ISSN 2320-9984
Volume 5 Issue 4 | December 2017 ISSN: 2320-9984 (Online)
International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

Challenges in Cloud Computing for Data Privacy

Loveleen Kaur
Assistant Professor
Jabalpur Engineering college Jabalpur
Jabalpur, (M.P.) [INDIA]
Email: lpabla@jecjabalpur.ac.in

Abstract**—***Cloud Computing is becoming a well-known exhortation nowadays. Many companies, such as Amazon, Google, and Microsoft and so on, accelerate their paces in developing Cloud Computing systems and enhancing their services to provide for a larger amount of users. However, security and privacy issues present a strong barrier for users to adapt into Cloud computing systems. In this paper, we investigate several Cloud computing system providers about their concerns on security and privacy issues. We find those concerns are not adequate and more should be added in terms of five aspects (i.e., availability, confidentiality, data integrity, control, audit) for security In this paper, on the one hand, the summary on the current security and privacy information challenges have been surveyed. Second, the current security measurements are summarized as well.*

Keywords:**—***cloud computing, data security, privacy information; cloud computing provider*

1. INTRODUCTION

Different from the conventional computing models, cloud computing [1-13] combines many new factors including distributed computing and virtualization together to form a novel mechanism which can be manageable and dynamic extended.

Cloud computing security concerns all the aspects of making cloud computing secure. Many of these aspects are not unique to the cloud setting: data is vulnerable to attack irrespective of where it is stored. Therefore, cloud computing security encompasses all the topics of computing security, including the design of security architectures. However, cloud computing also has several special characteristics [14-17]:

(a) Essentially, the cloud can be viewed as a shared resource, so we cannot guarantee that other sharers are not dangerous. In other words, we cannot confirm the legitimacy of other resources.

(b) Insecure APIs and protocols may get the authority to access the data on the cloud.

(c) Once the security mechanism falls, the illegal cloud provider is able to modify or delete the data in the cloud.

(d) It is fine for the data in the cloud to open, but the extent should be limited.

In order to overcome the above potential drawbacks, references [18-25] have proposed several novel models or approaches. For example, virtual machines can be deployed in the cloud to separate the processes. As regard the data security, an alternative is to deploy practical and feasible backup mechanism. Of course, several models are constructed to detect the improper modifications.

Based on the content mentioned above, this paper presents a summary of cloud computing and related security challenges, and potential approaches in the field are proposed. The organization of this paper is as follows. Section 2 introduces the classic theory of cloud computing. Section 3 presents solutions or potential ideas on the current issues existing in the cloud computing. Finally, Section 4 concludes the paper.

2. CLASSIC THEORY OF CLOUD COMPUTING

Cloud computing can provide large batches of task requests for a large number of clients simultaneously. Once receiving the service requests, cloud service providers will distribute corresponding computing resources based on different requests from the clients or the dispenses of the cloud computing resources the clients pay for. The traditional cloud computing model is shown in Figure 1.

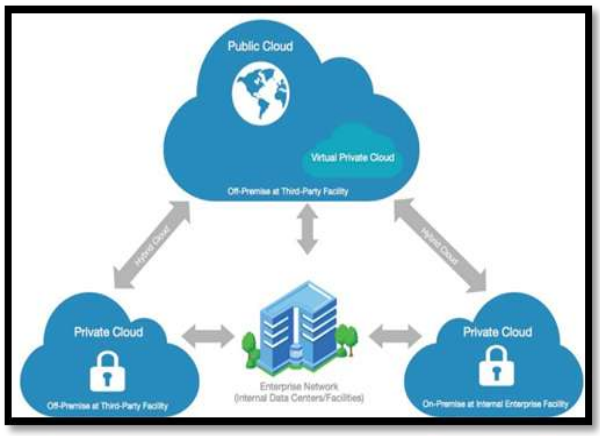

Figure 1. Traditional Cloud Computing Model

Cloud computing can be categorized into four types including private, public, community, and hybrid clouds [26].

(a) Private cloud is owned or rented by an organization. The whole cloud resource is dedicated to that organization for its private use. An example of this model is a cloud built by an enterprise to serve their business critical applications.

(b) Public cloud is owned by a service provider and its resources are sold to the public. End-users can rent parts of the resources and can typically scale their resource consumption up to their requirements. Amazon, Google, Rackspace, Salesforce, and Microsoft are examples of public cloud providers.

