SECURE AND EFFICIENT CLOUD COMPUTING ENVIRONMENT

БЕЗОПАСНОСТЬ И ЭФФЕКТИВНОСТЬ В СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Dr. PhD Associate Professor Chaikovska M. , Chaykovskyy O.
Odessa I. I. Mechnikov National University, Ukraine, Odessa
e-mail: chmp@ukr.net, ochaykovskyy@gmail.com

Abstract: *The cloud computing environments are cost and productivity efficient, they are quickly replacing the traditional centralized systems. These "clouds" inherit a lot of security concerns of the older systems, but also bring the new ones. This paper examines 3 most popular cloud vulnerabilities, as well as a vulnerability intrinsic to the cloud environments. It proposes solutions and classifies the risks.*

KEYWORDS: CLOUD COMPUTING, DATA BREACH, DATA LOSS, PUBLIC CLOUD, VULNERABLE INTERFACES, HARDWARE FAILURES, COMPARTMENTALIZATION, ISOLATION, STRIDE.

1. Introduction

The twenty first century rapidly brought computerization onto the industry and society. No modern enterprise can progress without leveraging the power of computers and the informational fluency they provide. Even the first version of this paper is being written using the popular cloud-based editor "Google docs." Computer networks of the early twenty first century are getting replaced with even more ever-present cloud technologies, and is information being accessible by more people in more locations.

This blessing however brings its own curses with it. While intellectual cloud provides efficient access and processing of information, this information becomes more vulnerable to adversaries. Being interconnected and having multiple access points means more exposed surfaces for hacker attacks. Furthermore, cloud storages are not only vulnerable on the outside surface. They also need to ensure the proper separation within the cloud. With thousands of tenants reusing the same physical infrastructure, we need to ensure that everyone's privacy is respected.

In order to achieve efficient yet secure computerized environments, and cloud environments in particular, we explore common approaches to isolation, compartmentalization, continuous security updating, monitoring of failures and breaches, authentication, hardware, and software security primitives. We conclude that the scope of the attacks will only broaden in the future and solely a comprehensive and up to date security system can ensure necessary and sufficient protection.

What are the advantages of cloud computing and why do we care?[1] Microsoft Azure, one of the leaders of the industry, defines the following advantage:

Cost -- companies get significant savings from not having to manage their own on-site hardware.

Speed -- or rather capacity flexibility. A business can provision significant amounts of resources within minutes comparing to months if they had to deploy their own hardware.

Global Scale -- businesses can use exact amounts of computing resources they need in a given time, rapidly scaling them up or down depending on their demands.

Productivity -- with the hardware centrally managed by the cloud provider, economies of scale easily materialize into huge deployment and maintenance savings.

Performance -- cloud providers can and will invest into the top tier hardware and the latest software upgrades. Cloud providers also operate several data centers globally, reducing geographical latency.

Reliability -- cloud providers ensure high level of mirroring and data redundancy, making sure hardware failures do not lead to data loss.

2. Prerequisites and means for solving the problem

There are three main ways to deploy the cloud computing environment:

1. **Private Cloud**
2. **Public Cloud**
3. **Hybrid Cloud**

The **private cloud** deployment is the most similar to the traditional on-site data centers. The cloud is centrally deployed and is serving only one business or organization. It can be deployed on or off the site, and either directly managed by the company or outsourced to the third party for IT support. In the simple terms private cloud is a highly virtualized private network.

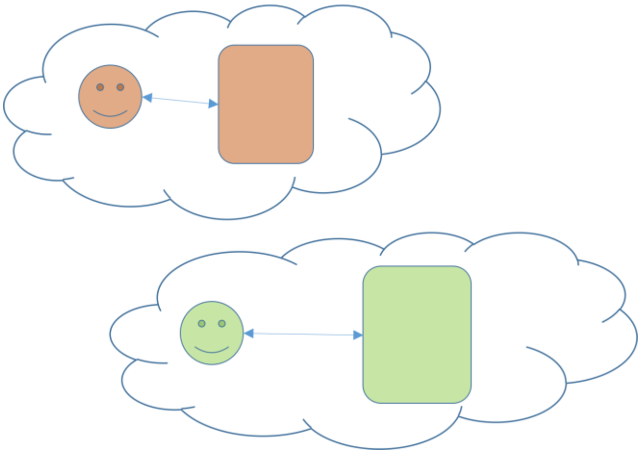

***Figure 1: Private Cloud** setup. Each user has their own cloud.*

In the **public cloud** deployment, all of the resources, hardware, and management of the cloud are controlled by the third party cloud service provider.

