Cloud Computing Security Challenges and Critical Technologies of Its Protection

Yuxing Yang

Computer and Science Department, Yunyang Teachers' College, Shiyan 442000, China

43967125@163.com

Keywords: Cloud Computing, Data, Security Challenges, Security Protection

Abstract. In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. With the continuous evolution of global information processes, cloud computing has become a new Internet service model following distributed computing, parallel computing and grid computing and it has attracted widespread concern from the industry and the government. Starting from the concept and development status of cloud computing, this paper proposes the connotation and two forms of cloud computing security with respect to services and data analysis, then it makes an in-depth analysis of the cloud computing security challenges encountered in the development process, and presents the critical technologies of security protection including data backup strategy, data partial encryption scheme and module design at last.

Introduction

Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. Cloud computing is an innovative Information System (IS) architecture, visualized as what may be the future of computing, a driving force demanding from its audience to rethink their understanding of operating systems, client-server architectures, and browsers. Cloud computing has leveraged users from hardware requirements, while reducing overall client side requirements and complexity. The cloud computing paradigm is still evolving, but has recently gained tremendous momentum. However, security and privacy issues pose as the key roadblock to its fast adoption. With the era advent of cloud computing, the Internet will always release massive amounts of data. A large number of economic and political interests are hidden behind the large amounts of data, particularly through data integration, analysis and mining, the power of data integration and control they exhibit has been far more than ever before. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market.

Essentially securing an Information System (IS), involves identifying unique threats and challenges which need to be addressed by implementing the appropriate countermeasures. Cloud computing due to its architectural design and characteristics imposes a number of security benefits, which include centralization of security, data and process segmentation, redundancy and high availability. While many traditional risks are countered effectively, due to the infrastructures singular characteristics, a number of distinctive security challenges are introduced.

Currently, the world's leading cloud services providers have developed cloud platform security policy, and attach great importance to national cloud computing security issues. To ensure the safety of government cloud computing applications, the United States introduced federal cloud computing security strategy to speed up the development of specific cloud computing security control requirements, to implement the Federal risk and authorization management Program. In recent years, the Chinese government and industry become increasingly concerned about cloud computing applications and it is more and more important to ensure the security of cloud computing.

Cloud computing security

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues. But as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. International Data Corporation (IDC) conducted a survey (see Fig.1.) of 263 IT executives and their line-of business colleagues to gauge their opinions and understand their companies' use of IT cloud services. Security ranked first as the greatest issue of cloud computing.

