Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 2852 – 2856

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineering and Information Science

Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments

Dawei Sun[a,*], Guiran Chang[b], Lina Sun[a] and Xingwei Wang[a]

[a]*School of Information Science and Engineering, Northeastern University, Shenyang, 110819, P.R. China,*
[b]*Computing Center, Northeastern University, Shenyang, 110819, P.R. China*

Abstract

Cloud computing is still in its infancy in spite of gaining tremendous momentum recently, high security is one of the major obstacles for opening up the new era of the long dreamed vision of computing as a utility. As the sensitive applications and data are moved into the cloud data centers, run on virtual computing resources in the form of virtual machine. This unique attributes, however, poses many novel tangible and intangible security challenges. It might be difficult to track the security issue in cloud computing environments. So this paper primarily aims to highlight the major security, privacy and trust issues in current existing cloud computing environments and help users recognize the tangible and intangible threats associated with their uses, which includes: (a) surveying the most relevant security, privacy and trust issues that pose threats in current existing cloud computing environments; and (b) analyzing the way that may be addressed to eliminate these potential privacy, security and trust threats, and providing a high secure, trustworthy, and dependable cloud computing environment. In the near future, we will further analysis and evaluate privacy, security and trust issues in cloud computing environment by a quantifiable approach, further develop and deploy a complete security, privacy trust evaluation, management framework on really cloud computing environments.

Selection and/or peer-review under responsibility of [CEIS 2011]

Keywords: privacy; security; trust; issue; threat; cloud computing

* Corresponding author. Tel.: +86-24-8368-2602.
E-mail address: sundaweicn@163.com.

doi:10.1016/j.proeng.2011.08.537

1. Introduction

Cloud computing, the long-held dream of "computing as a utility", has opening up the new era of future computing, transform a large part of IT industry, reshape the purchase and use of IT software and hardware, and receive considerable attention from global and local IT players, national governments, and international agencies [1] [2] [3] [4]. Cloud computing is a large-scale distributed computing paradigm driven by economies of scale, in which a pool of abstracted, virtualized, dynamically-scalable, highly available, and configurable and reconfigurable computing resources can be rapidly provisioned and released with minimal management effort in the data centers. Services are delivered on demand to external customers over high-speed Internet with the "X as a service (XasS)" computing architecture, which is broken down into three segments: "applications", "platforms", and "infrastructure". Its aims [3] [4] are to provide users with more flexible services, more scalable computing applications, storage and platforms in a transparent manner. Similarly, IT companies with innovative ideas for new application services are no longer required to make large capital outlays in the hardware and software infrastructures. By using cloud computing platform, they can register necessary service from the Internet and are free from the trivial task of setting up basic hardware and software infrastructures, which allow them to focus on the core aspects of their business.

High security is one of the major obstacles for opening up the new era of long dreamed vision of computing as a utility. As the sensitive applications and data are moved into the cloud data centers, run on virtual computing resources in the form of virtual machine. This unique attributes, however, poses many novel tangible and intangible security challenges [5] [6] such as accessibility vulnerabilities, virtualization vulnerabilities, and web application vulnerabilities. These challenges relate to cloud server having physical control of data, relate to identity and credential management, relate to data verification, tempering, integrity, confidentiality, data loss and theft. To protect private and sensitive data that are processed in data centers, the cloud user needs to verify (a) the real exists of the cloud computing environment in the world; (b) the security of information in the cloud; and (c) the trustworthiness of the systems in cloud computing environment. However, the management of data and services are not secure and trustworthy in cloud data centers.

This paper primarily aims to highlight the major security, privacy and trust issues in current existing cloud computing environments and help users recognize the tangible and intangible threats associated with their uses. Our contributions can be summarized as: (a) surveying the most relevant privacy, security and trust issues that pose threats in current existing cloud computing environments; and (b) analyzing the way that may be addressed to eliminate these potential security, privacy and trust threats, and providing a high secure, trustworthy, and dependable cloud computing environment.

The remainder of this paper is organized as follows. Section 2 presents security issues and addressing in cloud computing environments. Section 3 presents privacy issues and addressing in cloud computing environments. Section 4 presents trust issues and addressing in cloud computing environments. Finally, conclusions and a direction for future work are given in section 5.

