2014 Sixth International Conference on Measuring Technology and Mechatronics Automation

Data Security: the Challenges of Cloud Computing

Hu Shuijing

Shanghai University of Political Science and Law, Shanghai, 201701 China
husj_12@163.com

***Abstract*—Cloud computing is the fundamental change happening in the field of Information Technology. It is a representation of a movement towards the intensive, large scale specialization. On the other hand, it brings about not only convenience and efficiency problems, but also great challenges in the field of data security and privacy protection. Currently, security has been regarded as one of the greatest problems in the development of Cloud Computing. This paper describes the great requirements in Cloud Computing, such as security key technology, standard and regulation etc., and discusses ways in which they may be addressed.**

Keywords- Cloud Computing; Data Security; Encryption; Access Control

I. INTRODUCTION

In early 2011, China announced plans to build a "city-sized cloud computing and office complex that will include a mega data center," signaling a rapid growth in information technology (IT) spending. As the world becomes increasingly digitalized, concerns arise about the security and privacy of personal and commercial information. This information is being steadily moved to "the cloud," an Internet-based service that "provides consumers with vast amounts of cheap, redundant storage and allows them to instantly access their data from a web-connected computer anywhere in the world." However, this convenience comes with risks such as exposure to hackers and privacy invasion.

II. CLOUD COMPUTING FUNDAMENTALS

A. Defining Cloud Computing

The term "cloud computing" has become popular and trendy, but there are many concepts behind this idea. On a general level, "cloud" is used as a metaphor for the "ethereal Internet" and the virtual platform that it provides. Some view cloud computing abstractly as the result of the convergence of computing and communications, or more practically as a "scalable network of servers," as "IT as a service," or as the convenience of being able to access a shared pool of computing resources over a network like the World Wide Web.

Although there is no definitive definition for cloud computing, a definition that is commonly accepted is provided by the United States National Institute of Standards and Technologies (NIST):"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

B. Advantages and Disadvantages of Cloud Computing

Advantages of the cloud paradigm include data preservation, high levels of expertise on the part of cloud service providers, scalability, affordability, and availability. Additionally, some studies have shown that businesses that adopt SaaS enjoy a return-on-investment of almost 600%. Cloud providers are benefited because they have control over content, can set access terms, and can also monitor usage statistics. These additional advantages for cloud providers also make cloud services attractive to copyright holders because the control exercised by the cloud provider can provide additional security and protect the copyright holder from infringement.

There are also many disadvantages to the cloud paradigm, and many of these disadvantages arise in part because of consumers' loss of control over data. Because consumers are entrusting their data to a third party, they are relying on that third party to adequately secure the information, have the services and data available at all times, and allow the consumer to move their information between providers freely, all in a context in which it is unclear how modern privacy law (including the Fourth Amendment and laws related to confidentiality) may apply. Another disadvantage is related to the risk of loss. If a provider fails to secure data and a consumer's information is compromised, the risk of loss is likely to fall on the consumer rather than the cloud service provider.

III. DATA SECURITY ISSUES FOR CLOUD COMPUTING

Data security risks are compounded by the open nature of cloud computing. Access control becomes a much more fundamental issue in cloud-based systems because of the accessibility of the data therein. If you use a system that provides improved accessibility and opens up the platform to multi-node access, then you need to take into account the risks associated with this improvement. One way this can be done is by adding an element of control, in the form of access control, to afford a degree of risk mitigation. Information-centric access control (as opposed to access control lists) can help to balance improved accessibility with risk, by associating access rules with different data objects within an open and accessible platform, without losing the inherent usability of that platform. Here we discuss some of these key security challenges:

Data Location

978-1-4799-3435-5/14 $31.00 © 2014 IEEE
DOI 10.1109/ICMTMA.2014.52

In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. Some service providers also take advantage of their global datacenters. However, in some cases applications and data might be stored in countries, which can judiciary concerns. For example, if the user data is stored in XX country then service providers will be subjected to the security requirementsand legal obligations of XX country. This may also happen that a user does nothave the information of these issues.

Unwanted Access

Cloud computing may actually increase the risk of access to confidential information. First, this may be by foreign governments: there can be increased risks due to government surveillance over data stored in the cloud, as the data may be stored in countries where previously it was not. Governments in the countries where the data is processed or stored may even have legal rights to view the data under some circumstances, and consumers may not be notified if this happens. Second, as with other computing models, there is an underlying risk of unauthorized access that may be exacerbated if entities are involved in the provider chain that have inadequate security mechanisms in place. In general, cloud storage can be more at risk from malicious behavior

than processing in the cloud, because data may remain in the cloud for long periods of time and so the exposure time is much greater。

Data Segregation

Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data.