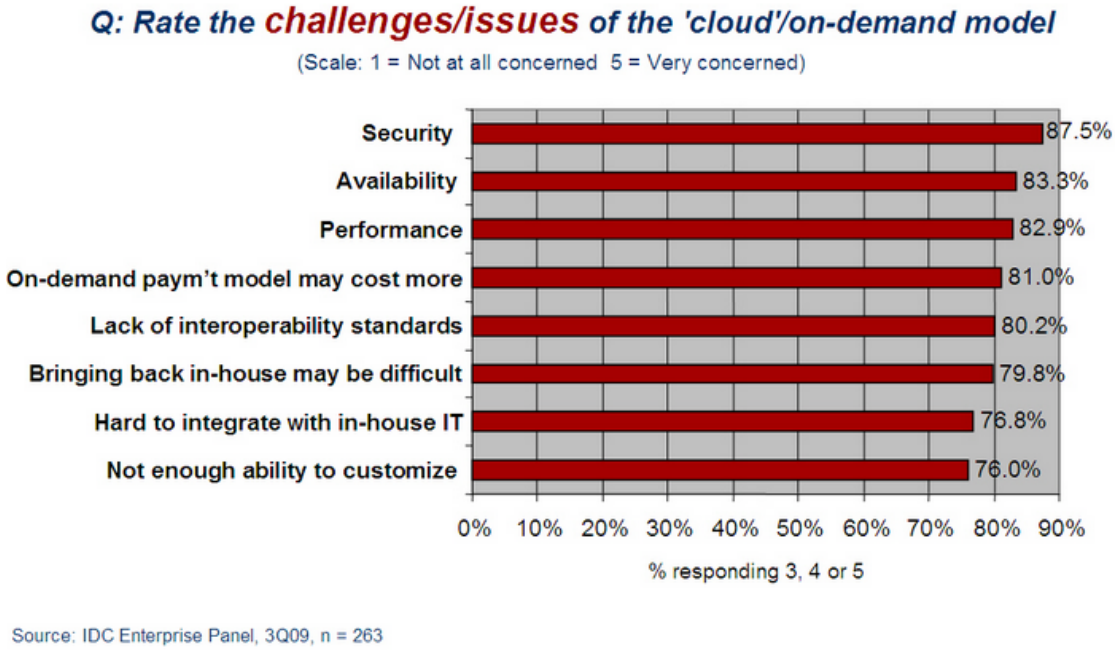

Fig.1 Results of IDC ranking security challenges

Cloud computing security mainly includes the following two forms: trust and security identification of threats, which will be discussed in detail next.

Trust. The concept of trust, adjusted to the case of two parties involved in a transaction, can be described as follows: ''An entity A is considered to trust another entity B when entity A believes that entity B will behave exactly as expected and required''. Trust in a cloud environment depends heavily on the selected deployment model, as governance of data and applications is outsourced and delegated out of the owner's strict control. In traditional architectures, trust was enforced by an efficient security policy, which addressed constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people. Security identification of threats.

Most importantly the cloud environment deteriorates the perception of perimeter security. Perimeter security is a set of physical and programmatic security policies that provide levels of protection on a conceptual borderline against remote malicious activity. In a cloud computing model, the perimeter becomes fuzzy, weakening the effectiveness of this measure. The emergence of cloud service models is expected to lead to a deconstruction of the application services as they are already delivered in existing "closed" service provisioning environments. From the traditional viewpoint of perimeter security, the cloud appears outside the trust borderline and should be viewed with suspicion, but this adversely leads to not trusting essential business processes and services that have been outsourced.

Security identification of threats. Cloud computing in its quintessence, has the capability to address a number of identified deficiencies of traditional architectures due to its unique characteristics, but the adoption of this innovative architecture may introduce a number of additional uncategorized threats, which can be seen in Fig.2.

Fig.2 Classification of threats

In general, security is related to the significant aspects of confidentiality, integrity and availability; they thus become building blocks to be used in designing secure systems. These important aspects of security, apply to the three broad categories of assets which are necessary to be secured, data, software and hardware resources. The cloud infrastructure proposes unique security challenges which need to be considered in detail.

Confidentiality refers to only authorized parties or systems having the ability to access protected data. The threat of data compromise increases in the cloud, due to the increased number of parties, devices and applications involved, that leads to an increase in the number of points of access. Privacy is the desire of a person to control the disclosure of personal information. Organizations dealing with personal data are required to obey to a country's legal framework that ensures appropriate privacy and confidentiality protection. The cloud presents a number of legal challenges towards privacy issues involved in data stored in multiple locations in the cloud, additionally increasing the risk of confidentiality and privacy breaches.

Integrity means that assets can be modified only by authorized parties or in authorized ways and refers to data, software and hardware. A cloud computing provider is trusted to maintain data integrity and accuracy. The cloud model presents a number of threats including sophisticated insider attacks on these data attributes.

Cloud computing security challenges

Though cloud computing is targeted to provide better utilization of resources using virtualization techniques and to take up much of the work load from the client, it is fraught with security risks. The complexity of security risks in a complete cloud environment is illustrated in Fig.3. The lower layer represents the different deployment models of the cloud namely private, community, public and hybrid cloud deployment models. The layer just above the deployment layer represents the different delivery models that are utilized within a particular deployment model. These delivery models are the SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) delivery models. These delivery models form the core of the cloud and they exhibit certain characteristics like on-demand self-service, multi-tenancy, ubiquitous network, measured service and rapid elasticity which are shown in the top layer.

