaaS, PaaS, IaaS) cloud infrastructure and services model. Additionally, the authors explain fundamental security concepts including vulnerabilities, threats, and attacks and provide mapping among these concepts. In [22], Zissis *et al*. evaluate cloud security requirements. They propose a Trusted Third Party solution that calls upon cryptography to ensure the authentication, integrity and confidentiality of data and communications. In [23], Whaiduzzaman *et al*. present key management and broad aspects of privacy and security issues in the domain of vehicular cloud computing.

Specifically, we need to: (i) investigate various cloud security attributes including vulnerabilities, threats, risks, and attack models; (ii) identify the security requirements including confidentiality, integrity, availability, transparency, *etc*.; (iii) identify the involved parties (clients, service provides, outsiders, insiders) and the role of each party in the attack-defense cycle; and (iv) understand the impact of security on various cloud deployment models (public, community, private, hybrid).

Cloud Security Categories: We classify cloud computing security related issues into the following five categories, which are also summarized in Table 1.

Table 1. Cloud Security Categories

Number	Category	Details
C#1	Security Standards	Defines the standards required to take preventive measures in cloud computing in order to avoid attacks. It governs the policies of cloud computing for security without compromising reliability and performance
C#2	Network	Includes network attacks such as Connection Availability, Denial of Service, flooding attack, internet protocol vulnerabilities, *etc*.
C#3	Access Control	Encompasses authentication and access control. It captures issues that affect privacy of user information and data storage.
C#4	Cloud Infrastructure	Covers attacks that are specific to the cloud infrastructure (IaaS, PaaS and SaaS) such tampered binaries and privileged insiders.
C#5	Data	Encompasses data related security issues including data migration, integrity, confidentiality, and data warehousing.

Network category (C#2) related issues are deemed to be the biggest security challenges in clouds since cloud computing is more prone to network related attacks compared to the traditional computing paradigms [2]. In addition, cloud operations are tightly coupled and highly depend on networking. Therefore, cloud network security issues receive more attention in this work compared to the other security categories. The ratio of network attacks and fraud dramatically increases as people and organizations migrates their data into clouds.

A single customer may access data and compose services from multiple cloud providers using a mobile application or a browser. This kind of access brings in an inherent level of risk and this risk has been called privileged user access [6]. Unauthorized access becomes possible through browser vulnerabilities. Therefore, Internet browser is the first stage where security measures should be considered because vulnerabilities in the browser open the door for many follow-on attacks.

The insecure interface of Application Programming Interface (API) issue covers the vulnerabilities in the set of APIs in the cloud portal (customers use these APIs to connect to a cloud) which can expose an organization to several threats such as unauthorized access, content transmission, reusable token and logging capabilities [1]. Quality of service (QoS) is an unattended issue [24] because many cloud service providers focus only on fast performance and low cost [25].

Table 2. Cloud Security Issues and Classifications

Category	Tag	Issues
Security Standards	T1	Lack of security standards
	T2	Compliance risks
	T3	Lack of auditing
	T4	Lack of legal aspects (Service level agreement)

	T5	Trust
Network	T6	Proper installation of network firewalls
	T7	Network security configurations
	T8	Internet protocol vulnerabilities
	T9	Internet Dependence
Access	T10	Account and service hijacking
	T11	Malicious insiders
	T12	Authentication mechanism
	T13	Privileged user access
	T14	Browser Security
Cloud Infrastructure	T15	Insecure interface of API
	T16	Quality of service
	T17	Sharing technical flaws
	T18	Reliability of Suppliers
	T19	Security Mis-configuration
	T20	Multi-tenancy
	T21	Server Location and Backup
Data	T22	Data redundancy
	T23	Data loss and leakage
	T24	Data location
	T25	Data recovery
	T26	Data privacy
	T27	Data protection
	T28	Data availability