Vendor Lock-In

So far， Cloud computing is still no interoperability standards. The lack of standards makes it difficult to establish security frameworks for heterogeneous environments and forces people for the moment to rely on common security best practice. As there is no standardized communication between and within cloud providers and no standardized data export format, it is difficult to migrate from one cloud provider to another or bring back data and process it in-house.

Data Remanence

Another major data issue for cloud is how to be sure that data that should be deleted really are deleted and are not recoverable by a cloud service provider (CSP). There are currently no ways to prove this as it relies on trust, and the problem is exacerbated in cloud because there can be many copies of the data (potentially held by different entities and some of which may not be available) or because it might not be possible to destroy a disk since it is storing other customers' data. The risks of data exposure vary according to the service model. Using IaaS or PaaS, one or more VMs are created in order for a program to be run within those – when the task is finished, the VMs and the temporary diskspace are released. In fact, IaaS providers can provide storage and VM services which are complementary but allow for persistency of data between usage of multiple VMs. An allocated VM could be started to carry out a task and stopped once the task is completed; this is logically separate from managing the lifecycle of a VM (as the VM can be deleted when the data are no longer needed). Using a SaaS approach, on the other hand, the customer is one of the users of a multi-tenant application developed by the cloud service provider, and the customers' data is stored in the cloud, to be accessible the next time the customer logs in. The data would only be deleted at the end of the lifecycle of the data, if the customer wishes to change service provider, etc. There is a correspondingly higher risk to the customer if hardware resources are reused than if dedicated hardware is used.

There are a number of data security issues for cloud, and these depend upon the service provision and deployment models. A number of open issues remain, including monitoring, transparency, and audit etc.

IV. DATA SECURITY MITIGATION

This section will presents a brief overview of solutions and research in progress that aim to help address the concern of data security in the cloud.

A. Encryption

At present the primary means of data security mitigation at this time is encryption. There has been some discussion in recent years about alternative data protection techniques; for example, in connection with the Data Accountability and Trust Act, reported in May 2006. These alternative techniques included indexing, masking, redaction, and truncation. However, there are no accepted standards for indexing, masking, redaction, or truncation—or any other data protection technique. The only data protection technique for which there are recognized standards is encryption. Not all encryption algorithms are created equal. Cryptographically, many algorithms provide insufficient security. Only algorithms that have been publicly vetted by a formal standards body (e.g., NIST) or at least informally by the cryptographic community should be used. Any algorithm that is proprietary should absolutely be avoided. We are talking about symmetric encryption algorithms here. Symmetric encryption involves the use of a single secret key for both the encryption and decryption of data.(See Figure 1) For symmetric encryption, the longer the key length, the stronger the encryption. Although long key lengths provide more protection, they are also more computationally intensive, and may strain the capabilities of computer processors. The usual practice is that key lengths should be a minimum of 112 bits for Triple DES (Data Encryption Standard) and 128 bits for AES.

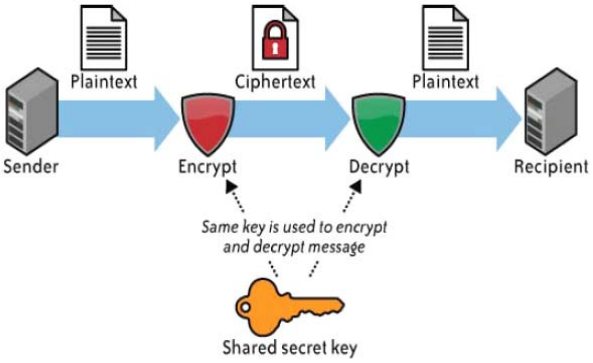

Figure 1. Symmetric encryption

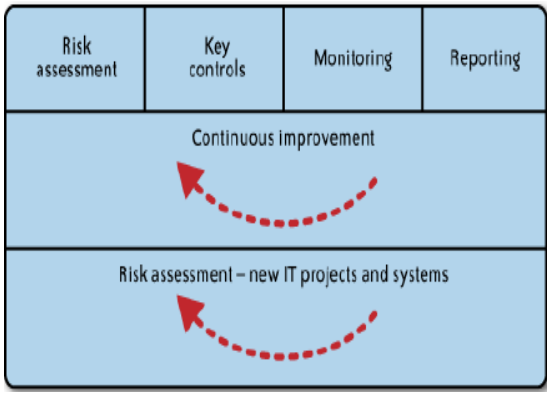

Figure 2. Security model

B. *Access Control*

For the data security risks, the first issue we have to concern is what access control exists to protect the data? Access control consists of both authentication and authorization. CSPs generally use weak authentication mechanisms (e.g., username + password), and the authorization ("access") controls available to users tend to be quite coarse and not very granular. In contrast to network-based access control, user access control should be strongly emphasized in the cloud, since it can strongly bind a user's identity to the resources in the cloud and will help with fine granular access control, user accounting, support for compliance, and data protection. User access management controls, including strong authentication, single sign-on (SSO), privilege management, and logging and monitoring of cloud resources, play a significant role in protecting the confidentiality and integrity of your information in the cloud. ISO/IEC 27002 has defined six access control objectives that cover end user, privileged user, network, application, and information access control. The following access management control statement from ISO 27002 is particularly relevant to cloud services: To ensure authorized user access and to prevent unauthorized access to information systems. Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