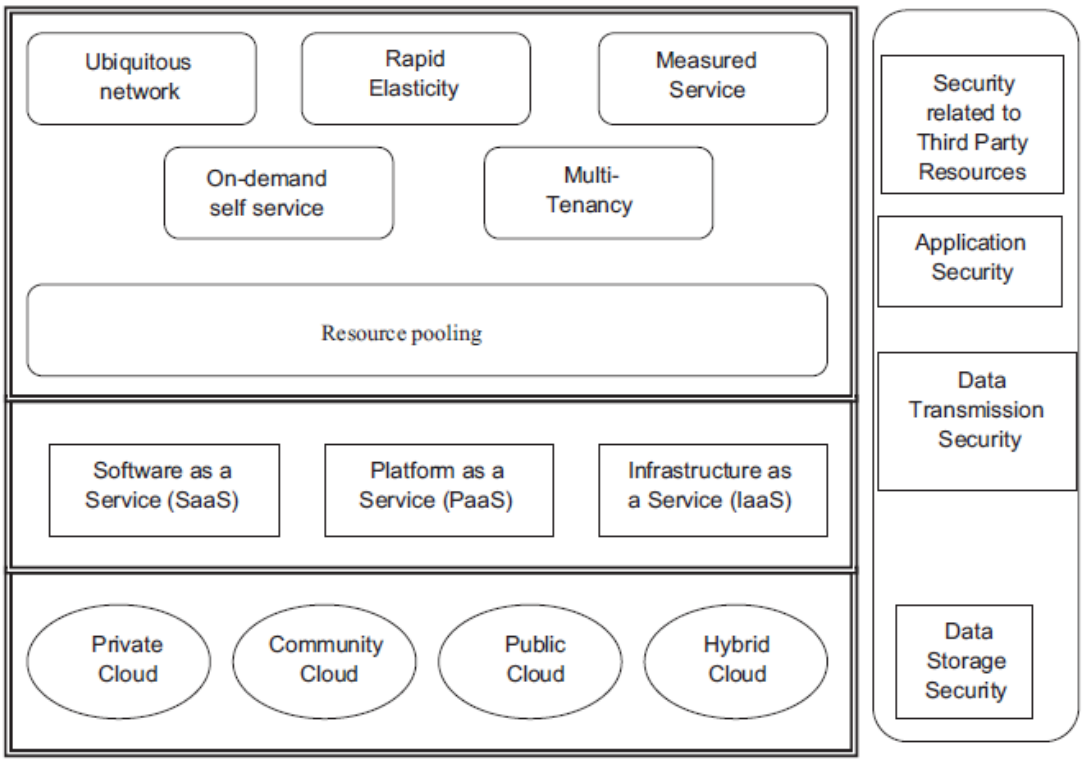

Fig.3 Complexity of security in cloud environment

Security challenges in SaaS. SaaS is the dominant cloud service model for the foreseeable future and the area where the most critical need for security practices and oversight will reside. In SaaS, the client has to rely on the provider for proper security measures. The provider must do the work to keep multiple users' from seeing each other's data. So it becomes difficult to the user to ensure that right security measures are in place and also difficult to get assurance that the application will be available when needed. The following key security elements should be carefully considered as an integral part of the SaaS application development and deployment process:

- ✧ Data security
- ✧ Network security
- ✧ Data locality
- ✧ Data integrity
- ✧ Data segregation
- ✧ Data access
- ✧ Authentication and authorization
- ✧ Data confidentiality
- ✧ Web application security
- ✧ Data breaches
- ✧ Virtualization vulnerability
- ✧ Availability
- ✧ Backup
- ✧ Identity management and sign-on process

Security challenges in PaaS. In PaaS, the provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider and the provider has to offer strong assurances that the data remains inaccessible between applications. PaaS is intended to enable developers to build their own applications on top of the platform. As a result it tends to be more extensible than SaaS, at the expense of customer-ready features. This tradeoff extends to security features and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security.

Security challenges in IaaS. With IaaS the developer has better control over the security as long

as there is no security hole in the virtualization manager. Also, though in theory virtual machines might be able to address these issues but in practice there are plenty of security problems. Due to the growing virtualization of 'everything' in information society, retaining the ultimate control over data to the owner of data regardless of its physical location will become a topic of utmost interest. IaaS is prone to various degrees of security issues based on the cloud deployment model through which it is being delivered. Public cloud poses the major risk whereas private cloud seems to have lesser impact. The complexity involved in IaaS due to each of the service deployment models is illustrated in Table 1.

Table 1 Cloud service deployment model

	Infrastructure management	Infrastructure ownership	Infrastructure location	Access and consumption
Public cloud	Third-party provider	Third-party provider	Off-premise	Untrusted
Private/community cloud	Organization or third-party provider	Organization or third-party provider	On-premise or off-premise	Trusted
Hybrid cloud	Both organization and third-party provider	Both organization and third-party provider	Both on-premise and off- premise	Trusted and untrusted

In a cloud, the risks are overwhelmingly high, which is because of cloud computing's vulnerability and the asset value of the resources and their nature of them residing together. Measures should be taken to make the cloud environment safe, private and isolated in the Internet to avoid being attacked by cyber criminals.

