Data security and privacy information challenges in cloud computing

Weiwei Kong*

Xijing University,
Xi'an, 710123, China
Email: kwwking@163.com
*Corresponding author

Yang Lei

Department of Electronics Technology,
Engineering University of Armed Police Force,
Xi'an, 710086, China
Email: surina526@163.com

Jing Ma

Key Laboratory of Information Assurance Technology,
Beijing, 100072, China
Email: mrsma919@163.com

Abstract: Cloud computing is becoming the hotspot in the area of information technology. However, when examining its convenience and strong ability in data processing, we also find that great challenges appear in terms of data security and privacy information protection. In this paper, firstly, the current security and privacy information challenges have been surveyed. Second, the current security measures are summarised as well.

Keywords: cloud computing; data security; privacy information; cloud computing provider.

Reference to this paper should be made as follows: Kong, W., Lei, Y. and Ma, J. (2018) 'Data security and privacy information challenges in cloud computing', *Int. J. Computational Science and Engineering*, Vol. 16, No. 3, pp.215–218.

Biographical notes: Weiwei Kong received his Bachelor's, Master's and PhD in Computer Science and Technology from the Air Force Engineering University, China, in 2005, 2008 and 2011, respectively. He is currently an Associate Professor in the Xijing University, China. He is a member of the IEEE and the Institute of Electronics, Information and Communication Engineers (IEICE). His research interests are in the areas of image cloud computing and pattern recognition.

Yang Lei received her Bachelor's, Master's and PhD in Computer Science and Technology from the Air Force Engineering University, China, in 2006, 2009 and 2012, respectively. She is currently a Lecturer in the Engineering University of Armed Police Force, China. She is a member of the IEEE. Her research interests are in the areas of network security and pattern recognition.

Jing Ma received her Bachelor's and Master's in Computer Science and Technology from Information Engineering University, China, in 2004 and 2007, respectively. She is currently an Engineer in the AirForce Institute, China. She is a member of the IEEE. Her research interest is network security.

1 Introduction

Different from the conventional computing models, cloud computing (Iosup et al., 2011; Prasad and Rao, 2014; Li et al., 2015; Yuriyama and Kushida, 2011; Mori et al., 2012; Raekow et al., 2013; Yao et al., 2013; Ye and Khoussainov, 2013; Zhu et al., 2013; Ronald et al., 2013; Narayana et al., 2014; Kong et al., 2016; Baek et al., 2010) combines many new factors including distributed computing and virtualisation together to form a novel mechanism which can be manageable and dynamically 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 (Ryan, 2013; Chen et al., 2010; Kumar, 2010; Christodorescu et al., 2009):

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 (Chang et al., 2016; Ali et al., 2015; Naser et al., 20015; Xiang et al., 2015; Oscar et al., 2015; Rasheed, 2014; Feng et al., 2011; Lin et al., 2013; Wlodarczyk et al., 2009; Ai and Mukaidono, 2011; Hsu et al., 2011; Kryvinska et al., 2010; Siemens IT Solutions and Services, 2011) 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 organisation 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.

Cloud computing can be categorised into four types including private, public, community, and hybrid clouds (Wlodarczyk et al., 2009).

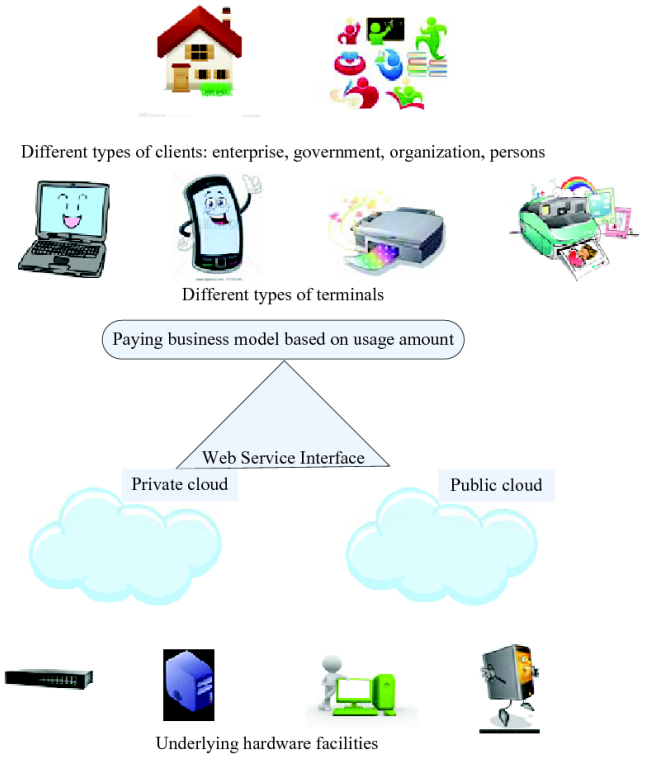
a Private cloud is owned or rented by an organisation. The whole cloud resource is dedicated to that organisation for its private use. An example of this model is a cloud built by an enterprise to serve their business critical applications.

