ISSN 2320 - 2602

Volume 12 No. 1, January 2023

International Journal of Advances in Computer Science and Technology

Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst021212023.pdf

https://doi.org/10.30534/ijacst/2023/0211212023

Concerns from Cloud Security Issues: Challenges and Open Problems

Shadi R. Masadeh [1], Faiz M.AlShrouf [2], A.V.Senthil Kumar[3]

[1]Isra University, Cyber security Department, Jordan, shadi.almasadeh@iu.edu.jo

[1]Isra University, Software Engineering Department, Jordan, Fayez.shrouf@iu.edu.jo

[3]Hindusthan College of Arts & Science, Coimbatore, India. avsenthilkumar@yahoo.com

Received Date : December 6, 2022 Accepted Date : December 30, 2022 Published Date :January 07, 2023

ABSTRACT

The Cloud has become a significant topic in computing; however, the trend has established a new range of security issues that need to be addressed. For example, the owners of data might be worried because the data and associated software are not under their control but rather possessed by the Cloud. In addition, the data owner may not be aware of where the data is geographically located at any particular time. So a question arises as to how secure is the data contained in the Cloud. To help address this question, clients of the Cloud should be given the ability to assess the effectiveness of the Cloud's security measures. Other concerns include unwarranted and unauthorized stoppage of clients' services in the Cloud, breach of security measures, and disruption to service availability. In this article, perspectives from Cloud computing practitioners are shown to help address clients concerns and bring about awareness of the measures put in place to ensure the security of the client services running in the Cloud. In addition, we have reviewed a number of the existing Cloud security approaches and techniques to put a systematic survey of the current security issues in the Cloud environment. Furthermore, we discuss challenges and open problems that these mechanisms face to be effective and efficient.

Key words: Cloud Computing, Security, Encryption, Availability, Scalability, SAS, PAS.

1. INTRODUCTION

Cloud computing is a new paradigm in the era of technology. This paradigm adds new concepts, techniques, and approaches to computing science. In Cloud, software and its data are created and managed virtually for the users and only accessible via a particular Cloud's software, platform, or infrastructure [20]. Before 2005, clients imagined renting resources, information, and software to operate, run and enhance their devices and programs. Currently, it is possible to rent whatever resources you like so that this dream is now realized. Cloud has four important characteristics:

- Availability: The services, platform, and data are accessible at any time and place. Cloud exposes potentially to greater security threats, particularly when the Cloud is based on the Internet rather than an organization's platform [14].
- Automatic backup: Day after day, a lot of manufacturers of electronic devices rely on the concept of Cloud computing and they are increasingly including this paradigm in their products since it brings the features of communication and automatic backup of information [2].
- Adding value and additional services to the user such as the ability to synchronize among friends on social networking sites such as Facebook and friends on phones registered with the same names on the Palm phones [2].

In this paper, we have attempted to put the readers in the current state of security issues in Cloud by reviewing the existing approaches and discussing

their strengths and limitations of them. The rest of the paper is organized as follows. Section 2 states six reasons for increasing clients' fears during the use of Cloud services and describes the current Cloud security tools. Section 3 describes the scenarios of the Cloud threads (or threats). In Section 4, we have reviewed the existing solutions and discussed several perspectives related to the client's fears against using Cloud services. Finally, we have drawn the open problems, conclusions, and future work.

2. REASONS BEHIND CLOUD'S CLIENTS CONCERNS

This section describes several common reasons that led to an increase in concerns among the clients who use Cloud services. The common reasons are as follows:

1. The first question is; what happens if I stop the company's servers for work or faced major problems preventing them from working? But the truth is that regardless of the capacity and capabilities of the company that manages these servers, the potential collapse of the system is taken place everywhere and at any moment, and then this meltdown happens [2]. Thus, the second question is, could Cloud computing fail? The answer to this question is outside of the scope of this paper.