Critical technologies of security protection

Several groups and organization are interested in developing security solutions and standards for the cloud. The Cloud Security Alliance (CSA) is gathering solution providers, non- profits and individuals to enter into discussion about the current and future best practices for information assurance in the cloud. The Cloud Standards web site is collecting and coordinating information about cloud-related standards, and the Open Web Application Security Project (OWASP) maintains list of top vulnerabilities to cloud-based or SaaS models and so on. Generally, there are mainly several critical technologies of cloud computing security protection.

The first is data backup strategy. Portability of mobile devices is one of the reasons why the majority of users love them, but it is for this reason that they will likely be damaged by external forces in the course of use. In that case, it may be impossible for the recovery of user data, so it is necessary for data backup of mobile devices. Users can upload important data to the cloud server, however, cloud server is not absolutely secure. Different types of cloud server may be highly reliable data distribution center or an old private PC, so only one data backup program is unscientific.

The second is data partial encryption scheme. This paper proposes a method that with the form of a direct stream of bytes, the data stream is cut into fixed-size blocks, and after processing it into its matrix and getting the initial chaos of the original data, then transformation parameters are generated randomly. The data out of order is processed in a certain way, after quantization, parameters will also be generated randomly, and we select part of the data for the symmetric encryption to get confusion data. Without large-scale encryption, users can set their own encrypted data percentage to the total number without separate storage of encrypted data in order to increase the degree of chaos. When the data is stored, hybrid of plain text and ciphertext can be used, so there is the need that the parameters and encryption key should have secondary encrypt to compose data packets with plaintext and ciphertext.

The third is module design. Cloud computing data encryption based on matrix disorder is divided into four cores consisting of data block and formatting, data disorder, encrypted part selection, file storage format. Wherein the data block and formatting refers that the data is cut into fixed-size

blocks in formatted way, to facilitate the input of the next module. Data disorder refers to transforming data reversible matrix to achieve the purpose of scrambling information. Encryption section means using AES algorithm to encrypt data at different locations to compose new file storage format mixed with the hybrid ciphertext and ciphertext mark text.

Summary

As described in the paper, though there are extreme advantages in using a cloud-based system, there are yet many practical problems which have to be solved. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Service providers and data owners should be responsible for cloud computing security in a cloud environment, if data privacy is not up to the regulatory requirements, it may face unpredictable consequences. This paper outlines cloud computing security and the challenges it may encounter, and point out the critical technologies of its protection, which will provide great reference for further research.

Acknowledgements

This work was financially supported by the Natural Science Foundation of Yunyang Teachers′ College (2015A10).

References

[1] Y. Liu. Privacy Protection Method in the Era of Cloud Computing and Big Data//MATEC Web of Conferences. EDP Sciences, 2015, 22: 01041.

[2] D. Zissis and D. Lekkas. Addressing cloud computing security issues. Future Generation computer systems, 2012, 28(3): 583-592.

[3] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 2011, 34(1): 1-11.

[4] K. Tserpes, F. Aisopos, D. Kyriazis and T. Varvarigou, Service selection decision support in the Internet of services, in: Economics of Grids, Clouds, Systems, and Services, in: Lecture Notes in Computer Science, vol. 6296, 2010, pp. 16–33.

[5] J. Yang, H. H. Wang and J. Wang. Survey on Some Security Issues of Cloud Computing. Journal of Chinese Computer Systems, 2012, 33(3): 472-479. (In Chinese)

[6] K. Popović. Cloud computing security issues and challenges//MIPRO, 2010 proceedings of the 33rd international convention. IEEE, 2010: 344-349.

[7] W. Li. Study and exploration on cloud computing security. Telecom Engineering Technics and Standardization, 2012, 25(4): 44-49. (In Chinese)

[8] K. Bai. Analysis of data security protection technology based on cloud computing environment. Electronic Design Engineering, 2015, 23(10):149-151. (In Chinese)

[9] C. Liu. Simulations for orbital maintenance of low-angle satellite based on STK. Energy Education Science and Technology Part A: Energy Science and Research, 32 (6): 6307-6316.

[10] T. Mather, S. Kumaraswamy and S. Latif. Cloud security and privacy: an enterprise perspective on risks and compliance. “O'Reilly Media, Inc.”, 2009.