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 setup by Siemens IT Solutions and Services (2011) 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.

Figure 1 Traditional cloud computing model (see online version for colours)



3 Current security measurements

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

3.1 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 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 for many corporations or organisations, 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 realised. 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.

3.2 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 realise privacy protection and complex logic expression.

3.3 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 utilised 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 summarised as well.

Acknowledgements

The authors would like to thank all the reviewers and editors for their valuable comments and works. The work was supported in part by the National Natural Science Foundations of China under Grant 61309008, 61309022 and 61473237; Natural Science Foundation of Shannxi Province of China under Grant 2014JQ8049; Foundation of Science and Technology on Information Assurance Laboratory under Grant KJ-15-102; Natural Science Foundations of the Engineering University of the Armed Police Force of China under Grant WJY-201414; Natural Science Foundation of Shaanxi Provincial Department of Education under Grant 16JK2246.

References

Ai, L.A.P. and Mukaidono, M. (2011) 'Selection of model in developing information security criteria for smart grid security system', *Journal of Convergence*, Vol. 2, No. 1, pp.39–46.

Ali, M., Khan, S.U. and Vasilakos, A.V. (2015) 'Security in cloud computing: opportunities and challenges', *Information Sciences*, Vol. 305, No. 3, pp.357–383.

Baek, S.J., Park, S.M., Yang, S.H. et al. (2010) 'Efficient server virtualization using grid service infrastructure', *Journal of Information Processing Systems*, Vol. 6, No. 4, pp.553–562.

Chang, V., Kuo, Y.H. and Ramachandran, M. (2016) 'Cloud computing adoption framework: a security framework for business clouds', *Future Generation Computer Systems*, Vol. 57, No. 1, pp.24–41.

Chen, Y., Paxson, V. and Katz, R.H. (2010) *What's New About Cloud Computing Security?*, Technical Report UCB/EECS-2010-5, Electrical Engineering and Computer Sciences, University of California at Berkeley.

Christodorescu, M., Sailer, R., Schales, D.L. et al. (2009) 'Cloud security is not (just) virtualization security: a short paper', in *Proceedings of the ACM Workshop on Cloud Computing Security*, pp.97–102.

Feng, D.G., Zhang, M., Zhang, Y. et al. (2011) 'Study on cloud computing security', *Journal of Software*, Vol. 22, No. 1, pp.71–83.

Hsu, P.H., Tang, W.S., Tsai, C. et al. (2011) 'Two-layer security scheme for AMI system', *Journal of Convergence*, Vol. 2, No. 1, pp.47–52.

Iosup, A., Ostermann, S., Yigitbasi, M.N. et al. (2011) 'Performance analysis of cloud computing services for many-tasks scientific computing', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22, No. 6, pp.931–945.

Kong, W.W., Lei, Y. and Ma, J. (2016) 'Virtual machine resource scheduling algorithm for cloud computing based on auction mechanism', *Optik*, Vol. 127, No. 12, pp.5099–5104.

Kryvinska, N., Thanh, D.V. and Strauss, C. (2010) 'Integrated management platform for seamless services provisioning in converged network', *International Journal of Information Technology Communications & Convergence*, Vol. 1, No. 1, pp.77–91.

