Cloud computing security issues and challenges

Conference Paper · June 2010

Source: IEEE Xplore

2 authors:

Kresimir Popovic
Siemens
4 PUBLICATIONS **201** CITATIONS
SEE PROFILE

Zeljko Hocenski
University of Osijek
86 PUBLICATIONS **486** CITATIONS
SEE PROFILE

Cloud computing security issues and challenges

Krešimir Popović, Željko Hocenski
Institute of Automation and Process Computing
Faculty of Electrical Engineering Osijek
Kneza Trpimira 2b, Osijek, 31000, Croatia
Phone: (+385) (0)31-234 810 Fax: (+385) (0)31 224 605 E-mail:popovic@etfos.hr

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. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost. 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. This paper discusses security issues, requirements and challenges that cloud service providers (CSP) face during cloud engineering. Recommended security standards and management models to address these are suggested for technical and business community.

I. INTRODUCTION

Cloud service providers (CSP) (e.g. Microsoft, Google, Amazon, Salesforce.com, GoGrid) are leveraging virtualization technologies combined with self-service capabilities for computing resources via the Internet. In these service provider environments, virtual machines from multiple organizations have to be co-located on the same physical server in order to maximize the efficiencies of virtualization. Cloud service providers must learn from the managed service provider (MSP) model and ensure that their customers' applications and data are secure if they hope to retain their customer base and competitiveness. Today, enterprises are looking toward cloud computing horizons to expand their on-premises infrastructure, but most cannot afford the risk of compromising the security of their applications and data.

International Data Corporation (IDC) conducted a survey [1] (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 challenge or issue of cloud computing.

Corporations and individuals are concerned about how security and compliance integrity can be maintained in this new environment. Even more concerning, though, is the corporations that are jumping to cloud computing while being oblivious to the implications of putting critical applications and data in the cloud. Moving critical applications and sensitive data to a public and shared cloud environment is a major concern for corporations that are moving beyond their data center's network perimeter defense. To alleviate these concerns, a cloud solution provider must ensure that customers can continue to have the same security and privacy controls over their applications and services, provide evidence to these customers that their organization and customers are secure and they can meet their service-level agreements, and show how can they prove compliance to their auditors.

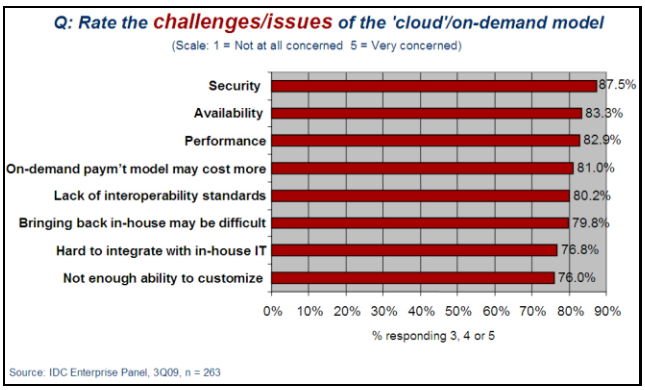

Fig. 1. Results of IDC ranking security challenges (3Q2009, n=263)

Regardless of how the cloud evolves, it needs some form of standardization (e.g. Information Technology Infrastructure Library -ITIL, ISO/IEC 27001/27002, Open Virtualization Format (OVF) [2][3][4]) so that the market can evolve and thrive. Standards should allow clouds to interoperate and communicate with each other no matter which vendor provides cloud services.

This professional paper discusses security and privacy issues as challenges, and recommends control objectives to technical and business community. It also highly recommends OVF standard as vendor and platform independent, open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines (software stack that incorporates the target applications, libraries, services, configuration, relevant data, and operating system).

II. SECURITY IN THE CLOUD

A. Security issues and challenges

Heightened security threats must be overcome in order to benefit fully from this new computing paradigm. Some security concerns are listed and discussed below:

1) Security concern #1: With the cloud model control physical security is lost because of sharing computing resources with other companies. No knowledge or control of where the resources run.

2) Security concern #2: Company has violated the law (risk of data seizure by (foreign) government).

