УДК 004.056.52
МРНТИ 81.93.29

SECURITY ISSUES IN CLOUD COMPUTING

ZH.M. TASHENOVA[1], SH. ORAZGALEYEVA[1], E.N. NURLYBAYEVA[2], SH.A. AMANZHOLOVA[3]

[1]L.N. Gumilyov Eurasian National University
[2]Kazakh National Academy of Arts named after T. Zhurgenov
[3]Kazakh National Conservatory named after Kurmangazy

Abstract: *Cloud computing is the result of the natural development of our everyday use of technology as a concept. Cloud computing has resulted in uplifting achievements in virtualization (eg. VMWare), increased computing with clusters of servers (eg. Google) and increased Internet access. Industry Leaders describe cloud computing as a supply of applications or IT services offered by a third-party (Rackspace, Microsoft, IBM) over the Internet. Recently, global economic downturn has provoked cloud computations, as organizations have sought to reduce their IT budget, which has allowed them to maintain productivity and profitability.*

Keywords: *computers, servers, clusters, Internet, network*

БҰЛТТЫ ЕСЕПТЕУЛЕРДЕГІ ҚАУІПСІЗДІК МӘСЕЛЕЛЕРІ

Аңдатпа: *Бұлттық есептеулер тұжырымдама ретінде ғаламтор арқылы ұсынылатын технологияларды пайдаланудың біздің күнделікті тәсіліміздің табиғи дамуының нәтижесі. Бұлттық есептеулер виртуалдау саласындағы жетістіктер (мысалы, VMWare), серверлер кластерлерімен бөлінген есептеулер (мысалы, Google) және ғаламторға кеңжолақты қатынау қолжетімділігін арттыру нәтижесінде алдыңғы сапқа шықты. Сала көшбасшылары бұлт есептеулерін үшінші тарап Интернет арқылы (Rackspace, Microsoft, IBM) ұсынатын қолданбаларды немесе АТ қызметтерін жеткізу ретінде сипаттайды.*

Түйінді сөздер: *есептеу машиналары, серверлер, ғаламтор, желі*

ПРОБЛЕМЫ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Аннотация: *Облачные вычисления привели к подъему достижений в области виртуализации (например, VMWare), расширению вычислений с кластерами серверов (например, Google) и расширению доступа в Интернет. Лидеры отрасли описывают облачные вычисления как набор приложений или ИТ-услуг, предлагаемых сторонними разработчиками (Rackspace, Microsoft, IBM) через Интернет. В последнее время глобальный экономический спад спровоцировал облачные вычисления, поскольку организации стремились сократить свой ИТ-бюджет, что позволило им поддерживать производительность и прибыльность.*

Ключевые слова: *вычислительные машины, серверы, кластеры, интернет, сети*

The National Institute of Standards and Technology defines cloud computing as follows: «cloud computing is a model that provides convenient network accessibility to the total pool of customized computing resources (for example, networks, servers, storage locations, applications, and services). This cloud model provides accessibility and consists of five main characteristics, three service models and four deployment models. « At present, cloud computing is characterized by the availability of flexible resources by means of a rental model.

It represents the sacred loyalty of computing technology, allowing the company to focus on its core business, paying for all IT resources as a service.

The description of the above cloud computing service models is as follows: in cloud computing, everything is provided as a service (XaaS), from testing and security to collaboration and metamoding. The cloud is quickly translated as «service». To date, the NIST contains three main types of services that are agreed and defined. They:

1. Software as the {SaaS} means the delivery of software through the Internet. This is the most popular cloud computing model. SaaS has been in place since the beginning of 2001, which is typically called an app service provider model (ASP). The software is a software that runs on the cloud infrastructure of the provider, which is delivered to customers (on demand) through a web-based Thin Client (such as a browser). Typical example - Google Docs and Salesforce. com CRM.

2. As a platform {PaaS} - it gives the client (developer) flexibility for creating (development, testing, deployment) applications on the provider's platform (API, warehousing and infrastructure). PaaS stakeholders include PaaS hosts that offer Infrastructure (servers, etc.), PaaS vendor, PaaS user development tools and platforms. PaaS examples are Microsoft Azure and Google AppEngine.

3. Infrastructure (IaaS), instead of buying servers and building a zero-data center, and, therefore, worries about what's going on when a website reaches million users, IaaS offers users flexible access to resources (networks, servers). service API. The base infrastructure is open to the end user, which controls the infrastructure and software running on the infrastructure. IaaS operates under a lease model that uses a pay-based payment method that allows users to pay only the resources they actually use.

Depending on the infrastructure, four cloud deployment models have been identified and each has its own advantages and disadvantages. Security issues will start here.