Kumar, S.N. (2010) *Top Threats to Cloud Computing v1.0*, Cloud Security Alliance [online] http://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

Li, J., Tan, X., Chen, X.F. et al. (2015) 'OPoR: enabling proof of retrievability in cloud computing with resource-constrained devices', *IEEE Transactions on Cloud Computing*, Vol. 3, No. 2, pp.195–205.

Lin, C., Su, W.B., Meng, K. et al. (2013) 'Cloud computing security: architecture, mechanism and modeling', *Chinese Journal of Computers*, Vol. 36, No. 9, pp.1765–1784.

Mori, T., Nakashima, M. and Ito, T. (2012) 'SpACCE: a sophisticated ad hoc cloud computing environment built by server migration to facilitate distributed collaboration', *International Journal of Space-Based and Situated Computing*, Vol. 2, No. 4, pp.230–239.

Narayana, I.N.C.S., Gopinath, G., Mogan, K.P.C. et al. (2014) 'A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment', *International Journal of Grid and Utility Computing*, Vol. 5, No. 4, pp.236–248.

Naser, S., Kamil, S. and Thomas, N. (2015) 'A case study in inspecting the cost of security in cloud computing', *Electronic Notes in Theoretical Computer Science*, Vol. 318, No. 11, pp.179–196.

Oscar, R., Daniel, M., Eduardo, F.M. et al. (2015) 'Empirical evaluation of a cloud computing information security governance framework', *Information and Software Technology*, Vol. 58, No. 2, pp.44–57.

Prasad, A.S. and Rao, S. (2014) 'A mechanism design approach to resource procurement in cloud computing', *IEEE Transactions on Computers*, Vol. 63, No. 1, pp.17–30.

Raekow, Y., Simmendinger, C., Jenz, D. et al. (2013) 'On-demand software licence provisioning in grid and cloud computing', *International Journal of Grid and Utility Computing*, Vol. 4, No. 1, pp.10–20.

Rasheed, H. (2014) 'Data and infrastructure security auditing in cloud computing environments', *International Journal of Information Management*, Vol. 34, No. 3, pp.364–368.

Ronald, P., Stephan, S. and Christoph, S. (2013) 'A privacy-friendly architecture for future cloud computing', *International Journal of Grid and Utility Computing*, Vol. 4, No. 4, pp.265–277.

Ryan, M.D. (2013) 'Cloud computing security: the scientific challenge, and a survey of solutions', *The Journal of Systems and Software*, Vol. 86, No. 9, pp.2263–2268.

Siemens IT Solutions and Services (2011) *Community Clouds: Supporting Business Ecosystems with Cloud Computing* [online] http://docplayer.net/1234732-Community-clouds-supporting-business-ecosystems-with-cloud-computing.html.

Wlodarczyk, T., Rong, C.M. and Thorsen, K.A. (2009) 'Industrial cloud: toward inter-enterprise integration', *Cloud Computing, Lecture Notes in Computer Science*, Vol. 5931, pp.460–471, Springer, Berlin/Heidelberg.

Xiang, Y., Martino, B.D., Wang, G.L. et al. (2015) 'Cloud computing: security, privacy and practice', *Future Generation Computer Systems*, Vol. 52, No. 11, pp.59–60.

Yao, Z.Q., Xiong, J.B., Ma, J.F. et al. (2013) 'Access control requirements for structured document in cloud computing', *International Journal of Grid and Utility Computing*, Vol. 4, Nos. 2–3, pp.95–102.

Ye, X.F. and Khoussainov, B. (2013) 'Fine-grained access control for cloud computing', *International Journal of Grid and Utility Computing*, Vol. 4, Nos. 2–3, pp.160–168.

Yuriyama, M. and Kushida, T. (2011) 'Integrated cloud computing environment with IT resources and sensor devices', *International Journal of Space-Based and Situated Computing*, Vol. 1, Nos. 2–3, pp.163–173.

Zhu, X.D., Li, H. and Li, F.H. (2013) 'Privacy-preserving logistic regression outsourcing in cloud computing', *International Journal of Grid and Utility Computing*, Vol. 4, Nos. 2–3, pp.144–150.