Cloud Infrastructure Security

Dimiter Velev, Plamena Zlateva

Cloud Infrastructure Security

Dimiter Velev[1] and Plamena Zlateva[2]

[1] University of National and World Economy,
UNSS - Studentski grad, 1700 Sofia, Bulgaria
dvelev@unwe.acad.bg
[2] Institute of Control and System Research - Bulgarian Academy of Sciences
Acad. G. Bonchev Str., Bl. 2, P.O.Box 79, 1113 Sofia, Bulgaria
plamzlateva@abv.bg

Abstract. Cloud computing can help companies accomplish more by eliminating the physical bonds between an IT infrastructure and its users. Users can purchase services from a cloud environment that could allow them to save money and focus on their core business. At the same time certain concerns have emerged as potential barriers to rapid adoption of cloud services such as security, privacy and reliability. Usually the information security professionals define the security rules, guidelines and best practices of the IT infrastructure of a given organization at the network, host and application levels. The current paper discusses miscellaneous problems of providing the infrastructure security. The different aspects of data security are given a special attention, especially data and its security. The main components of cloud infrastructure security are defined and the corresponding issues and recommendations are given.

Key words: cloud, service, infrastructure, IaaS, security, data.

1 Introduction to Cloud Computing Basics

Currently one of the major topics of many information technology discussions is cloud computing and the key point in them is cloud computing security. Usually conversations focus on all standard security advantages, disadvantages and requirements. Nevertheless the fact the most common security measures protect data from loss, unauthorized access, integrity disruption, etc., there are other necessary and important characteristics of any IT infrastructure that must implemented in a much more serious way. One of those structures is the cloud infrastructure.

1.1 Cloud Computing Definition

Cloud computing is an on-demand service model for IT provision based on virtualization and distributed computing technologies [1], [9], [10]. Typical cloud computing providers deliver common business applications online as services which are accessed from another web service or software like a web browser,

while the software and data are stored on servers. The abstraction of computing, network and storage infrastructure is the foundation of cloud computing. The infrastructure is a service, and its components must be readily accessible and available to the immediate needs of the application stacks it supports. Cloud computing removes the traditional application silos within the data center and introduces a new level of flexibility and scalability to the IT organization. This flexibility helps address challenges facing enterprises and IT service providers that include rapidly changing IT landscapes, cost reduction pressures, and focus on time to market. Cloud users are maybe identified as follows [1]:

- Individual consumers;
- Individual businesses;
- Start-ups;
- Small and medium-size businesses;
- Enterprise businesses

Cloud computing architectures offer to its users numerous advantages that can be briefly summarized to [2]:

- reduced cost since services are provided on demand with pay-as-you-use billing system;
- highly abstracted resources;
- instant scalability and flexibility;
- instantaneous provisioning;
- shared resources, such as hardware, database, etc.;
- programmatic management through API of Web services;
- increased mobility - information is accessed from any location.

1.2 Cloud Computing Categories

The following cloud computing categories have been identified and defined in the process of cloud development [1], [10]:

- Infrastructure as Service (IaaS): provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service Application Programming Interface (API). IaaS includes the entire infrastructure resource stack from the facilities to the hardware platforms that reside in them. It incorporates the capability to abstract resources as well as deliver physical and logical connectivity to those resources. IaaS provides a set of APIs which allow management and other forms of interaction with the infrastructure by consumers.
- Platform as a Service (PaaS): allows customers to develop new applications using APIs, implemented and operated remotely. The platforms offered include development tools, configuration management and deployment platforms. PaaS is positioned over IaaS and adds an additional layer of integration with application development frameworks and functions such as database, messaging, and queuing that allow developers to build applications for the platform with programming languages and tools are supported by the stack.

- Software as a Service (SaaS): is software offered by a third party provider, available on demand, usually through a Web browser, operating in a remote manner. Examples include online word processing and spreadsheet tools, CRM services and Web content delivery services. SaaS in turn is built upon the underlying IaaS and PaaS stacks and provides a self-contained operating environment used to deliver the entire user experience including the content, its presentation, the applications and management capabilities.
- Multi-Tenancy: the need for policy-driven enforcement, segmentation, isolation, governance, service levels and billing models for different consumer constituencies. Consumers might utilize a public cloud provider's service offerings or actually be from the same organization, but would still share infrastructure.