3) Security concern #3: Storage services provided by one cloud vendor may be incompatible with another vendor's services if user decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud). [5]

4) Security concern #4: Who controls the encryption/decryption keys? Logically it should be the customer.

5) Security concern #5: Ensuring the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exist.

6) Security concern #6: In case of Payment Card Industry Data Security Standard (PCI DSS) data logs must be provided to security managers and regulators. [6][7][8]

7) Security concern #7: Users must keep up to date with application improvements to be sure they are protected.

8) Security concern #8: Some government regulations have strict limits on what data about its citizens can be stored and for how long, and some banking regulators require that customer's financial data remain in their home country.

9) Security concern #9: The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure the auditability of records.

10) Security concern #10: Customers may be able to sue cloud service providers if their privacy rights are violated, and in any case the cloud service providers may face damage to their reputation. Concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties.

Privacy sensitive information: [9]

- Personally identifiable information (PII [10]): any information that could be used to identify or locate an individual (e.g. state, name, address) or information that can be correlated with other information to indentify an individual (e.g. credit card number, Internet protocol (IP) address).
- Information on religion, race, health, union membership, sexual orientation, job performance, financial information, biometric information or any other information that may be considered sensitive.
- Data collected from computer devices (e.g. notebook, smartphone, iPad).
- Information uniquely traceable to a user device (e.g. IP address, Radio Frequency Identity (RFID) MAC address).

Additional considerations to be aware of:

- *Access*: Data subjects have a right to know what personal information is held and, in some cases, can make a request to stop processing it. If a data subject exercises this right to ask the organization to delete his data, will it be possible to ensure that all of his information has been deleted in the cloud?
- *Compliance*: What are the applicable laws, regulations, standards, and contractual commitments that govern this information, and who is responsible for maintaining the compliance? Clouds can cross multiple jurisdictions in multiple states.
- *Storage*: Where is the data in the cloud stored? Was it transferred to another data center in another country? Privacy laws in various countries place limitations on the ability of organizations to transfer some types of personal information to other countries.
- *Retention*: How long is personal information (that is transferred to the cloud) retained? Who enforces the retention policy in the cloud, and how are exceptions to this policy (such as litigation holds) managed?
- *Destruction*: How can we know that the cloud service provider (CSP) didn't retain additional copies? Did the CSP really destroy the data, or just make it inaccessible to the organization? Is the CSP keeping the information longer than necessary so that it can mine the data for its own use?
- *Audit and monitoring*: How can organizations monitor their CSP and provide assurance to relevant stakeholders that privacy requirements are met when their PII is in the cloud?
- *Privacy breaches*: How can we ensure that the cloud service provider (CSP) notifies us when a breach occurs, and who is responsible for managing the breach notification process (and costs associated with the process)? If contracts include liability for breaches resulting from negligence of the CSP, how is the contract enforced and how is it determined who is at fault?

B. Security management standards

Standards that are relevant to security management practices in the cloud are Information Technology Infrastructure Library (ITIL), ISO/IEC 27001/27002 and Open Virtualization Format (OVF).

1) Information Technology Infrastructure Library (ITIL): it is set of best practices and guidelines that define an integrated, process-based approach for managing information technology services. ITIL can be applied across almost every type of IT environment including cloud operating environment. ITIL seeks to ensure that effective information security measures are taken at strategic, tactical, and operational levels. Information security is considered an iterative process that must be controlled, planned, implemented, evaluated, and maintained.

ITIL provides a systematic and professional approach to the management of IT service provision. Adopting its guidance offers users a huge range of benefits that include:

- Reduced costs
- Improved IT services through the use of proven best practice processes
- Improved customer satisfaction through a more professional approach to service delivery
- Standards and guidance
- Improved productivity
- Improved use of skills and experience
- Improved delivery of third party services through the specification of ITIL or ISO 20000 as the standard for service delivery in services procurements
- ITIL helps you separate administrative tasks and technical tasks so that you assign the most appropriate resources
- better measure technical support performance

The ITIL-process Security Management describes the structured fitting of information security in the management organization. It is based on the code of practice for *information security management* now known as ISO/IEC 27002.

