Protection Cloud Computing Systems from Threats

Nasrullaev Nurbek Baxtiyorovich,
PHD Student, Providing of Information Security Department,
Tashkent University of Information Technologies, Uzbekistan,
n.bakhtyarovich@gmail.com

Islomov Shahboz Zokirugli,
Teacher Assistant, Department of Cytology and Discrete Mathematics,
Tashkent University of Information Technologies, Tashkent, Uzbekistan,
shaxboz4044@gmail.com

Zokirov Odiljon Yoqubjonugli
, Teacher Assistant, Providing of Information Security Department,
Tashkent University of Information Technologies, Uzbekistan,
z.odil044@gmail.com

Murtozaev Sherzod Abdullaevich,
Teacher Assistant, Department of Software Engineering,
Karshi Branch of Toshkent University of Information Technologies,Uzbekistan,
Sherzod_tmi@mail.ru

***Abstract*—**Cloud Computing technologies play an important role in information processing and stores now days. Also with these systems we can work with high level programming languages, high definition video games and collect any user into one network easily, so, without expensive hardware and software. At this time helps to user three main services SaaS, PaaS and IaaS. Besides all the salient features of cloud environment, there are the big challenges of privacy and security. In this paper, a review of different security issues like trust, confidentiality, authenticity, encryption, key management and new approach to security architecture by services.

Keywords- *scalable, flexible, monitoring, infra protection, virtual security.*

*****

I. Introduction

Security for cloud computing has become one of the top concerns for cloud actors such as cloud service providers, tenants and tenants’ customers, as well as for governments and regulators. The paper includes a list of recommendations, along with guidance and strategies, designed to help these decision makers evaluate and compare security offerings from different cloud providers in key areas. When considering a move to cloud computing, customers must have a clear understanding of potential security benefits and risks associated with cloud computing, and set realistic expectations with their cloud provider. Consideration must be given to the different service categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) as each model brings different security requirements and responsibilities.

In [1] paper was discussed several threats, technology risks, and safeguards for cloud computing environments, and provides the insight needed to make informed IT decisions on their treatment. Although in this paper is provided, each organization must perform its own analysis of its needs, and assess, select, engage, and oversee the cloud services that can best fulfill those needs.

II. ANALYSES OF CLOUD TYPES

Before going to methods or ways of protection cloud computing we need to recognize types of cloud. There are four types of cloud: public, private, hybrid and dedicated servers.

Private cloud: Private cloud is cloud infrastructure over a network that is open for public use. Public cloud services may be free.

Public cloud: A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free.

Hybrid cloud: Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models.Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources. In this following table is given analyses of above given types of cloud

TABLE I. ANALYSES OF CLOUD TYPES

	Public cloud	Private cloud	Dedicated servers	Hybrid cloud
Physical hardware	Shared	Dedicated	Dedicated	Shared + Dedicated
Scalable	+	+		+
Low cost, utility billing	+			+
Flexible	+			+
Customizable		+	+	+
High Performance		+	+	+
Enhanced security and control		+	+	+
Predictable cost		+	+	+

III. PROTECTION FROM THREATS

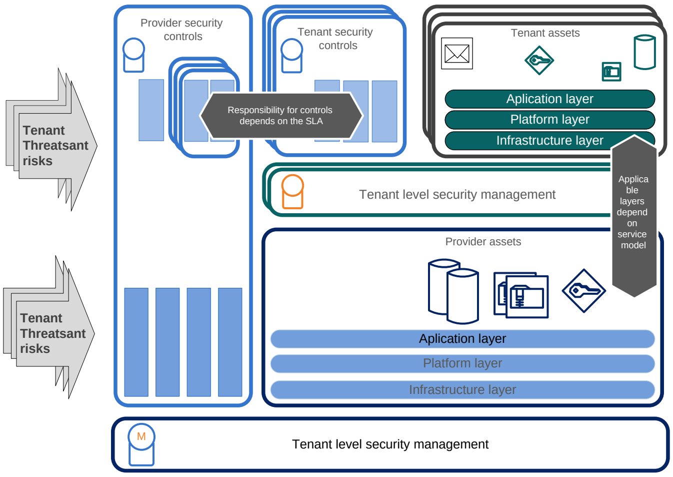

Figure 1. Logical cloud security architecture

For protection from unauthorized accesses are used control methods. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:

Deterrent controls. These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed.

Preventive controls. These controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

Detective controls. These type of controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.

Corrective controls. Thesecontrols reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

By these methods are built security architecture (figure 1). Also, cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management. [2] The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. In practice, cloud security architecture addresses the build and deploy, operate and control, and predict and learn parts of the Trust Engine, while the other parts of the Trust Engine are more governance-oriented.

Every cloud security architecture must consist of following components [3]:

- IdAM;
- Key and certificate management;
- Data protection;
- Security monitoring analytics;
- Network and infra protection;
- HW assisted and virtual security;
- Other security functions.