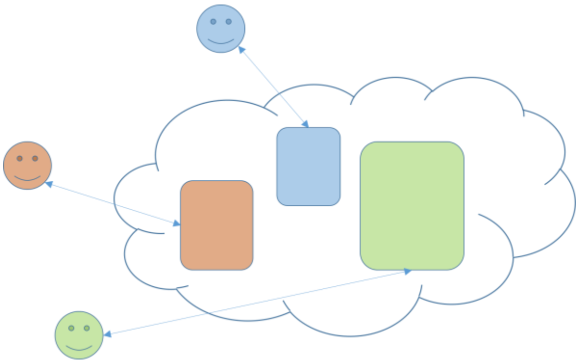

Figure 2: Public cloud - all the users share the same cloud

The third party has full control of the infrastructure, and users access it through the web portals, most commonly through webbrowsers. Examples of such clouds are Microsoft Azure, Amazon Web Services, and Oracle Cloud.

Hybrid cloud deployment combines the public and private cloud, bound together by a network technology to route traffic between them. Hybrid cloud gives users more flexibility and control over the deployment options.

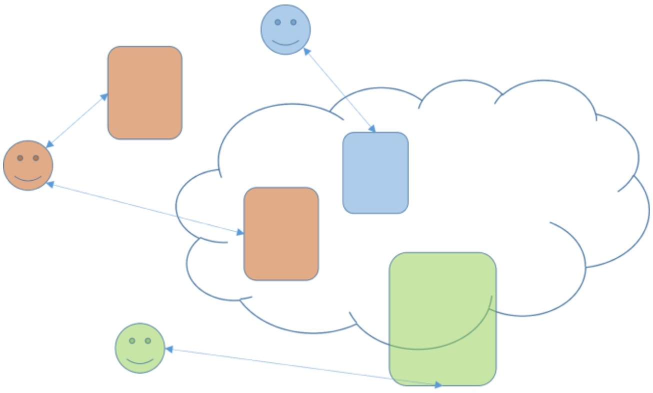

Figure 3 Hybrid cloud -- users utilize a mic of shared and private cloud and non cloud setups.

In the scope of this paper, we will only be concerned with the **public cloud**. This is the most popular and the "most cloud" type of deployment, and it is the most effective in showing advantages and shortcomings of the cloud based approach.

According to the Cloud Security Alliance, the top three threats in the cloud are **Insecure Interfaces and API's, Data Loss & Leakage, and Hardware Failure**—which accounted for 29%, 25% and 10% of all cloud security outages respectively[2]. We will discuss these three issues and possible mitigation techniques in this paper. In addition, we will discuss issues that pertain more specifically to the cloud-based systems, such as internal cloud isolation and compartmentalization.

In a typical cloud-based environment, the user does not have access to the hardware, and interacts with the system through a set of User Interfaces (UIs) or Application Programming Interfaces (APIs). Consequently, these become the most vulnerable attack surfaces, since the majority of commands and interactions go through them. Thus these interfaces need to be designed in such a way as to protect against both malicious and accidental misuse. As these interfaces are exposed to the internet and are accessed by a lot of users, they become even more prone to hackings and human-factor accidents.

Data Loss & Leakage (also known as Data Breach) is an incident when confidential information is released, viewed or stolen by an unauthorized actor. Data breach can be malicious, e.g a hacker gaining access to the data, or unintentional, e.g. human error in setting access permissions. While this threat is not unique to the cloud computing environments, their high data density and accessibility make them a likely target of a hacking attack. In addition, public opinion about the resilience of the cloud-based storage is significantly more volatile as a result of such breaches due to it relative novelty to the users. Damage to the user is quantified depending on the sensitivity of the information, while damage to the cloud service provider is harder to quantify as it can involve massive fines, legal consequences and most importantly loss of future revenue due to the loss of customer trust [3].

Hardware failures can represent a very significant issue for both cloud users and providers. It is also closely associated with data loss, in cases when the hardware was used for storage, but could also be connected to performance reduction, data access and others.