C. *Innovative Regulatory Frameworks*

The cloud service providers (CSPs) are typically challenged to meet the requirements of client. To build a security model(See Figure2), it is essential that the CSP establish a strong foundation of controls that can be applied to all of its clients.

Key procedures of this approach include:

1) *Risk assessment*

This approach begins with an assessment of the risks that face the CSP and identification of the specific compliance regimes/requirements that are applicable to the CSP's services. The CSP should address risks associated with key areas such as appropriate user authentication mechanisms for accessing the cloud, encryption of sensitive data and associated key management controls, logical separation of customers' data, and CSP administrative access.

2) *Key controls*

Key controls are then identified and documented to address the identified risks and compliance requirements. These key controls are captured in a unified control set that is designed to meet the requirements of the CSP's customers and other external requirements. The CSP drives compliance activities based on its key controls rather than disparate sets of externally generated compliance requirements.

3) *Monitoring*

Monitoring and testing processes are defined and executed on an ongoing basis for key controls. Gaps requiring remediation are identified with remediation progress tracked. The results of ongoing monitoring activities may also be used to support any required external audits. Refer to "Auditing the Cloud for Compliance" on page 194 for a discussion of external audit approaches.

4) *Reporting*

Metrics and key performance indicators (KPIs) are defined and reported on an ongoing basis. Reports of control effectiveness and trending are made available to CSP management and external customers, as appropriate.

5) *Continuous improvement*

Management improves its controls over time—acting swiftly to address any significantgaps identified during the course of monitoring and taking advantage of opportunities to improve processes and controls.

6) *Risk assessment—new IT projects and systems*

The CSP performs a risk assessment as new IT projects, systems, and services are developed to identify new risks and requirements, to assess the impact on the CSP's current controls, and to determine whether additional or modified controls and monitoring processes are needed. The CSP also performs an assessment when considering entry into a new industry or market or taking on a major new client with unique control requirements.

V. CONCLUSIONS

In this paper we have assessed some of the key data security issues involved in moving to cloud scenarios, and set out the basis of some approaches that address the situation. We discussed a number of mechanisms that illustrate promising approaches addressing the data security considered above. This paper argues, encryption, access control, and strengthening management are effective measures to reduce security risks. Given the economic considerations of cloud computing today, as well as the present limits of cryptography, CSPs are not offering robust enough controls around data security. It may be that those economics change and that providers offer their current services, as well as a "regulatory cloud environment" (i.e., an environment where customers are willing to pay more for enhanced security controls to properly handle sensitive and regulated data). Currently, the best viable option for mitigation is to ensure that any sensitive or regulated data may be not put into a public cloud.

VI. ACKNOWLEDGEMENTS

This research was supported by the Special Fund of Shanghai Outstanding Young Teachers (Study on the Intellectual Property Risk in the Undertaking Service Offshore Outsourcing. shzf010) and the Young Project of SHUPL (QK2012004).

REFERENCES

[1] Dhar S. From outsourcing to Cloud computing: evolution of IT services [J]. Management Research Review, 2012, 35(8): 664-675.

[2] Armbrust M, Fox A, Griffith R, et al. A view of cloud computing [J]. Communications of the ACM, 2010, 53(4): 50-58.

[3] Low C, Chen Y, Wu M. Understanding the determinants of cloud computing adoption [J]. Industrial management & data systems, 2011, 111(7): 1006-1023.

[4] Bradshaw S, Millard C, Walden I. Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services [J]. International Journal of Law and Information Technology, 2011, 19(3): 187-223.

[5] Cervone H F. An overview of virtual and cloud computing [J]. OCLC Systems & Services, 2010, 26(3): 162-165.

[6] Joint A, Baker E. Knowing the past to understand the present–issues in the contracting for cloud based services [J]. Computer Law & Security Review, 2011, 27(4): 407-415.

[7] Hamlen K W, Thuraisingham B. Data security services, solutions and standards for outsourcing [J]. Computer Standards & Interfaces, 2012.

[8] Ferrer A J, Hernández F, Tordsson J, et al. OPTIMIS: A holistic approach to cloud service provisioning [J]. Future Generation Computer Systems, 2012, 28(1): 66-77.