Special attention is required towards mutual security standards such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS), XML signature, XML Encryption Syntax and Processing, and Key Management Interoperability Protocols. Currently, cloud computing lacks appropriate security standards (T1) [1]. Even if security standards are defined properly, many security issues are still associated with compliance risks (T2) due to lack of governess for audits and assessment of corporate standards [1]. Cloud customers do not have enough knowledge of procedures, processes and practices of the provider, especially in the areas of identity management and segregation of duties. One of the most important aspects of cloud computing security is audit ability (T3). Account and service hijacking (T10) involves phishing, fraud and software vulnerabilities where attackers steal credentials and gain unauthorized access to servers [1]. This unauthorized access is a threat to integrity, confidentiality and availability of data and services [1]. A single customer may access data and compose services from multiple cloud providers using a mobile application or a browser. This kind of access brings in an inherent level of risk and this risk has been called privileged user access (T13) [6]. Unauthorized access becomes possible through browser vulnerabilities. Therefore, Internet browser (T14) is the first stage where security measures should be considered because vulnerabilities in the browser open the door for many follow-on attacks.

Data redundancy (T22) [6], data loss and leakage (T23) [26], data location (T24) [6], data recovery (T25) [27], data privacy (T26) [28], data protection (T27) [29] and data availability (T28) have been marked as major and important issues in different case studies which require data to be properly encrypted, transmitted, protected, controlled and available in the time of need. Identifying cloud security issues and classifying them into several categories, there are dependencies among these categories and the security issues they encompass. If one of the categories is prone to certain attacks, other categories may also become prone to these attacks.

The Theft of Service attack [30] utilizes vulnerabilities in the scheduler of some hypervisors. The
attack is realized when the hypervisor uses a scheduling mechanism, which fails to detect and account of Central Processing Unit (CPU) usage by poorly behaved virtual machines. This failure may further allow malicious customers to obtain cloud services at the expense of others. This attack is more relevant in the public clouds where customers are charged by the amount of time their VM is running rather than by the amount of CPU time used.

Most of the serious attacks in cloud computing come from denial of service (DoS), particularly HTTP, XML and Representational State Transfer (REST)-based DoS attack. The cloud users initiate requests in XML, then send requests over HTTP protocol and usually build their system-interface through REST protocols. Due to vulnerabilities in the system interface, DoS attacks are easier to implement and very difficult for security experts to countermeasure. XML-based distributed denial of service (DDoS) and HTTP-based DDoS attacks are more destructive than traditional DDoS because these protocols are widely used in cloud computing with no strong deterrence mechanisms available to avoid them. HTTP and XML are critical and important elements of cloud computing, so security over these protocols becomes crucial to providing healthy development of a cloud platform.

Cloud malware injection attack refers to a manipulated copy of the victim's service instance, uploaded by attacker to cloud, so that some service requests to the victim's service are processed within that malicious instance. An attacker can get access to user data through this attack. The attacker actually exploits its privileged access capabilities in order to attack that service security domain. The incidents of this attack include credential information leakage, user private-data leakage and unauthorized access to cloud resources. The challenge does not only lie in the failure to detect the malware injection attack but also in the inability to determine the particular node on which the attacker has uploaded the malicious instance [31]. Retrospective detection (examination of hard-drive and memory) has been a widely used technique to detect the host of malware instances. Liu *et al*. in [32] propose a new retrospective detection approach based on portable executable (PE) format file relationship. This approach has been implemented and validated in HADOOP platform. This approach proves higher detection rate as well as lower false positive rate. The main drawback of this approach is that its success is based on three assumptions (pre-requisites): (1) most legitimate programs and malware files are in PE format and lie within a windows platform; (2) the number of legitimate files is greater than that of malware files in user's computer; and (3) creating/writing/reading PE format files seldom happen in a user's computer.

VM side channel attack is an access-driven attack in which an attacker VM alternates execution with the victim VM and leverages the processor cashes to infer the behavior of the victim. It requires that the attacker resides on a different VM on the same physical hardware as that of the victim's VM. Ristenpart *et al*. in [33] discuss a comprehensive example on how to collect information from a target VM through cross VM side channel attack.

Targeted shared memory attacks take advantage of shared memory (cache or main memory) of both physical and virtual machines. It is an initial level attack in cloud computing that can lead up to several different types of attacks such as side channel attacks and malware injection attacks [34]. Phishing is an attempt to access personal information from unsuspecting user through social engineering techniques. It is commonly achieved by sending links of webpage's in emails or through instant messages. These links appear to be correct, leading to a legitimate site such as bank account login or credit card information verification but they practically take users to fake locations.