1. The public cloud is a traditional approach to cloud computing in everyday life. Usually it belongs to a large organization (for example, Amazon EC2, Google AppEngine and Microsoft Azure). The owner of the organization makes public accessible through the multiethnic model based on self-service offered on the Internet. The physical location of this provider's infrastructure usually crosses many national borders, as it is the most cost-effective way to bring considerable savings to the user, along with the privacy and security issues.

2. A private cloud is a cloud infrastructure in the middle of one customer. It differs from the traditional data center using virtualization. It can be managed by a third party, either inside or outside the hiring organization's or tenant's home. The private cloud is publicly accessible, but it is much more economical than the data processing center, as witnessed by Concur Technologies (ie $ 7 million in 3 years since 2009). The private cloud gives organizations much control over their data and resources. As a result, the private cloud will be attractive to businesses, especially those most relevant to security and safety.

3. The community cloud - according to NIST, a community refers to a cloud infrastructure that will be shared with multiple organizations within a particular community. They can manage any organization or a third party. A common example is the Open Cirrus Cloud Computing test bench, which is a set of federated data centers across six sites from North America to Asia.

4. Hybrid cloud - consists of any two (or all) combination of three of the three types described above. API standardization has led to the easy distribution of applications between different cloud models. This will allow you to use new models such as "Surge Computing", where emissions from workloads from private cloud to public accessible cloud.

The cloud model that provides access is composed of three service models and four deployment models where cloud computing issues are emerging.

Security has always been a major problem for horsemen when it comes to cloud technologies. In 2008 and 2009, IDC ranked first in the list

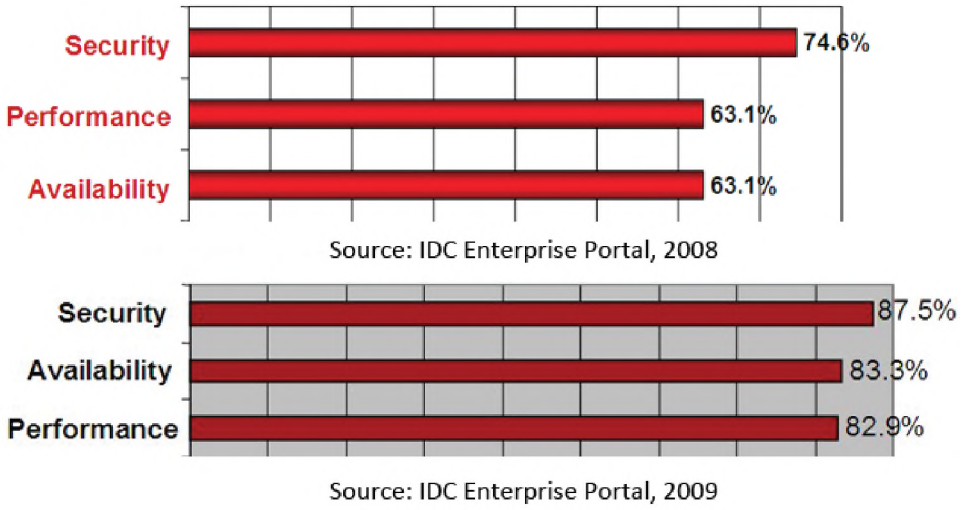

Figure 1 – The biggest 3 issues of cloud demand

of two surveys (see Figure 1). However, cloud computing is a combination of these technologies, operating systems, storage systems, networks, virtualization, each with security problems. For example, browsing attacks, attempts to deny servicing, and attacks on the network become threats to cloud computing. Opportunities for a new wave of large-scale attacks through the virtualization platform. "Fear of the Cloud" is characterized by the fact that security issues are addressed to three traditional issues: access and control of third party data.

Gartner research firm presented seven risks for resetting and allocating data from reset and long-term viability. The European Network and Information Security Agency has published a list of 35 cloud computations in 4 categories. Organizations such as ISACA and Cloud Security Alliance publish recommendations and best practices on cloud security issues.

Before getting more deeply into cloud computing, Nist v. It should be noted some advantages of cloud security as shown by Peter Mell and Tim Gren. Cloud computing companies can also provide a dedicated security group and spend more on security infrastructure. Other advantages include the rapid intelligent scalability of resources, standardized security interfaces, and the overall benefit of the scale (security measures are cheaper on a large scale). Some important security issues in cloud computing include:

1. Accessibility limits data accessibility when needed. This mission is one of the key tasks of organizations responsible for security. Accessibility problems relate to the need to move to another provider, the duration of the current provider's work, or the long term viability of the cloud provider. Some known issues with cloud computing are shown in Table 1.