ITIL breaks information security down into:

- *Policies*: The overall objectives an organization is attempting to achieve
- *Processes*: What has to happen to achieve the objectives
- *Procedures*: Who does what and when to achieve the objectives:
- *Work instructions*: Instructions for taking specific actions

A basic goal of security management is to ensure adequate information security. The primary goal of information security, in turn, is to protect information assets against risks, and thus to maintain their value to the organization. This is commonly expressed in terms of ensuring their confidentiality, integrity and availability, along with related properties or goals such as authenticity, accountability, non-repudiation and reliability.

Note: Organizations and management systems cannot be certified as "ITIL-compliant." Only practioners can be certified.

2) International Organization for Standardization (ISO) 27001/27002: ISO/IEC 27001 formally defines the mandatory requirements for an Information Security Management System (ISMS). It is also a certification standard and uses ISO/IEC 27002 to indicate suitable information security controls within the ISMS.

Essentially, the ITIL, ISO/IEC 20000, and ISO/IEC 27001/27002 frameworks help IT organizations internalize and respond to basic questions such as:

- "How do I ensure that the current security levels are appropriate for your needs? "
- "How do I apply a security baseline throughout your operation? "

Simply to say, they help to respond to the question: "how do I ensure that my services are secure?"

3) Open Virtualization Format: OVF enables efficient, flexible, and secure distribution of enterprise software, facilitating the mobility of virtual machines and giving customers vendor and platform independence. Customers can deploy an OVF formatted virtual machine on the virtualization platform of their choice.

With OVF, customers' experience with virtualization is greatly enhanced, with more portability, platform independence, verification, signing, versioning, and licensing terms. OVF lets you:

- Improve your user experience with streamlined installations
- Offer customers virtualization platform independence and flexibility
- Create complex pre-configured multi-tiered services more easily
- Efficiently deliver enterprise software through portable virtual machines
- Offer platform-specific enhancements and easier adoption of advances in virtualization through extensibility

The rising investments to virtual appliances (IBM, Microsoft, Hewlett-Packard, Dell, VMware, and XenSource) not only simplify the deployment of applications for individual users but also power next-generation cloud computing architectures. Rather than the considerable time required to build a specialized distribution with applications, most cloud computing infrastructures provide ready-to-deploy virtual appliances to satisfy any need. And because a virtual appliance is simply a file with a wrapper (the XML description), *it's easy to replicate and distribute such appliances with all security and privacy configurations.*

In the future, clouds that are enabled by a virtualization layer will provide new go-to-market opportunities, and software appliances (software products that integrate operating system and layered software into an easily managed composite package that can be deployed aboard industry-standard client or server hardware, either on a virtual machine or directly on the hardware) will help simplify this transition. Cloud computing, in conjunction with software appliances, will also create new business models that will allow companies to sell a single product on premises, on demand, or in a hybrid deployment model. While both of these technologies remain relatively immature, it is necessary to start understanding the new dynamics that will start to emerge to sell software and hardware to end users.

Note: Software appliances market should exceed revenue of $360.9 million by the end of 2010, $1,184.4 billion by the end of 2012. [11]

C. Security management models

This section describes twenty recommended security management models and their requirements for cloud computing that cloud service providers should definitely consider as they develop or refine their compliance programs.

1) Software-as-a-Service (SaaS) security: 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. Just as with a managed service provider, corporations or end users will need to research vendors' policies on data security before using vendor services to avoid losing or not being able to access their data. The technology analyst and consulting firm Gartner lists [12] seven security risks which one should discuss with a cloud-computing vendor:

- *Privileged user access*: Get as much information as you can about the people who manage your data. Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.
- *Regulatory compliance:* Make sure that the vendor is willing to undergo external audits and/or security certifications.
- *Data location:* When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.
- *Data segregation:* Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.
- *Recovery:* Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."
- *Investigative support:* Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then only safe assumption is that investigation and discovery requests will be impossible.
- *Long-term viability*: Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application.

To address the security issues listed above, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves.