The security controls and services are divided into 7 groups in the logical cloud security architecture [4]. They should be seamlessly coupled with security management and orchestration to achieve end-to-end security responses. Security management ensures consistent security across the system. It translates business and operational security policies of providers and customers into actionable security policies. Cloud computing is the large sphere in IT and there are a lot of measurements to protect from threats [5].

There are:

Loss of governance. In a public cloud deployment, customers cede control to the cloud provider over a number of issues that may affect security. Yet cloud service agreements may not offer a commitment to resolve such issues on the part of the cloud provider, thus leaving gaps in security defenses.

Responsibility ambiguity. Responsibility over aspects of security may be split between the provider and the customer, with the potential for vital parts of the defenses to be left unguarded if there is a failure to allocate responsibility clearly. This split is likely to vary depending on the cloud computing model used (e.g., IaaS vs. SaaS).

Authentication and Authorization. The fact that sensitive cloud resources are accessed from anywhere on the Internet heightens the need to establish with certainty the identity of a user -- especially if users now include employees, contractors, partners and customers. Strong authentication and authorization becomes a critical concern.

Isolation failure. Multi-tenancy and shared resources are defining characteristics of public cloud computing. This risk category covers the failure of mechanisms separating the usage of storage, memory, routing and even reputation between tenants (e.g. so-called guest-hopping attacks).

Compliance and legal risks. The cloud customer ’ s investment in achieving certification (e.g., to demonstrate compliance with industry standards or regulatory requirements) may be lost if the cloud provider cannot provide evidence of their own compliance with the relevant requirements, or does not permit audits by the cloud customer. The customer must check that the cloud provider has appropriate certifications in place.

Handling of security incidents. The detection, reporting and subsequent management of security breaches may be delegated to the cloud provider, but these incidents impact the customer. Notification rules need to be negotiated in the cloud service agreement so that customers are not caught unaware or informed with an unacceptable delay.

Management interface vulnerability. Interfaces to manage public cloud resources (such as self-provisioning) are usually accessible through the Internet. Since they allow access to larger sets of resources than traditional hosting providers, they pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

Application Protection. Traditionally, applications have been protected with defense-in-depth security solutions based on a clear demarcation of physical and virtual resources, and on trusted zones. With the delegation of infrastructure security responsibility to the cloud provider, organizations need to rethink perimeter security at the network level, applying more controls at the user, application and data level. The same level of user access control and protection must be applied to workloads deployed in cloud services as to those running in traditional data centers. This requires creating and managing workload-centric policies as well as implementing centralized management across distributed workload instances.

Data protection. Here, the major concerns are exposure or release of sensitive data as well as the loss or unavailability of data. It may be difficult for the cloud service customer (in the role of data controller) to effectively check the data handling practices of the cloud provider. This problem is exacerbated in cases of multiple transfers of data, (e.g., between federated cloud services or where a cloud provider uses subcontractors).

Malicious behavior of insiders. Damage caused by the malicious actions of people working within an organization can be substantial, given the access and authorizations they enjoy. This is compounded in the cloud computing environment since such activity might occur within either or both the customer organization and the provider organization.

Business failure of the provider. Such failures could render data and applications essential to the customer's business unavailable over an extended period.

Service unavailability. This could be caused by hardware, software or communication network failures.

Vendor lock-in. Dependency on proprietary services of a particular cloud service provider could lead to the customer being tied to that provider. The lack of portability of applications and data across providers poses a risk of data and service unavailability in case of a change in providers; therefore it is an important if sometimes overlooked aspect of security. Lack of interoperability of interfaces associated with cloud services similarly ties the customer to a particular provider and can make it difficult to switch to another provider.

Insecure or incomplete data deletion. The termination of a contract with a provider may not result in deletion of the customer’s data. Backup copies of data usually exist, and may be mixed on the same media with other customers’ data, making it impossible to selectively erase. The very advantage of multi-tenancy (the sharing of hardware resources) thus represents a higher risk to the customer than dedicated hardware.

Visibility and Audit. Some enterprise users are creating a “shadow IT” by procuring cloud services to build IT solutions without explicit organizational approval. Key challenges for the security team are to know about all uses of cloud services within the organization (what resources are being used, for what purpose, to what extent, and by whom), understand what laws, regulations and policies may apply to such uses, and regularly assess the security aspects of such uses.

Requirements to secure cloud computing systems:

A. Traffic screening:

– Certain traffic is almost never legitimate – for example, traffic to known malware ports. If the cloud provider does not automatically screen traffic, the cloud customer should do so.

– Screening is generally performed by firewall devices or software. Some considerations:

– Does the provider publish a standard perimeter block list that aligns with the terms of service for the offering? If so, customers should request a copy of the block list; a reasonable block list can provide a customer with both assurance of a network protection plan as well as some functional guidelines on what is allowed. There may be some cause for concern if the block list is not in line with the terms of service.

– Does the provider's firewall control IPv6 access, or protect against both IPv4 and IPv6 attacks? More and more devices are IPv6 capable, and some providers forget to limit IPv6 access – which can allow an attacker an easy way around the IPv4 firewall.