2. Reputable companies attempted to mitigate client fears by confirming that the Cloud model is secure, the Cloud services are protected, the Datacenters and hosted servers are encrypted and the communication channel between the client and the Cloud resources is secured and then it is protected from any kind of attack. However, some attackers claimed that the Cloud resources are penetrated much more easily than the non-Cloud environment [20]. So that who informs us the truth and what is the level of protection we believe it does! If Sony is telling the truth about encrypting the data, it seems that the level of encryption is not strong enough [22].

3. Due to a lack of control over Cloud software, platform, and/or infrastructure, academics and practitioners stated that security is a major challenge in the Cloud. In Cloud computing, the data will be virtualized across different host machines and accessed on the Web [14, 17]. From the business point of view, the Cloud provides a channel to the service or platform in which it could operate [14]. Stallman [5] from the Free Software Foundation re-called Cloud computing with Careless Computing because the Cloud clients will not control their data and software and then there is no monitoring over the Cloud providers and subsequently the data owner may not recognize where data is geographically located at any particular time.

4. Threats in Cloud computing might have resulted from the generic Cloud infrastructure available to the public; while it is possessed by an organization selling Cloud services ([16, 17].

Several companies are now offering Cloud applications and services including Microsoft Azure Services Platform, [1] Web Services, Google, and open sources Cloud systems such as Sun Open Cloud Platform for academics, clients, and administrative purposes [14]. Yet, some organizations have not realized the importance of the security of Cloud systems. These organizations adopted some readily available security and protection tools to secure their systems.

Today, Amazon uses the Cloud platform for introducing several web services for clients. Amazon constructed Amazon Web Services (AWS) platform to secure access to web services. The AWS platform introduces protection against traditional security issues in the Cloud network [1]. Physical access to AWS Datacenters is limited and controlled since the data owner may be aware of where the data is geographically located at any particular time. The authorized staff has to log-in in two authentication phases with a restricted number of times for accessing AWS and AWS Datacenters at a maximum [1]. Note that Amazon only offers restricted Datacenter access and information to people who have a legal business need for these privileges. If the business need for these privileges is revoked, then the access is stopped, even if employees continue to be an employee in Amazon or AWS [1]. However, one of the weaknesses of the AWS is the dynamic data, which is generated from the AWS, and could be listened to and penetrated by users [20].

Microsoft proposed a new secure system, which consists of five main services forming the core of the operating system: (i) Windows Azure, which is the main part of the system and is specialized for hosting services and data storage; (ii) Microsoft SQL Services, which is a part of the relevant databases for these services developed and hosted by the system; (iii) Microsoft. NET Services, which is an application framework; (iv) Live Services, which share photos and synchronize with computers and portable devices; and (v) Microsoft SharePoint Services and Microsoft Dynamics CRM Services for business content management [3].

Fiore and Aloisio [24] have proposed a new security technique to measure the legitimacy of Cloud

resources and the trustiness or trustworthiness of Cloud database management using metadata and privilege-based access control. Using metadata of files or everything-as-a-service (XaaS) and system context user information have gained several benefits together with assurance of Cloud resources for trust services.

3. SCENARIOS OF CLOUD THREATS

Security principles in the Cloud can be lost [1, 7]; for example, criminals might penetrate the Cloud in many forms. An insider adversary, who gains physical access to Datacenters, can destroy any type of static content at the root of a web server. It is not only physical access to Datacenter that can corrupt data, but malicious web manipulation software can penetrate servers and Datacenter machines.

Once they are installed malicious software can monitor, intercept, and tamper with online transactions in a trusted organization. The result typically allows criminals full root access to Datacenter and web server application. As soon as such access has been established, the integrity of data or software is in question [15, 20].
There are several security products (e.g. Antivirus, Firewalls, gateways, and scanners) to secure the Cloud systems but they are not sufficient as each one of them has only a specific purpose and hence, they are called ad-hoc security tools. For example, Network firewalls provide protection only at the host and network levels [4]. There are, however, three reasons why these security defenses cannot be only used to secure systems [4]:
1. They cannot stop malicious attacks that perform illegal transactions, because they are designed to prevent vulnerabilities of signatures and specific ports.