2. Security Issues

Security is viewed as a composite notion, namely "the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of the unauthorized withholding of information" [13]. Security is the absence of unauthorized access to, or handling of, the system state. The main dimensions of security are availability, confidentiality and integrity. Security is one of the most obstacles for opening up the new era of the long dreamed vision of computing as a utility.

Security issues in cloud computing environments can be divided into six sub-categories [5] [6] [7] [11] [14], which include: (a) how to provide safety mechanisms, so that to monitor or trace the cloud server, (b) how to keep data confidentiality for all the individual and sensitive information, (c) how to avoid malicious insiders illegal operation under the general lack of transparency into provider process and procedure environments, (d) how to avoid service hijacking, where phishing, fraud and exploitation are well known issues in IT, (e) how to management multi-instance in multi-tenancy virtual environments, which assume all instance are completely isolated from each other. However, this assumption can sometime break down, allowing attackers to cross virtual machines side channel, escape the boundaries of the sandboxed environment and have full access to the host, and (f) how to develop appropriate law and implement legal jurisdiction, so that users have a chain against their providers if need.

3. Privacy Issues

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively, and it is include [15]: (a) when: a subject may be more concerned about her current or future information being revealed than information from the past, (b) how: a user may be comfortable if friends can manually request his information, but may not want alerts sent automatically, (c) extent: a user may rather have her information reported as an ambiguous region rather than a precise point. In the commercial, consumer context and privacy needs the protection and appropriate use of the information about customers and meeting the expectations of customers about its use. In the organizations, privacy entails the application of laws, mechanisms, standards and processes by which personally identifiable information is managed [8].

The privacy issues differ according to different cloud scenario, and can be divided into four sub-categories [5] [6] [8], which include: (a) how to make users remain control over their data when it is stored and processed in cloud, and avoid theft, nefarious use and unauthorized resale, (b) how to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is an usually choice, and avoid data loss, leakage and unauthorized modification or fabrication, (c) which party is responsible for ensuring legal requirements for personal information, and (d) what extent cloud sub-contractors involved in processing can be properly identified, checked and ascertained.

4. Trust Issues

Trust is viewed as a measurable belief that utilizes experience, to make trustworthy decisions. It is originally used in social science in constructing human beings' relationship and is now an essential substitute for forming security mechanism in distributed computing environments, as trust has many soft security attributes, such as, reliability, dependability, confidence, honest, belief, trustfulness, security, competence, and suchlike. In fact, trust is the most complex relationship among entities because it is extremely subjective, context-dependent, non-symmetric, uncertain, and partially transitive [9] [10]. Trust evaluation is a multi-faceted and multi-phased phenomenon based on multi-dimensional factors and trust evaluation cycle, and it is used to find the answer to the question "With which node(s) should I interact and with which I should not?" A measurable trust view is adapted by [16], "Trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context (in relation to service X)." Another mathematical trust view is given in [17], "Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action

(or independently or his capacity ever be able to monitor it) and in a context in which it affects his own action."

To protect clouds, traditional hard security techniques such as encryption and authorization provide a solid foundation, but they fail when cooperating entities act maliciously due to scale and temporary nature of collaborations. Trust as a soft social security philosophy can fight against such security threats by restricting malicious entities from participating in interactions and consequently offers a high trustworthiness cloud computing environment.

Trust issues in cloud computing environments can be divided into four sub-categories [5] [6] [8] [12], which include: (a) how to definition and evaluation trust according to the unique attribute of cloud computing environments, (b) how to handle malicious recommend information, which is very important in cloud computing environments, as trust relationship in clouds is temporary and dynamic, (c) how to consider and provide difference security level of service according to the trust degree, (d) how to manage trust degree change with interaction time and context, and to monitor, adjust, and really reflect trust relationship dynamic change with time and space.

5. Conclusions and Future Work

High security is one of the major obstacles for opening up the new era of the long dreamed vision of computing as a utility. As the sensitive applications and data are moved into the cloud data centers, run on virtual computing resources in the form of virtual machine. This unique attributes, however, poses many novel security challenges such as accessibility vulnerabilities, virtualization vulnerabilities, and web application vulnerabilities. With advancement of cloud computing and increasing number of cloud user, security, privacy and trust dimensions will continuously increase. To protect private and sensitive data that are processed in data centers, the cloud user needs to verify (a) the real exists of the cloud computing environment in the world; (c) the security of information in the cloud; and (b) the trustworthiness of the systems in cloud computing environment.