1.3 Cloud Deployment Models

The cloud services can be implemented in four deployment models [1], [10]:

- Public Cloud. The cloud infrastructure is made available to the general public or large industry group and is owned by an organization selling cloud services.
- Private Cloud. The cloud infrastructure is operated entirely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises.
- Community Cloud. The cloud infrastructure is shared by several organizations and supports a specific community. It may be managed by the organizations or a third party, and may exist on-premises or off-premises.
- Hybrid Cloud. The cloud infrastructure is a composition of two or more clouds (private, community or public) that are bound together by standardized or proprietary technology that enables portability of data and application.

2 Risks and Security Concerns With Cloud Computing

Many of the cloud computing associated risks are not new and can be found in the computing environments. There are many companies and organizations that outsource significant parts of their business due to the globalization. It means not only using the services and technology of the cloud provider, but many questions dealing with the way the provider runs his security policy. After performing an analysis the top threats to cloud computing can be summarized as follows [3], [7]:

- Abuse and Unallowed Use of Cloud Computing;
- Insecure Application Programming Interfaces;
- Malicious Insiders;
- Shared Technology Vulnerabilities;
- Data Loss and Leakage

- Account, Service and Traffic Hijacking;
- Unknown Risk Profile.

It has been established that the most common topics related with cloud computing risk at present include [6], [11]:

- The cloud provider takes responsibility for information handling which is a critical part of the business. Failure to perform to agreed service levels can impact not only confidentiality but also availability.
- The dynamic nature of cloud computing may result in confusion as to where information actually resides. This may create delays when information retrieval is required.
- Third-party access to sensitive information creates a risk of compromise to confidential information. This can pose a significant threat to ensuring the protection of intellectual property and trade secrets.
- Public clouds allow high-availability systems to be developed at service levels often impossible to create in private networks. Compliance to regulations and laws in different geographic regions can be a challenge for business.
- Due to the dynamic nature of the cloud, information may not be located in the event of a disaster immediately. Business continuity and disaster recovery plans must be well documented and tested. Recovery time objectives should be stated in the contract. When faced with the paradigm change and nature of services provided through cloud computing, there are many challenges for cloud providers [6]. Some of the major security issues that will need to be addressed are [4], [5], [12]:
- Transparency - Service providers must provide for the existence of effective and robust security controls, assuring customers that their information is properly secured against unauthorized access, change and
- Privacy - With privacy concerns growing across the globe it will be imperative for cloud computing service providers to prove to existing and prospective customers that privacy controls are in place and demonstrate their ability to prevent, detect and react to breaches in a proper manner. Information and reporting communication lines need to be organized and agreed before service provisioning starts. These communication channels should be tested periodically during operations.
- Compliance - Most organizations must comply with a wide set of laws, regulations and standards. There are concerns with cloud computing that data may not be stored in one place and may not be easily retrievable. Audits completed by legal, standard and regulatory authorities demonstrate that there can be plenty of problems. When using cloud services there is no guarantee that a certain company can get its information when needed, and even some providers are reserving the right to withhold information from authorities.
- Transborder information flow - When information can be stored anywhere in the cloud, the physical location of the information can become an issue. Physical location rules jurisdiction and legal obligation. Country laws governing personally identifiable information may vary significantly.

- Certification - Cloud computing service providers will need to provide their customers assurance that they operate surely. Independent assurance from third-party audits and/or service auditor reports should be a vital part of any assurance program.

3 Cloud Security Principles

Public cloud computing requires a security model that coordinates scalability and multi-tenancy with the requirement for trust. As enterprises move their computing environments with their identities, information and infrastructure to the cloud, they must be willing to give up some level of control. In order to do so they must be able to trust cloud systems and providers, as well as to verify cloud processes and events. Important building blocks of trust and verification relationships include access control, data security, compliance and event management - all security elements well understood by IT departments today, implemented with existing products and technologies, and extendable into the cloud. The cloud security principles comprise three categories: identity, information and infrastructure.