Lastly we need to discuss some of the issues specific to the cloud based computing environment. While these do not represent a significant portion of reported issues, they pertain specifically to the cloud setup, and the public cloud we are discussing in particular. A lot of the advantages of the cloud are attained by sharing the infrastructure. Often enough, the infrastructure hardware components (CPU caches, GPUs etc) were not designed with the cloud application in mind, and do not intrinsically provide any isolation in a multitenant setup of the cloud.

3. Solution of the examined problem

A good example of a successful attack on an insecure interface would be the US Internal Revenue Service (IRS) data breach in 2015 [4]. The IRS database represents a high asset target since it contains a lot of personal information about taxpayers, which can be used in identity theft. The IRS only used a single tier authentication, based on the user attributes such as their Social Security Number (SSN). This incident highlighted the importance of using the "Adaptive approach" to security, when access rules are configured dynamically based on machine learning and statistical models. These techniques are still being developed, but some good examples include learning to distinguish "good" from "bad" access scenarios. Examples of "good" scenarios would include user accessing his account from a usual IP address, entering his password on the first try etc. Examples of "bad" behaviors include random access from suspicious IPS, high access error rates, bruteforce attempts at guessing the credentials etc.

There is a number of possible approaches cloud providers that are used to protect the cloud data from breaches. They are all centered around good software engineering and protecting the main attack surfaces and APIs, such as scalable identity management, strong password requirements, ongoing automated rotation of cryptographic keys, passwords and certificates. Most of these approaches are rolled over from the traditional non-cloud systems, so it is important to scale them appropriately to the multi-million user requirements of the cloud computing environments [5]. Unfortunately, none of those guarantee a hacker-proof environment. Even the strongest system is sensitive to human errors. Consequently, users should be proactively responsible for protecting their data. The two main approaches for that are multifactor authentication and encryption. Multi Factor authentication makes it harder for a hacker to impersonate an authorized user and gain unauthorized access to the data. Authorized users must have access to a second mode of authentication beyond their password, such as a smart card or a phone. Even if an attacker gains access to the passwords, he is unlikely to have access to the second mode of authentication. Encryption provides security for the data even if it is leaked. However, encryption cannot prevent unauthorized deletion of the data [6].

Hardware failures were just as much of an issue in the older non-cloud system. Mitigation approaches here are similar. First and foremost cloud provider had to be concerned with the data redundancy, where any particular piece of data has to be stored on multiple units of hardware.

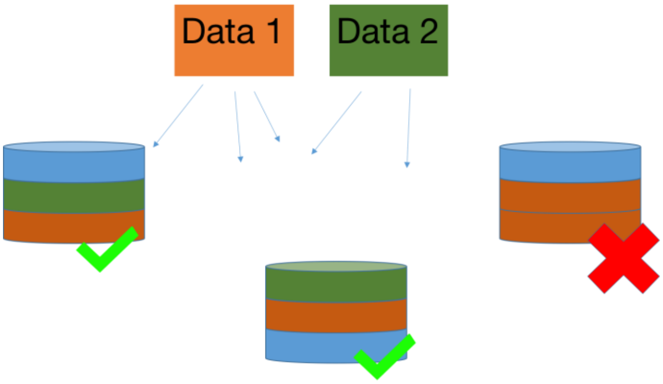

Figure 4: Redundancy for data. We need to male sure copies of data are properly distributed among the hardware nodes

Good redundancy practices include efficient fragmentation of data and geographic distribution of copies. In other words, we make sure that the data is split into not-too small and not too-big chunks, that are easy to move around, but losing one of the copies will not significantly slow down our system. We also need to make sure that if one datacenter in Europe goes down, say due to a natural disaster, we have a copy of the data on a US server.

In order to mitigate the internal breach concern, the cloud provider needs to ensure proper isolation and compartmentalization of the cloud. It is important to enumerate all the possible access surfaces and make sure that all of them follow the rules and specifications. In a simple example: imagine a hardware machine hosting a cloud and two users hosting their data on that cloud. We want to ensure that under no circumstances users can access the data of each other. Possible approaches for that include multi-factor authorization on all separate hosts, Intrusion detection systems, least privileged access approach segmentation and careful monitoring of shared resources.