2) Security management (People): One of the most important actions for a security team is to develop a formal charter for the security organization and program. The charter should be aligned with the strategic plan of the organization or company the security team works for. Lack of clearly defined roles and responsibilities, and agreement on expectations, can result in a general feeling of loss and confusion among the security team about what is expected of them, how their skills and experienced can be leveraged, and meeting their performance goals.

3) Security governance: A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies. This committee must clearly define the roles and responsibilities of the security team and other groups involved in performing information security functions.

4) Risk management: Risk management entails identification of technology assets [13]; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities. Actions should also include maintaining a repository of information assets. Owners have authority and accountability for information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy controls.

5) Risk assessment: Security risk assessment is critical to helping the information security organization make informed decisions when balancing the dueling priorities of business utility and protection of assets [14][15]. A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or as-needed basis. More detailed and technical security risk assessments in the form of threat modeling should also be applied to applications and infrastructure.

6) Security awareness: People are the weakest link for security. Knowledge and culture are among the few effective tools to manage risks related to people. Not providing proper awareness and training to the people who may need them can expose the company to a variety of security risks for which people, rather than system or application vulnerabilities, are the threats and points of entry. Social engineering attacks, lower reporting of and slower responses to potential security incidents, and inadvertent customer data leaks are all possible and probable risks that may be triggered by lack of an effective security awareness program.

7) Education and training: Programs should be developed that provide a baseline for providing fundamental security and risk management skills and knowledge to the security

team and their internal partners. This entails a formal process to assess and align skill sets to the needs of the security team and to provide adequate training and mentorship-providing a broad base of fundamental security, inclusive of data privacy, and risk management knowledge.

8) Policies and standards: Many resources and templates are available to aid in the development of information security policies and standards. A cloud computing security team should first identify the information security and business requirements unique to cloud computing, SaaS, and collaborative software application security. Policies should be developed, documented, and implemented, along with documentation for supporting standards and guidelines. To maintain relevancy, these policies, standards, and guidelines should be reviewed at regular intervals or when significant changes occur in the business or IT environment.

9) Third party risk management: Lack of a third-party risk management program may result in damage to the provider's reputation, revenue losses, and legal actions should the provider be found not to have performed due diligence on its third-party vendors.

10) Vulnerability assessment: Classifies network assets to more efficiently prioritize vulnerability-mitigation programs, such as patching and system upgrading.

11) Security image testing: Virtualization-based cloud computing provides the ability to create "Test image" VM secure builds and to clone multiple copies. Gold image VMs also provide the ability to keep security up to date and reduce exposure by patching offline. Offline VMs can be patched off-network, providing an easier, more cost-effective, and less production-threatening way to test the impact of security changes.

12) Data governance: This framework should describe who can take what actions with what information, and when, under what circumstances, and using what methods.

13) Data security: Security will need to move to the data level so that enterprises can be sure their data is protected wherever it goes. For example, with data-level security, the enterprise can specify that this data is not allowed to go outside of the European Union. It can also force encryption of certain types of data, and permit only specified users to access the data. It can provide compliance with the Payment Card Industry Data Security Standard (PCI DSS).

14) Application security: This is where the security features and requirements are defined and application security test results are reviewed. Application security processes, secure coding guidelines, training, and testing scripts and tools are typically a collaborative effort between the security and the development teams. Although product engineering will likely focus on the application layer, the security design of the application itself, and the infrastructure layers interacting with the application, the security team should provide the security requirements for the product development engineers to implement.

15) Virtual machine security: In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not only can data center security teams replicate typical security controls for the data center at large to secure the virtual machines, they can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate.

16) Identity Access Management (IAM): identity and access management is a critical function for every organization, and a fundamental expectation of SaaS customers is that the "principle of least privilege" is granted to their data. The principle of least privilege states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary.

17) Change management: The security team can create security guidelines for standards and minor changes, to provide self-service capabilities for these changes and to prioritize the security team's time and resources on more complex and important changes to production.