2. They cannot manipulate form operations such as asking the user to submit certain information or validate false data because they cannot distinguish between the original request-response conversation and the tampered conversation.

3. They do not track conversations and do not secure the session information. For example, they cannot track when session information in cookies is exchanged over an HTTP request-response model.

Figure 1 shows the data storage and Datacenters, which are possibly targeted by the criminals. According to computer forensics, the distrusted servers and Datacenters are the target of crime. Therefore, the question that needs to be answered is whether or not data is safe and secure.
Data confidentiality might be compromised either by insider user threats or outsider user threats [6]. For instance, insider user threats might maliciously come from Cloud operator/provider, a Cloud client, or a malicious third party.

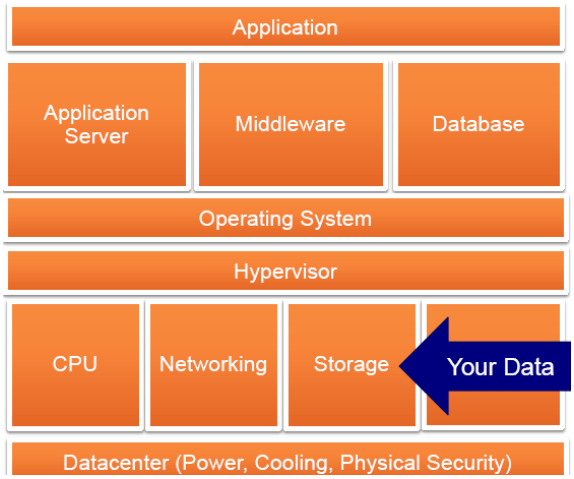

Figure 1: Cloud Computing Security - taken from [17]

4. CURRENT CLOUD SECURITY APPROACHES

We survey a number of the current solutions in Cloud security as shown in Table 1. This Table includes the existing solutions and their strengths, weaknesses, and limitations.

Table 1: The existing approaches and techniques and their strengths, weaknesses, and limitations

Approaches and Techniques	Strengths	Weaknesses	Limitations
An approach introduced in [25] suggested the use of five-level securities; which are based on authentication, confidentiality, and integrity to the data stored and accessed by the cloud user at Datacenters.	The authentication scheme is based on hashed password storage between the cloud provider and the cloud client. The data confidentiality and integrity are provided	The authentication schema limited the access to the predefined IP or MAC address of the cloud client, which makes the access to the data restricted to one location.	The cloud client can access the Datacenter only from one location.

	through the MD5 cryptosystem hash technique.		
The authors in [26] presented a wide variety of methods that can be included to protect and secure cloud computing.			There were no implementation or performance results of efficiency WEP OR SSID through wireless devices.
In [27] an approach was adopted by using DNA cryptography for the optimization of data security in cloud security.	The DNA cryptography approach is not constrained to specific encryption and decryption algorithms.		DNA cryptography is still mostly a theoretical concept and still not implemented.
In [28] the authors proposed an approach that is based on three cryptographic techniques (Key Policy Attribute-based Encryption, Proxy Re-Encryption, and Lazy re-encryption) to secure data in cloud Datacenters.		The implications of the KP-ABE scheme may not be entirely realistic, because the approach assumes the existence of a single trusted party who monitors all attributes and issues all decryption keys between cloud client and provider.	
In [29] the authors introduced a framework for a secure client cloud environment through the use of a VPN to access the network of the cloud provider.			

5.OPEN PROBLEMS AND CONCLUSIONS

Several open problems are drawn in this paper:

• The authentication schema limited the access to the predefined IP or MAC address of the cloud client, which makes the access to the data restricted to one location.