Table 1-Cloud problems and time to resolve them

Cloud service	Output duration	Dates
Google Gmail	30 hours	Oct. 16-17, 2008
Google Gmail, Apps	24 hours	Aug. 11, 2008
Windows Azure	22 hours	Mar. 13-14, 2009
FlexiScale	18 hours	Oct. 31, 2008
Amazon	7 hours	Jul. 20, 2008
Salesforce.com	40 minutes	Jan. 6, 2009

2. Data security. This risk is primarily due to loss of physical, personnel and logical data. Issues include Vulnerability Vulnerabilities, SaaS vulnerabilities (such as opening personal Docs user files), phishing fraud, and other potentially damaging data. Other security risks include data leakage, detection, loss of service, and loss of encryption keys. Failure to fully disable data or block individual users can lead to unnecessary disclosure of sensitive data when checking the situation with the tenants.

The vulnerability of the hypervisor can also be used to trigger attacks on client accounts. Data covering social and national insurance information, medical data and financial information raises questions about authorizations, rights management, authentication, and access control.

In addition, Abadi has shown that it is difficult to maintain the ACID (atomic, consensus, isolation, durability) properties in data replication in large geographical areas. Remembering or storing data is a matter of replication and distribution of data, even after the user leaves the cloud provider.

3. Third observation: The cloud may be the main cause of concern. Access by third parties with increased corporate value may lead to potential loss of intellectual property and commercial secrets. There is also a problem with the Insider problem, which abuses the right of the tenant to access information. Corporate spyware and information warfare is also under the control of the third-party. Providers maintain these rules, for example, in matters of audit, as well as issues that can be carried out locally in a global multi-media environment. There may also be situations in which a user is tied to a specific provider. This may be due to problems with data transfer to a new vendor. Other risks may be caused by deprecation of service terms after the cloud provider has been added or acquired. The latest reminder for faster recovery after troubleshooting will result in a third-party data tracking.

4. Confidentiality and legal issues-Cloud information is usually transmitted around the world, causing concern about jurisdiction, access to information, and privacy. Pearson summarized the main issues of cloud computing. Users have to keep their own information, where they are stored, or what future goals they do not know. Organizations are exposed to the risk of non-compliance with government policies, which will be further explained, and cloud service providers will be liable for sensitive information. Sharing in a single host of virtual and non-sensitive data, as well as their potential risks.

If you use public, public, and hybrid cloud, information is hosted on non-secure servers. This also creates security problems. Thus, all responsibility for the technical component is entrusted to the person who will provide this service. Thus, information about these systems can not be kept confidential. Also, when copying virtual machines, there is a problem with storing virtual files. If the memory is not deleted before moving to another virtual machine, there is a risk of data corruption.

Conclusion. The hypertrophy provides several operating systems, but this is a security issue. This danger arises because of the possibility of a threat to the new layer (and the new double layer, depending on the type of hypervisor). Thus, the original OS and the hypervisor (if used with hypervisor 2) should be protected. Although the virtualization system should be blocked by guests, this is not guaranteed in general. Currently, data protection issues in the cloud are not regulated in practice. Many organizations that provide cloud computing can deny all responsibility for data integrity.

REFERENCES

1. Virtualization Overview. White Paper. Vmware. Retrieved April 6, 2011, available at: http://www.vmware.com/pdf/virtualization.pdf
2. Web Search For A Planet: The Google Cluster Architecture. Retrieved April 6, 2011, available at: http://labs.google.com/papers/googlecluster-ieee.pdf
3. What is Cloud. Retrieved April 6, 2011, available at: http://www.rackspace.co.uk/cloud-hosting/learn-more/whatis-cloud/
4. What is Cloud Computing. Retrieved April 6, 2011, available at: http://www.microsoft.com/business/engb/solutions/Pages/Cloud.aspx
5. What is Cloud Computing. Retrieved April 6, 2011, available at: http://www.ibm.com/developerworks/cloud/newto.html#WHATIS

6. Recession is good for cloud computing – Microsoft agrees - http://www.cloudave.com/2425/recession-is-goodfor-cloud-computing-microsoft-agrees/
7. National Institute of Standards and Technology - Computer Security Division http://csrc.nist.gov/groups/SNS/cloud-computing/
8. Bhaskar P., Admela J·, Dimitrios K·, Yves G.: Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. J. Grid Computing 9(1), 3- 26 (2011)
9. What the Hell is Cloud Computing. Retrieved April 6, 2011, available at: http://www.youtube.com/watch?v=0FacYAI6DY0