B. Denial-of-service protection:

– Is the provider able to withstand and adapt to high-traffic attacks, such as Distributed Denial-of-Service attacks? DDOS attacks are commonly used for extortion purposes, and the ability of a cloud service provider and its Internet service provider to assist in blocking the unwanted traffic can be crucial to withstanding an attack.

– If the solution deployed in the cloud is accessed by the customer's customers, a DDOS attack against the cloud provider may result in loss of business for the customer.

C. Intrusion detection and prevention:

– Some traffic may initially look legitimate, but deeper inspection indicates that it is carrying malicious payload such as spam, viruses, or known attacks. The customer must understand whether the provider will block or notify the customer about this traffic.

– Intrusion detection and/or prevention systems (IDS/IPS) may be virtual or real devices. While a firewall usually only makes decisions based on source/destination, ports, and existing connections, an IDS/IPS looks at overall traffic patterns as well as the actual contents of the messages. Many firewalls now include IDS/IPS capabilities.

– Although technically not IDS/IPS devices, application-level proxies (such as e-mail gateways) will often perform similar functions for certain types of network traffic.

– An IDS will typically only flag potential problems for human review; an IPS will take action to block the offending traffic automatically. Some IDS/IPS considerations:

– IDS/IPS content matching can detect or block known malware attacks, virus signatures, and spam signatures, but are also subject to false positives. If the cloud provider provides IDS/IPS services, is there a documented exception process for allowing legitimate traffic that has content similar to malware attacks or spam?

– Similarly, IDS/IPS traffic pattern analysis can often detect or block attacks such as a denial-of-service attack or a network scan. However, in some cases this is legitimate traffic (such as using cloud infrastructure for load testing or security testing).

IV. RECOMMENDATIONS TO PROTECT

Cloud computing does not only create new security risks: it also provides opportunities to provision improved security services that are better than those many organizations implement on their own. Cloud service providers could offer advanced security and privacy facilities that leverage their scale and their skills at automating infrastructure management tasks. This is potentially a boon to customers who have little skilled security personnel.

As a result of our paper we can recommend ways of protection cloud computing by services. Threats on the services were given in [1].

A. Protection on Infrastructure as a Service:

– The application security policy should closely mimic the policy of applications hosted internally by the customer.

– The customer should focus on network, physical environment, auditing, authorization, and authentication considerations as outlined in this document.

– Appropriate data encryption standards should be applied in the handling of data and to user interaction (e.g., secure browsing) by the application.

– System assurance principles, and development and testing methods that minimize the risk of introducing vulnerabilities in the code, should be applied even more rigorously than for an on premises application, since the application will reside outside of the customer's security perimeter.

B. Protection Platform as a Service:

– The customer has responsibility for application deployment and for securing access to the application itself.

– The provider has responsibility for properly securing the infrastructure, operating system and middleware.

– The customer should focus on audit, authorization, and authentication considerations as outlined in this document.

– Appropriate data encryption and key management standards should be applied.

C. Protection Software as a Service:

– Application-tier security policy constraints are mostly the responsibility of the provider and are dependent upon terms in the contract and SLA. The customer must ensure that these terms meet their confidentiality, integrity and availability requirements.

– It is Important to understand the provider's patching schedule, controls against malware, and release cycle.

– Scaling policies help deal with fluctuating loads placed on the application. Scaling policies are based on resources, users and data requests.

– Typically, the customer is only able to modify parameters of the application that have been exposed by the provider. These parameters are likely independent of application security configurations, however, the customer should ensure that their configuration changes augment; not inhibit the provider's security model.

– The customer should have knowledge of how their data is protected against administrative access by the provider. In a SaaS model, the customer will likely not be aware of the location and format of the data storage.

– The customer must understand the data encryption standards which are applied to data at rest and in motion.

The customer needs to be aware of how sensitive data, as defined in their data classification, is being handled in general and by configuration options.

V. CONCLUSION

In this paper, different security issues faced by cloud computing are discussed along with the possible available remedies to these problems. It can be concluded that the data encryption and trust are the two major issues in this regard followed by the authenticity and data integrity. Also, in this paper are given several recommendations by services IaaS, PaaS and SaaS.

REFERENCES

[1] Tashev Komil Akhmatovich, Islomov Shahboz Zokir ugli, Zokirov Odiljon. “Analyze threats in cloud computing”. Journal of Electrical and Electronic Engineering. 2016.

[2] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture. “Cloud Security: A Comprehensive Guide to Secure Cloud Computing”. Indianapolis, IN: Wiley, 2010. 179-80.

[3] Boritz, J. “IS Practitioners' Views on Core Concepts of Information Integrity”. International Journal of Accounting Information Systems. Elsevier. Retrieved 12 August 2011.

[4] “Cloud security architecture”. Ericson white paper. 2015.

[5] A. Yun, C. Shi, and Y. Kim, “On protecting integrity and confidentiality of cryptographic file system for outsourced storage in Proceedings of the ACM workshop on Cloud computing security”, Chicago, Illinois, USA, 2009, pp. 67-76.