• The implications of the KP-ABE scheme may not be entirely realistic, because the approach assumes the existence of a single trusted party who monitors all attributes and issues all decryption keys between cloud client and provider.

• Who certifies the cloud provider to be trusted to be used by the cloud client? The need for a third party is to distribute keys between CC and CP. No implementation model proves or justifies that the three algorithms can calm the fears of cloud clients.

The existing Cloud services might face various security issues at the Cloud models level. One main challenge is the lack of control over the Cloud Datacenters. Furthermore, security is not integrated into the service development process.

Indeed, the traditional security tools alone would not be able to resolve the recent security issues and so it will be helpful to incorporate security components upfront into the development methodology of the Cloud system. In this paper, several Cloud practitioners' perspectives are presented to calm the clients' fears against Cloud concerns. As a part of future work, we will present a conceptual framework of several components that assist to indicate the levels of Cloud security that should be taken into account by researchers and practitioners.

ACKNOWLEDGEMENT

The authors owe many thanks to Isra University and the Faculty of Information Technology for supporting this research.

REFERENCES

[1] Amazon (2010) Amazon Web Services: Overview of Security Processes. Available at http://www.awsmedia.s3.amazonaws.com/pdf/AWSSecurity_Whitepaper.pdf.

[2] A. Jaber (2009) Beware!! When they show cloud computing and uglier faces. Available at: http://www.swalif.net/.

[3] B. Calder, J. Wang, A. Ogus, N. Nilakantan, A. Skjolsvold, S. McKelvie, Y. Xu, S. Srivastav, J. Wu, H. Simitci, J. Haridas, C. Uddaraju, H. Khatri, A. Edwards, V. Bedekar, S. Mainali, R. Abbasi, A. Agarwal, M. F. ul Haq, M. I. ul Haq, D. Bhardwaj, S. Dayanand, A. Adusumilli, M. McNett, S. Sankaran, K. Manivannan, and L.(2011) Windows Azure Storage: a highly available cloud storage service with strong consistency. In Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles (SOSP '11). ACM, New York, NY, USA, 143-157. DOI=10.1145/2043556.2043571 http://doi.acm.org/10.1145/2043556.2043571.

[4] B. Gehling, B & Stankard, D. (2005) eCommerce security. In Proceedings of Information Security Curriculum Development (InfoSecCD) Conference 05, Kennesaw, GA, USA, pp 32-37.

[5] C. Arthur (2010) Google's ChromeOS means losing control of data, warns GNU founder Richard Stallman. Available at http://www.guardian.co.uk/technology/blog/2010/dec/14/chrome-os-richard-stallman-warning.

[6] CPNI (2010) Information Security Briefing 01/2010 Cloud Computing. Available at www.cpni.gov.uk/Documents/.../2010/2010007-ISB_cloud_computing.pdf.

[7] DM. Cappelli, RF. Trzeciak, & AB. Moore (2006) Insider Threats in the SLDC: Lessions Learned From Actual Incidents of Fraud: Theft of Sensitive Information, and IT Sabotage, Carnegie Mellon University, USA: CERT.

[8] R. S. Dr. Ulrich Lang, Top SOA security concerns & OpenPMF model-driven security, Object Security White Paper, topics Cloud Computing, and Security Management, 2009.

[9] Google (2011b) Google Trends: Private Cloud, Public Cloud. Available at http://www.google.de/trends?q=private+cloud%2C+public+cloud.

[10] H. Wang, Y. Zhang, & J. Cao (2005) Effective Collaboration with Information Sharing in Virtual Universities. In Proc. Knowledge and Data Engineering, USA: IEEE Transactions, 21 (6); 40-853.