3.1 Identity security

End-to-end identity management, third-party authentication services and identity must become a key element of cloud security. Identity security keeps the integrity and confidentiality of data and applications while making access readily available to appropriate users. Support for these identity management capabilities for both users and infrastructure components will be a major requirement for cloud computing and identity will have to be managed in ways that build trust. It will require:

- Stronger authentication: Cloud computing must move beyond authentication of username and password, which means adopting methods and technologies that are IT standard IT such as strong authentication, coordination within and between enterprises, and risk-based authentication, measuring behavior history, current context and other factors to assess the risk level of a user request.
- Stronger authorization: Authorization can be stronger within an enterprise or a private cloud, but in order to handle sensitive data and compliance requirements, public clouds will need stronger authorization capabilities that can be constant throughout the lifecycle of the cloud infrastructure and the data.

3.2 Information security

In the traditional data center, controls on physical access, access to hardware and software and identity controls all combine to protect the data. In the cloud, that protective barrier that secures infrastructure is diffused. The data needs its own security and will require [5], [14]:

- Data isolation: In multi-tenancy environment data must be held securely in order to protect it when multiple customers use shared resources. Virtualization, encryption and access control will be workhorses for enabling varying degrees of separation between corporations, communities of interest and users.
- Stronger data security: In existing data center environments the role-based access control at the level of user groups is acceptable in most cases since the information remains within the control of the enterprise. However, sensitive data will require security at the file, field or block level to meet the demands of assurance and compliance for information in the cloud.
- Effective data classification: Enterprises will need to know what type of data is important and where it is located as prerequisites to making performance cost-benefit decisions, as well as ensuring focus on the most critical areas for data loss prevention procedures.
- Information rights management: it is often treated as a component of identity on which users have access to. The stronger data-centric security requires policies and control mechanisms on the storage and use of information to be associated directly with the information itself.
- Governance and compliance: A major requirement of corporate information governance and compliance is the creation of management and validation information - monitoring and auditing the security state of the information with logging capabilities. The cloud computing infrastructures must be able to verify that data is being managed per the applicable local and international regulations with appropriate controls, log collection and reporting.

3.3 Security Compromises Between the Three Cloud Deployment Models

The following security compromises between the three cloud deployment models have been identified [7], [10]:

- SaaS provides the most integrated functionality built directly into the offering, with the least consumer extensibility, and a relatively high level of integrated security since at the least the provider bears a responsibility for the security.
- 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.
- IaaS provides few if any application-like features, but enormous extensibility. This generally means less integrated security capabilities and functionality beyond protecting the infrastructure itself. This model requires that operating systems, applications, and content be managed and secured by the cloud consumer.

4 Infrastructure Security

IaaS application providers treat the applications within the customer virtual instance as a black box and therefore are completely indifferent to the operations and management of a applications of the customer [13]. The entire pack (customer application and run time application) is run on the customers' server on provider infrastructure and is managed by customers themselves. For this reason it is important to note that the customer must take full responsibility for securing their cloud deployed applications [7], [8], [12].

- Cloud deployed applications must be designed for the internet threat model.
- They must be designed with standard security countermeasures to guard against the common web vulnerabilities.
- Customers are responsible for keeping their applications up to date - and must therefore ensure they have a patch strategy to ensure their applications are screened from malware and hackers scanning for vulnerabilities to gain unauthorized access to their data within the cloud.
- Customers should not be tempted to use custom implementations of Authentication, Authorization and Accounting as these can become weak if not properly implemented.

The foundational infrastructure for a cloud must be inherently secure whether it is a private or public cloud or whether the service is SAAS, PAAS or IAAS. It will require [7], [9]:

- Inherent component-level security: The cloud needs to be architected to be secure, built with inherently secure components, deployed and provisioned securely with strong interfaces to other components and supported securely, with vulnerability-assessment and change-management processes that produce management information and service-level assurances that build trust.
- Stronger interface security: The points in the system where interaction takes place (user-to-network, server-to application) require stronger security policies and controls that ensure consistency and accountability.
- Resource lifecycle management: The economics of cloud computing are based on multi-tenancy and the sharing of resources. As the needs of the customers and requirements will change, a service provider must provision and decommission correspondingly those resources - bandwidth, servers, storage and security. This lifecycle process must be managed in order to build trust.