18) Physical security: Since customers lose control over physical assets, security model may need to be reevaluated. The concept of the cloud can be misleading at times, and people forget that everything is somewhere actually tied to a physical location. The massive investment required to build the level of security required for physical data centers is the prime reason that companies don't build their own data centers, and one of several reasons why they are moving to cloud services in the first place. Some samples of controls mechanisms:

- 24/7/365 onsite security.
- Biometric hand geometry readers.
- Security cameras should monitor activity throughout the facility.
- Heat, temperature, air flow, and humidity should all be kept within optimum ranges for the computer equipment.
- Policies, processes, and procedures are critical elements of successful physical security that can protect the equipment and data housed in the hosting center.

19) Disaster recovery: In the SaaS environment, customers rely heavily on 24/7/365 access to their services and any interruption in access can be catastrophic. Using the virtualization software virtual server can be copied, backed up, and moved just like a file (live migration). Benefits are:

- Quickly reallocating computing resources without any downtime
- Ability to deliver on service-level agreements and provide high-quality service

20) Data privacy: A privacy steering committee should also be created to help make decisions related to data privacy. The security compliance team, if one even exists, will not have formalized training on data privacy. The answer is to hire a consultant in this area, hire a privacy expert, or have one of your existing team members trained properly. This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators.

III. CONCLUSION

We have argued that it is very important to take security and privacy into account when designing and using cloud services. In this paper security in cloud computing was elaborated in a way that covers security issues and challenges, security standards and security management models.

- Security issues indicate potential problems which might arise.
- Security standards offer some kind of security templates which cloud service providers (CSP) could obey. The most promising standard for the future would be OVF format which promises creation of new business models that will allow companies to sell a single product on premises, on demand, or in a hybrid deployment model.
- Security management models offer recommendations based on security standards and best practices. [16]

These are all very important topics which will be certainly discussed in the upcoming years of cloud computing. Based on IDC survey [17] the security and vulnerability market should exceed revenue of $4.4 billion by the end of 2013, with a climbing annual growth rate resulting in a compound annual growth rate (CAGR) of 10.8%. This survey shows that products that fall within the security and vulnerability management market will remain in high demand.

REFERENCES

[1] International Data Corporation, http://blogs.idc.com/ie/wp-content/uploads/2009/12/idc_cloud_challenges_2009.jpg, 2009

[2] Information Technology Infrastructure Library, http://www.itil-officialsite.com/home/home.asp

[3] International Organization for Standardization, http://www.iso.org/iso/home.htm

[4] Distributed Management Task Force, http://www.dmtf.org/standards/published_documents/DSP2017_1.0.0.pdf, 22.02.2009

[5] M. Casassa-Mont, S. Pearson and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services", Proc. DEXA 2003, IEEE Computer Society, 2003, pp. 377-382

[6] https://www.pcisecuritystandards.org/index.shtml

[7] http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard, 24 January 2010

[8] J. Salmon, "Clouded in uncertainty – the legal pitfalls of cloud computing", Computing, 24 Sept 2008, http://www.computing.co.uk/computing/features/2226701/clouded-uncertainty-4229153

[9] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services", CLOUD'09, May 23, 2009, Vancouver, Canada

[10] Wikipedia, 20 January 2010, http://en.wikipedia.org/wiki/Personally_identifiable_information

[11] International Data Corporation, B. Waldman, A. Gillen http://www.novell.com/rc/docrepository/public/37/basedocument.2009-07-28.4081031793/IDC-The%20Market%20for%20Software%20Appliances_en.pdf, July 2009

[12] Gartner: Seven cloud-computing security risks, 02 July 2008, http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0

[13] Wikipedia, 6 February 2010, http://en.wikipedia.org/wiki/Risk_management

[14] Wikipedia, 27 January 2010, http://en.wikipedia.org/wiki/Risk_assessment

[15] D. Catteddu, Giles Hogben: European Network and Information Security Agency, November 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[16] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/, December 2009

[17] International Data Corporation, Worldwide Security and Vulnerability Management 2009–2013 Forecast and 2008 Vendor Shares, http://vulnerabilitymanagement.com/docs/IDC_MA_2009.pdf