[11] L. M. Vaquero, J. Cáceres, & D. Morán (2011) The Challenge of Service Level Scalability for the Cloud. International Journal of Cloud Applications and Computing (IJCAC), 1(1), 34-44. doi:10.4018/ijcac.2011010103

[12] J. Arshad, P. Townend, & J. Xu (2011) An Abstract Model for Integrated Intrusion Detection and Severity Analysis for Clouds. International Journal of Cloud Applications and Computing (IJCAC), 1(1), 1-16. doi:10.4018/ijcac.2011010101

[13] N. Kolakowski (2012) Public Cloud Security: 5 Things to Consider. Slashdot Magazine, Available at http://slashdot.org/topic/cloud/public-cloud-security-5-things-to-consider/.

[14] M. Taylor (2010) Enterprise Architecture – Architectural Strategies for Cloud Computing: Oracle. Retrieved from http://www.techrepublic.com/whitepapers/oracle-white-paper-in-enterprise-architecture-architecture-strategies-for-cloud-computing/2319999.

[15] N. Provos, D. McNamee, P. Mavrommatis, K. Wang, & N. Modadugu (2007) The ghost in the browser analysis of web-based malware. In: HotBots'07: Proceedings of the RST conference on First Workshop on Hot Topics in Understanding Botnets, Berkeley, CA, USA: USENIX Association; 4-4.

[16] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, & J. Molina (2009) Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW '09). ACM, New York, NY, USA, 85-90. DOI=10.1145/1655008.1655020 http://doi.acm.org/10.1145/1655008.1655020

[17] R. Marchany (2010) Cloud Computing Security Issues: VA Tech IT Security. Retrieved from www.issa-centralva.org/.../01-2010_CCSecIssues.ppt.

[18] RG. Cárdenas, & E. Sanchez (2005) Security Challenges of Distributed e-Learning Systems. ISSADS: Springer, Series Lecture Notes in Computer Science, 3563, http://dblp.uni-trier.de/db/conf/issads/issads2005.html#CardenasS05; 538-544.

[19] S. Ragan (2012) Cloud Security: What You Need to Know to Lock It Down. Slashdot Magazine. Retrieved from http://slashdot.org/topic/cloud/cloud-security-what-you-need-to-know/.

[20] S. Aljawarneh (2011) Cloud Security Engineering: Avoiding Security Threats the Right Way. International Journal of Cloud Applications

and Computing (IJCAC), 1(2), 64-70. doi:10.4018/ijcac.2011040105.
[21] http://www.linkedin.com.
[22] T. Bradley (2011) Sony says data is protected, attackers say it's for sale. PC World (US online). Retrieved from http://www.cio.com.au/article/384858/sony_says_data_protected_attackers_say_it_sale/.
[23] Trusted Computing Group (2010) Cloud Computing and Security –A Natural Match. Retrieved from www.infosec.co.uk/.../Cloud_Computing_and_Security-A_Natural_Match_ TCG_Whitepaper_20.pdf.
[24] S. Fiore and G. Aloisio (eds.), Grid and Cloud Database Management, Chapter 6, Springer-Verlag, Berlin Heidelberg, 2011.S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[25] Bina Kotiyal, Priti Saxena, R H Goudar and Rashmi M Jogdand.. A 5-Level Security Approach for Data Storage in Cloud. International Journal of Computer Applications. 54(11):29-34, September 2012.
[26] Priyanka Naik, Sugata Sanyal: Increasing Security in Cloud Environment. The Computing Research Repository (CoRR).pp1301-0315 (2013).
[27] Anup R. Nimje. Cryptography In Cloud-Security Using DNA (Genetic) Techniques. International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue5, September-October 2012, pp.1358-1359.
[28] Suresh B 1 Sangeetha Guptha. Enhanced Data Security and Access Control Approach in Cloud Environment. International Journal Of Advanced Research and Innovations Vol.1, Issue .2 (2013) :pp 81-85.
[29] ASHA MATHEW. SECURITY AND PRIVACY ISSUES OF CLOUD COMPUTING; SOLUTIONS AND SECURE FRAMEWORK. International Journal of Multidisciplinary Research Vol.2 Issues 4, April 2012,pp182-193.