The infrastructure security can be viewed, assessed and implemented according its building levels - the network, host and application levels [7], [11].

4.1 Infrastructure Security - The Network Level

When looking at the network level of infrastructure security, it is important to distinguish between public clouds and private clouds. important to distinguish between public clouds and private clouds. With private clouds, there are no new

attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider. If public cloud services are chosen, changing security requirements will require changes to the network topology and the manner in which the existing network topology interacts with the cloud provider's network topology should be taken into account [7]. There are four significant risk factors in this use case:

- Ensuring the confidentiality and integrity of organization's data-in-transit to and from a public cloud provider;
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources are used at the public cloud provider;
- Ensuring the availability of the Internet-facing resources in a public cloud that are being used by an organization, or have been assigned to an organization by public cloud providers;
- Replacing the established model of network zones and tiers with domains.

4.2 Infrastructure Security - The Host Level

When reviewing host security and assessing risks, the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models public, private, and hybrid) should be considered [7]. The host security responsibilities in SaaS and PaaS services are transferred to the provider of cloud services. IaaS customers are primarily responsible for securing the hosts provisioned in the cloud (virtualization software security, customer guest OS or virtual server security).

4.3 Infrastructure Security - The Application Level

Application or software security should be a critical element of a security program. Most enterprises with information security programs have yet to institute an application security program to address this realm. Designing and implementing applications aims at deployment on a cloud platform will require existing application security programs to reevaluate current practices and standards. The application security spectrum ranges from standalone single-user applications to sophisticated multiuser e-commerce applications used by many users. The level is responsible for managing [7], [9], [10]:

- Application-level security threats;
- End user security;
- SaaS application security;
- PaaS application security;
- Customer-deployed application security
- IaaS application security
- Public cloud security limitations

It can be summarized that the issues of infrastructure security and cloud computing lie in the area of definition and provision of security specified aspects each party delivers.

5 Conclusion

The cloud is a major challenge in how computing resources will be utilized since aim of the cloud computing is to change the economics of the data center, but before sensitive and regulated data move into the public cloud, issues of security standards and compatibility must be addressed including strong authentication, delegated authorization, key management for encrypted data, data loss protections and regulatory reporting. All are elements of a secure identity, information and infrastructure model and can be applied to private and public clouds as well as to IAAS, PAAS and SAAS services. In the development of public and private clouds the service providers will need to use these guiding principles to adopt and extend security tools and secure products to build and offer end-to-end trustworthy cloud computing and services.

References

1. Cloud Computing, http://en.wikipedia.org/wiki/Cloud_computing.
2. Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives. An ISACA Emerging Technology White Paper, http://www.isaca.org.
3. Dhanjani, N., Rios, B., Hardi, B.: acking: The Next Generation. HO'Reilly Media, Inc., (2009).
4. ENISA.: Cloud Computing: Information Assurance Framework. ENISA, http://www.enisa.europa.eu/, November 2009.
5. ENISA.: Cloud Computing: Benefits, risks and recommendations for information security. ENISA, http://www.enisa.europa.eu/, November 2009.
6. Lyong, L.: How to Select a Cloud Computing Infrastructure Provider. Gartner, Inc. Research. ID Number: G00166565.
7. Mather, T., Kumaraswamy, S., Latif, S.: Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc., 2009.
8. Owens, K.: Securing Virtual Compute Infrastructure in the Cloud. White Paper: Cloud Computing, www.savvis.net.
9. Reese, G.: Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. O'Reilly Media, Inc., 2009.
10. Rittinghouse, J.W., Ransome, J.F.: Cloud Computing: Implementation, Management and Security. CRC Press, 2009.
11. Secure Cloud Architecture, NetApp, August 2009, WP-7083-0809.
12. Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Cloud Security Alliance http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf, 2009.
13. Securing Microsoft's Cloud Infrastructure. A Microsoft White Paper. http://blogs.technet.com/gfs/archive/2009/05/27/securing-microsoft-s-cloud-infrastructure.aspx
14. The Role of Security in Trustworthy Cloud Computing. RSA, White paper. www.rsa.com.