In this paper, we primarily aims to highlight the major security, privacy and trust issues in current existing cloud computing environments and help users recognize the tangible and intangible threats associated with their uses. We cover two main aspects of security, privacy and trust issues, which include: (a) surveying the most relevant privacy, security and trust issues that pose threats in current existing cloud computing environments, and (b) analyzing the way that may be addressed to eliminate these potential security, privacy and trust threats, and providing a high secure, trustworthy, and dependable cloud computing environment.

Future works will focus on the following: (a) analyzing and evaluating privacy, security and trust issues in cloud computing environment by a quantifiable approach, the surveying and analyzing approach method suggested in this paper is a first step toward analyzing privacy, security and trust issues, (b) developing a complete security, privacy trust evaluation, management framework as a part of cloud computing services to satisfy the security demands; and (c) deploying the framework on really cloud computing environments.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No. 61070162, No. 71071028, No. 60802023 and No. 70931001; the Specialized Research Fund for the Doctoral Program of Higher Education under Grant No. 20100042110025 and No. 20070145017; the

Fundamental Research Funds for the Central Universities under Grant No. N100604012, No. N090504003 and No. N090504006. The authors gratefully thank Junling Hu for her help and comments.

References

[1] Foster I, Zhao Y, Raicu I, Lu, S. Cloud Computing and Grid Computing 360-degree compared. *Proceedings of the Grid Computing Environments Workshop, GCE 2008*; IEEE Press, Nov. 2008, 1-10.

[2] Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*; 2009;**25(6)**:599–616.

[3] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A View of Cloud Computing. *Communications of the ACM*; 2010;**53(4)**:50–58.

[4] Mell P, Grance T. The NIST Definition of Cloud Computing. *Communications of the ACM*; 2010;**53(6)**:50.

[5] Paquette S, Jaeger P T, Wilson S C. Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*; 2010;**27(3)**:245–253.

[6] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*; 2011;**34(1)**:1–11.

[7] Vaquero L M, Rodero-Merino L, Morán D. Locking the sky: A survey on IaaS cloud security. *Computing*; 2011;**91(1)**:93–118.

[8] Pearson S, Benameur A. Privacy, security and trust issues arising from cloud computing. *Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010*; IEEE Press, Nov. 2010, 693-702.

[9] Ahamed S I, Haque M M, Endadul Hoque M, Rahman F, Talukder N. Design, analysis, and deployment of omnipresent formal trust model (FTM) with trust bootstrapping for pervasive environments. *Journal of Systems and Software*; 2010;**83(2)**:253–270.

[10] Karaoglanoglou K, Karatza H. Resource discovery in a Grid system: Directing requests to trustworthy virtual organizations based on global trust values. *Journal of Systems and Software*; 2011;**84(3)**:465–478.

[11] Takabi H, Joshi J B D, Ahn G. Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*; 2010;**8(6)**:24–31.

[12] Sangroya A, Kumar S, Dhok J, Varma V. Towards analyzing data security risks in cloud computing environments. *Communications in Computer and Information Science*; 2010;**54**:255–265.

[13] Algirdas A, Jean-Claude L, Brian R, Carl L. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*; 2004;**1(1)**:11–33.

[14] Tchifilionova V. Security and privacy implications of cloud computing - Lost in the cloud. *Proceedings of the IFIP WG 11.4 International Workshop on Open Research Problems in Network Security, iNetSec 2010*; Springer Verlag Press, Mar. 2010, 149-158.

[15] Krumm J. A survey of computational location privacy. *Personal and Ubiquitous Computing*; 2009;**13(6)**:291–399.

[16] Shekarpour S, Katebi S D. Modeling and evaluation of trust with an extension in semantic web. *Journal of Web Semantics*; 2010;**8(1)**:26–36.

[17] Iltaf N, Hussain M, Kamran F. A mathematical approach towards trust based security in pervasive computing environment. *Proceedings of the Third International Conference and Workshops, ISA 2009*; IEEE Press, Jun. 2009, 702-711.