Cloud computing is an emerging paradigm that involves all the basic components of computing such as end-user machines (PCs), communication networks, access management systems and cloud infrastructures. To achieve comprehensive cloud security, the data and cloud infrastructure must be protected against known/unknown attacks across all cloud components.

III. CONCLUSION

The adoption of cloud computing paradigm is continuously growing. With the massive growth in cloud computing adoption, the security attracted the attention of researchers and practitioners but still has not received enough attention. The number of browser based attacks increased significantly. This notable increase is mainly due to the wide adoption of cloud computing which makes the platform very attractive for attackers due to the growing value of the data assets and resources available on the clouds. Unfortunately, we cannot protect the cloud-computing infrastructure from all the known/unknown attacks because it requires additional computational overhead and resources. Therefore, the major cloud security research challenge lies not only in providing high level security measures but also in doing so with minimum resources and reduced performance degradation.

REFERENCES

[1] Wang, J.-J.; Mu, S. Security issues and countermeasures in cloud computing. In Proceedings of the 2011 IEEE International Conference on Grey Systems and Intelligent Services (GSIS), Nanjing, China, 15–18 September 2011; pp. 843–846.

[2] Final Version of NIST Cloud Computing Definition Published. Available online: http://www.nist.gov/itl/csd/cloud-102511.cfm (accessed on 25 August 2013).

[3] Lv, H.; Hu, Y. Analysis and research about cloud computing security protect policy. In Proceedings of the 2011 International Conference on Intelligence Science and Information Engineering (ISIE), Wuhan, China, 20–21 August 2011; pp. 214–216. **4**. Mell, P and Grance, T. *The NIST Definition of Cloud Computing*, NIST, USA. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, USA, 2009.

[4] Jain, P.; Rane, D.; Patidar, S. A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment. In Proceedings of the 2011

[5] World Congress on Information and Communication Technologies (WICT), Mumbai, India, 11– 14 December 2011; pp. 456–461.

[6] Gowrigolla, B.; Sivaji, S.; Masillamani, M.R. Design and auditing of cloud computing security. In Proceedings of the 2010 5th International Conference on Information and Automation for Sustainability (ICIAFs), Colombo, Sri Lanka, 17–19 December 2010; pp. 292–297.

[7] Khalil, I.M. ELMO: Energy aware local monitoring in sensor networks. *IEEE Trans. Dependable Secur. Comput.* **2011**, *8*, 523–536.

[8] Khalil, I.; Bagchi, S. MISPAR: Mitigating stealthy packet dropping in locally-monitored multihop wireless Ad Hoc networks. In Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks (SecureComm '08), Istanbul, Turkey, 22–25 September 2008; ACM: New York, NY, USA, 2008; article 28, pp. 1–10.

[9] Khalil, I. MCC: Mitigating colluding collision attacks in wireless sensor networks. In Proceedings of the 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010), Miami, FL, USA, 6–10 December 2010; pp. 1–5.

[10] M. Hayajneh, I. Khalil and Y. Gadallah, "An OFDMA-based MAC protocol for under water acoustic wireless sensor network," Proceedings of the 2009 ACM International Conference on Wireless Communications and Mobile Computing (IWCMC'09), Leipzig, Germany, June 21 – 24 2009, pp. 810-814.

[11] Khalil, I.; Hayajneh, M.; Awad, M. SVNM: Secure verification of neighborhood membership in static multi-hop wireless networks. In Proceedings of the IEEE Symposium on Computers and Communications, 2009, ISCC 2009, Sousse, 5–8 July 2009; pp. 368–373.

[12] Sengupta, S.; Kaulgud, V.; Sharma, V.S. Cloud computing security—Trends and research directions. In Proceedings of the 2011 IEEE World Congress on Services (SERVICES), Washington, DC, USA, 4–9 July 2011; pp. 524–531.

[13] Chow, R.; Golle, P.; Jakobsson, M.; Shi, E.; Staddon, J.; Masuoka, R.; Molina, J. Controlling data in the cloud: Outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security, Chicago, IL, USA, 13 November 2009; ACM Press: New York, NY, USA, 2009; pp. 85–90.

[14] Samarati, P.; di Vimercati, S.D.C. Data protection in outsourcing scenarios: Issues and directions. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10), Chicago, IL, USA, 4–8 October 2010; ACM: New York, NY, USA, 2010; pp. 1–14.