The compartmentalization can also help us mitigate influences of other vulnerabilities. Imagine that one of the customers in the example above is breached. If our system is properly compartmentalized, we can make sure that the other customer is safe. In the opposite scenario, the malicious actor would likely be able to spread across more and more users and machines, after finding just one vulnerability and entering the system through it.

4. Results and discussion

Microsoft has developed a computer security threat classification model called **STRIDE**. It encompasses six major threat categories, which provide a helpful mnemonic:

1. **S**poofing of user identity
2. **T**ampering
3. **R**epudiation
4. **I**nformation disclosure
5. **D**enial of Service
6. **E**levation of Privilege

All of the threats we discussed above are related to one or several of these categories. Similarly, the mitigations also help us to secure one or several of these categories.

Table 1: Threat classification

	Data Breach	Insecure Interfaces and APIs	Hardware Failure	Improper Compartmentalization
Spoofing				
Tampering		■		
Repudiation	■	■		
Information disclosure	■	■		■
Denial of Service	■		■	
Elevation of Privilege		■		■

Our proposed mitigations overlap the issues and provide additional advantages. First let us consider the adaptive security approach. It can be separated into two main stages: data collection (or algorithm drafting) and actionable items. Collecting data about the usage of our system can not only help us to make it more secure, but also improve its efficiency and usability. It is however important to take user privacy considerations seriously.

Multi factor authorization is becoming an industry standard. The old login/password paradigm is way too vulnerable to theft and hacking. In the meantime, obtaining a physical device would be beyond hacker possibilities in the most cases. This approach, if implemented correctly, also can be very efficient and user friendly. Instead of remembering dozens of complicates passwords user can use his physical device, such as the phone.

While the primary goal of encryption presented in this paper is to prevent third-party attackers from using stolen data, it can also help user privacy concerns related to the cloud service provider. Per most user agreements, data belongs to the user, not to the provider, and its usage is strictly regulated. Having the data encoded makes sure that there is no risk of cloud service provider intentionally or unintentionally using it in violation of said user agreement [7].

Data redundancy, when implemented on a global scale, can also significantly reduce latency. Think of a previous example with datacenters in Europe and the USA. While their primary goal is to prevent all the data going down simultaneously, they can also make sure that users get access to the closest copy of data. A user in New York will download a file faster from a US server than from a server in Europe.

Overall we can see that often enough theses approaches serve both as a security and a performance improvement. Which is vital for the profit-oriented business to be incentivized in using these.

5. Conclusion

Cloud computing is a relatively new, yet powerful technology. It provides a lot of advantages comparatively to the traditional centralized systems. The security considerations for a cloud based system are in many ways similar to the centralized system once we take the massive scalability into account. There are however a number of additional security consideration we need to be aware of when we are dealing with the public cloud. The shared hardware introduced additional surfaces of vulnerability.

In the end, we need to accept that no system is ever fully secure. We need a dynamic, comprehensive approach, that includes all of the known principle of computer system security and we have to be ready to adapt it to the new challenges coming up.

6. References

1. Microsoft Azure. Official site. What is the cloud computing? - https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

2. Top Threats Working Group. The Treacherous 12. Cloud Computing Top Threats in 2016. – CSA, 2016. – 35 p. - https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

3. Chaikovska M. Adoptive models of management modern IT-projects/ Materials I International Scientifical and Practical Conference Forsight-management: best world practice of development and integration of education, science and business.- Tbilisi:TSU, 2017. – c.114-116.

4. Subra Kumaraswamy. The IRS Breach and the Importance of Adaptive API Security, JUN 05, 2015 - https://apigee.com/about/blog/technology/irs-breach-and-importance-adaptive-api-security

5. Security Guidance for Critical Areas of Focus in Cloud Computing. – CSA, 2014. – 177 p. - https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf

6. Чайковська М.П. Моделювання комплексної системи інформаційної безпеки організацій в сучасних економічних реаліях/ А.С.Азеєв, М.П. Чайковська //Global aspects of World Economy and International Relations in an unstable economy. – Polska, Czestochowie, Akademia Polonia, 2016. – C.879-889.

7. Чайковська М.П., Азєєв А. С. Сучасні напрямки типологізації інформаційних загроз та тренди ринку інформаційної безпеки// "Економіка та суспільство" # 13/2017. Електронне фахове видання. Мукачівський державний університет . - http://www.economyandsociety.in.ua/index.php/journal-13