(c) Community cloud is similar to a private cloud, but where the cloud resource is shared among members of a closed community with similar interests. An example of a community cloud is the Media Cloud set up by Siemens IT Solutions and Services for the media industry. A community cloud may be operated by a third party (as in the Siemens case), or may be controlled and operated in a collaborative fashion as in the Grid Computing paradigm.

(d) Hybrid cloud is the combination of two or more cloud infrastructures; these can be private, public, or community clouds. The main purpose of a hybrid cloud is usually to provide extra resources in cases of high demand, for instance enabling to transfer some computation tasks from a private cloud to a public cloud.

3. CURRENT SECURITY MEASUREMENTS

In order to deal with the problems mentioned above, the current security measurements are summarized as follows.

A. Privacy data access processing

The community cloud is composed of two or more clouds running independently, which supports the data and application transferring among different clouds. The community cloud which consists of private cloud and public cloud has the both advantages, namely it has not only the privacy property of the private cloud, but also the low computational costs of the public cloud. As a result, the community cloud becomes the preferred pattern towards many corporations or

organizations, and it is regarded as the prime mode of the future cloud computing as well.

Although the combination of the public and private clouds is a reasonable scheme to deal with the cloud computing security and privacy, how to effectively integrate the two types of clouds is still a tough problem. The ideal object is composed of two parts. On the one hand, we are able to make adequate use of the rich computing and storage resources of the public cloud. On the other hand, the privacy information of the clients should be protected effectively.

Several scholars proposed a novel community cloud mode, which added the privacy protection module based on the Hadoop MapReduce concept; so that the privacy-sensing-based community cloud computing is realized. The core idea is to split the computing tasks, and the sensitive privacy data is disposed in the private cloud, while the insensitive data is dealt in the public cloud. The limitation lies in that the client has to assign the sensitive data, so the above mode could do nothing to the unknown sensitive data.

B. Encoding data searching

The encoding may destroy the original ordering, comparability and other properties, so that the data searching may become more difficult. A direct searching scheme in the cloud storage is as follows. Firstly, the data owner downloads the cipher text from the cloud server. Then the cipher text is decoded to be the plaintext. Finally, let the computer search for the data plaintext. Obviously, the above method is lack of efficiency.

Early references involved a encrypt data searching based practical algorithm, which adopts symmetric encryption algorithm to encode the text and its keywords respectively. The server can search which texts include the corresponding keywords offered by the clients, but it cannot obtain the practical information on the text content. Moreover, current searching scheme can only complete searching of the single keyword, but it cannot satisfy the common searching of the clients. In order to guarantee that the public-key encryption with the keyword searching can be better applicable to the cloud computing environments, we should construct another better public-key encryption scheme which can realize privacy protection and complex logic expression.

C. Encoding data computing

With the fast development of the cloud computing, the data owner is able to upload massive data upon the cloud server to conduct computing and searching, which is helpful to decrease the costs of storage, computation and managements. Recently, property encryption and homomorphic encryption are utilized to deal with the issue of encoding data computing.

Homomorphic encryption is to conduct the cipher text and the plaintext simultaneously and directly. With this algorithm, the cipher text still can be done even though the plaintext is unknown. The clients encode the data firstly, and then the cipher text is uploaded to the cloud server. The server can conduct the data cipher text according to the clients' requirements, and put the computed result to the clients. The clients can use the private-key to decode the cipher text to achieve corresponding computed result of the plaintext. However, the clients cannot verify the correctness of the computed result from the cloud server.

4. CONCLUSIONS

Cloud computing has evolved as a popular and universal paradigm for service oriented computing where computing infrastructure and solutions are delivered as a service. This paper firstly introduces the classic theory of cloud computing. Then, the potential security and privacy information challenges are given. Ultimately, the current measurements are summarized as well.

REFERENCES:

[1] K. Zaerens. Gaining the profits of cloud computing in a public authority environment. International Journal of Computational Science and Engineering, vol. 7, 2012, pp. 269-279.

[2] W. Ren, Y. L. Liu. A lightweight possession proof scheme for outsourced files in mobile cloud computing based on chameleon hash function. International Journal of Computational Science and Engineering, vol. 9, 2014, pp. 339-346.

[3] W. M. Shi, B. Hong. Task scheduling in budget-constrained cloud computing systems to maximise throughput. International Journal of Computational Science and Engineering, vol. 7, 2012, pp. 319-328.