[15] Popovic, O.; Jovanovic, Z.; Jovanovic, N.; Popovic, R. A comparison and security analysis of the cloud computing software platforms. In Proceedings of the 2011 10th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS), Nis, Serbia, 5–8 October 2011; Volume 2, pp. 632–634.

[16] Gul, I.; ur Rehman, A.; Islam, M.H. Cloud computing security auditing. In Proceedings of the 2011 the 2nd International Conference on Next Generation Information Technology (ICNIT), Gyeongju, Korea, 21–23 June 2011; pp. 143–148.

[17] Kandukuri, B.R.; Paturi, V.R.; Rakshit, A. 18.Cloud security issues. In Proceedings of the IEEE International Conference on Services computing, 2009 (SCC '09), Bangalore, India, 21–25 September 2009; pp. 517–520.

[18] Chen, Z.; Yoon, J. IT auditing to assure a secure cloud computing. In Proceedings of the 2010 6th World Congress on Services (SERVICES-1), Miami, FL, USA, 5–10 July 2010; pp. 253–259.

[19] Ryan, G.W.; Bernard, H.R. Data Management and Analysis Methods. Available online: http://www.rand.org/pubs/external_publications/EP20000033.html (accessed on 25 August 2013).

[20] Hashizume, K.; Rosado, D.G.; Fernández-Medina, E.; Fernandez, E.B. An analysis of security issues for cloud computing. *J. Internet Serv. Appl.* **2013**, *4*, 5.

[21] Zissis, D.; Lekkas, D. Addressing cloud computing security issues. *Future Gener. Comput. Syst.***2012**, *28*, 583–592.

[22] Whaiduzzaman, M.; Sookhak, M.; Gani, A.; Buyya, R. A survey on vehicular cloud computing. *J. Netw. Comput. Appl.* 2013, doi:10.1016/j.jnca.2013.08.004.

[23] Braun, V.; Clarke, V. Using thematic analysis in psychology. *Qual. Res. Psychol.* 2006, *3*, 77–101.

[24] A Survey on Cloud Computing Security, Challenges and Threats|Whitepapers|TechRepublic. Available online: http://www.techrepublic.com/whitepapers/a-survey-on-cloud- computing security- challenges-and-threats/3483757 (accessed on 18 March 2012).

[25] Behl, A. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In Proceedings of the 2011 World Congress on Information and Communication Technologies (WICT), Mumbai, India, 11–14 December 2011; pp. 217–222.

[26] Mathisen, E. Security challenges and solutions in cloud computing. In Proceedings of the 2011 5th IEEE International Conference on Digital Ecosystems and Technologies Conference (DEST),Daejeon, Korea, 31 May–3 June 2011; pp. 208–212.

[27] Bhardwaj, A.; Kumar, V. Cloud security assessment and identity management. In Proceedings of the 2011 14th International Conference on Computer and Information Technology (ICCIT),Dhaka, Bangladesh, 22–24 December 2011; pp. 387–392.

[28] Mahmood, Z. Data location and security issues in cloud computing. In Proceedings of the 2011 International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), Tirana,Albania, 7–9 September 2011; pp. 49–54.

[29] Fangfei, Z.; Goel, M.; Desnoyers, P.; Sundaram, R. Scheduler vulnerabilities and coordinated attacks in cloud computing. In Proceedings of the 2011 10th IEEE International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 25–27 August 2011; pp. 123–130.

[30] Gruschka, N.; Jensen, M. Attack surfaces: taxonomy for attacks on cloud services. In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD), Miami, FL, USA, 5–10 July 2010; pp. 276–279.

[31] Liu, S.-T.; Chen, Y.-M. Retrospective detection of malware attacks by cloud computing. In Proceedings of the 2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Huangshan, China, 10–12 October 2010; pp. 510–517.

[32] Ristenpart, T.; Tromer, E.; Shacham, H.; Savage, S. 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 (CCS '09), Chicago, IL, USA, 9–13 November 2009; ACM: New York, NY, USA, 2009; pp. 199–212.

[33] Khorshed, M.T.; Ali, A.B.M.S.; Wasimi, S.A. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Gener.Comput. Syst.*2012, *28*, 833–851.