[4] M. Ficco. Security event correlation approach for cloud computing. International Journal of High Performance Computing and Networking, vol. 7, 2013, pp. 173-185.

[5] P. Xiao, N. Han. A novel power-conscious scheduling algorithm for data-intensive precedence-constrained applications in cloud environments. International Journal of High Performance Computing and Networking, vol. 7, 2014, pp. 299-306.

[6] Q. N. T. Do, F. K. Hussain. A hybrid approach for the personalisation of cloud-based e-governance services. International Journal of High Performance Computing and Networking, vol. 7, 2013, pp. 205-214.

[7] W. W. Kong, Y. Lei, J. Ma. Virtual machine resource scheduling algorithm for cloud computing based on auction mechanism. Optik, vol. 127, 2016, pp. 5099-5104.

[8] X. F. Ye, B. Khoussainov. Fine-grained access control for cloud computing. International Journal of Grid and Utility Computing, vol. 4(2-3), 2013, pp. 160-168.

[9] X. D. Zhu, H. Li, F. H. Li. Privacy-preserving logistic regression outsourcing in cloud computing. International Journal of Grid and Utility Computing, vol. 4(2-3), 2013, pp. 144-150.

[10] P. Ronald, S. Stephan, S. Christoph. A privacy-friendly architecture for future cloud computing. International Journal of Grid and Utility Computing, vol. 4(4), 2013, pp. 265-277.

[11] I. N. C. S. Narayana; G. Gopinath, K. P. C. Mogan, et al. A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment. International Journal of Grid and Utility Computing, vol. 5(4), 2014, pp. 236-248.

[12] W. W. Kong, Y. Lei, J. Ma. Virtual machine resource scheduling algorithm for cloud computing based on auction mechanism. Optik, vol. 127(12), 2016, pp. 5099-5104.

[13] S. J. Baek, S. M. Park, S. H. Yang, et al. Efficient server virtualization using grid service infrastructure. Journal of Information Processing Systems, vol. 6(4), 2010, pp. 553-562.

[14] M. D. Ryan. Cloud computing security: The scientific challenge, and a survey of solutions. The Journal of Systems and Software, vol. 86(9),

2013, pp. 2263-2268.

[15] Y. Chen, V. Paxson, R. H. Katz. What's new about cloud computing security? Technical Report UCB/ EECS-2010-5, Electrical Engineering and Computer Sciences, University of California at Berkeley, 2010.

[16] Cloud Security Alliance, 2010. Top threats to cloud computing v1.0. http:// cloudsecurityalliance.org/ topthreats/csathreats.v1.0.pdf.

[17] M. Christodorescu, R. Sailer, D. L. Schales, et al. Cloud security is not (just) virtualization security: a short paper. In: Proceedings of the ACM Workshop on Cloud Computing Security, 2009, pp. 97-102.

[18] V. Chang, Y. H. Kuo, M. Ramachandran. Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, vol. 57(1), 2016, pp. 24-41.

[19] M. Ali, S. U. Khan, A. V. Vasilakos. Security in cloud computing: Opportunities and challenges. Information Sciences, vol. 305(3), 2015, pp. 357-383.

[20] S. Naser, S. Kamil, N. Thomas. A case study in inspecting the cost of security in cloud computing. Electronic Notes in Theoretical Computer Science, vol. 318(11), 2015, pp. 179-196.

[21] Y. Xiang, B. D. Martino, G. L. Wang, et al. Cloud computing: security, privacy and practice. Future Generation Computer Systems, vol. 52(11), 2015, pp. 59-60.

[22] R. Oscar, M. Daniel, F. M. Eduardo, et al. Empirical evaluation of a cloud computing information security governance framework. Information and Software Technology, vol. 58(2), 2015, pp. 44-57.

[23] H. Rasheed. Data and infrastructure security auditing in cloud computing environments. International Journal of Information Management, vol. 34 (3), 2014, pp. 364-368.

[24] D. G. Feng, M. Zhang, Y. Zhang, et al. Study on cloud computing security. Journal of Software, vol. 22 (1), 2011, pp. 71-83.

[25] C. Lin, W. B. Su, K. Meng, et al. Cloud computing security: architecture, mechanism and modeling. Chinese Journal of Computers, vol. 36(9), 2013, pp. 1765-1784.

[26] V. Jain, V. Sharma. Surveying and analyzing security challenges and privacy in cloud computing. International Journal of Computer Science and Information Technology & Security, vol. 3(5), 2013, pp. 316-321.