Quantifying security risks in the cloud environment in the quest for minimizing energy consumption

S Eftimie[1] , M Rogobete[2] and C Răcuciu[3]

[1] Military Technical Academy, Bucharest, Romania
[2] GE Power Romania
[3] Titu Maiorescu University, Bucharest, Romania

Abstract. In this paper we investigate the practices and methods used for quantifying the security risks involved with the usage of cloud services. The usage of external cloud services greatly reduces the consumption of energy related to hardware and the industry needs a way to evaluate those risks and address them accordingly. This work proposes a unified framework for quantifying security risks that enables companies to reduce operational risk related to cloud while minimizing energy consumption and reducing the environmental impact.

Keywords: Cloud, Framework, Risk quantification, Energy consumption

1. Introduction

Cloud computing has become a highly innovative space with an active community and a growing client base. Current developments in technology and the increasing focus towards mobility have changed the way we look at cloud and its inherent issues. Businesses and individuals have begun to use external cloud servers managed by other companies to access data or computing services from any physical location. This move came with a major trust concern related to cloud providers.

Security remains one of the major obstacles to large-scale cloud adoption. SaaS (Software-as-a-Service) providers are working to secure their products to protect their business. A breach may have a devastating effect to a company since image damages can translate to huge financial losses. SaaS providers invest in security products and hire good talent to protect their business and work on preventing attacks to their infrastructure, such as denial of service attacks. Since SaaS providers do not prioritize the security related to the client’s access control policies, the companies that use their services should implement their own security measures.

The biggest risks that the consumers of cloud services are facing are related to the data disclosure or data loss. The benefits of cloud computing are significant: low cost, high reliability and immediate availability of additional computing resources when needed. Despite these advantages, both cloud service providers and consumers must be aware of their own set of unique risks of cloud computing, which is usually associated with storing and processing data.

In the recent years, there have been a series of incidents in which customer data hosted in the cloud was released online (for purposes of hacktivism and vandalism) or stolen for criminal purposes. Cloud computing is made possible using technologies such as Internet access, virtualization and third-party data centres. In the case of online access to a cloud service provider, access controls take the form of usernames and passwords. In the case of virtualization, such access controls can be implemented through the logical separation of data. In the case of third-party datacentres, such access controls may take the form of physical access controls or software-based access to prevent unauthorized access to customer data of people working in the organization.

In principle, the access controls mentioned above are solid. However, in practice, such controls have been circumvented. If any of those access controls are compromised, the risk of data leakage is high. However, in the event of a data breach where the associated data is acquired in encrypted form, it is essentially useless for an attacker (unless the encryption algorithm used is weak and / or the attacker knows the associated decryption key).

Otherwise, if a security breach occurs and the associated data in plain text is stolen by the attackers, the effects can be disastrous for a company, from negative publicity and damaged reputations to fines in accordance with the data protection legislation.

A framework that would allow a transparent communication of the security risks that would essentially put actual value on possible security events in the cloud environment would allow stakeholders to make informed decisions and better understand the impact of a potential cyber-attack. For this reason, we have started to investigate ways in which we can quantify risks in ways that can be easily understood by non-technical people.

2. Risk quantification

Risk quantification represents the process of assessing the dangers that have been recognized for a project and building up the information that will be required for addressing them. Risk management is performed during the whole duration of a project. During a project, there are situations where both qualitative and quantitative analysis are required. The target of the risk quantification is to set up a method for arranging the risks in the order of their impact on the business. The next step is to address them using this classification and it is expected that in most projects there won't be sufficient time or money to address every risk that is recognized. One practical measure for evaluating risks represents the severity of the risk. Severity can be though as a pair combination between the risk impact and the risk probability. A quantitative investigation should be made with care since utilizing bad or wrong data can lead to bad decision making regarding the risks. There should also be an assessment regarding to the collection of data because the total cost of the risk can be lower than the collection of data used to quantify it.

In a previous work [1] we have identified the threats and risks involved with cloud computing. Other works such as [2] have categorized those risks into general ones, risks that emerge from the service models and risks that emerge from deployment models as can be seen in table 1.

Table 1. Cloud computing risks

		Specific risks	**General risks**
Service model	IaaS	Malicious insiders	Data breaches Data loss Account hijacking Insecure APIs Denial of Service Cloud abuse Malicious insiders Shared technology vulnerabilities Insufficient due diligence
Service model	PaaS	Loss of control over hosted applications	
Service model	SaaS	Loss of data ownership	
Deployment model	Public Cloud	Tenant breach	
Deployment model	Private Cloud	Insufficient resources	
Deployment model	Hybrid Cloud	Interdependence risk	
Hosting type	External hosting	Resource relocation Environments are not isolated	
Hosting type	Internal hosting	N/A	

Qualitative risk assessment is suitable early in the implementation of a solution and its scope should be the categorization of the risks and the appropriate actions that need to be made to address them. This type of analysis does not give an exact value of the risk but it's useful in the case of a short assessment period. When using this type of analysis, quantitative values can be associated with the identified risks to calculate their severity.

Cloud risk management is difficult because the technology is not controlled by the company that uses it. Conventional risk frameworks such as [3] ISACA [4], are not entirely suitable in the cloud environment because they were conceived for other types of risk.

Companies are finding hard to assess the cloud risk for a few reasons. The rapid developments in technology make it hard to identify security controls and risk parameters. Cloud providers also update constantly their service and infrastructures.

This leads to the conclusion that new risk frameworks must be developed to meet the demands of the new advancements surrounding cloud. Risk quantification is particularly useful when interacting with stakeholders. Decisions regarding the usage of different cloud services should be made in respect to the risks involved and a good measure can be represented by the balance between investment and risk.

The European Network and Information Security Agency (ENISA) released a risk assessment framework [5] for the cloud environment that has become a standard in the industry. Two documents are part of the ENISA release, a cloud information assurance framework and a guide for risk assessment. The agency completed an investigation of the risks and advantages of using cloud services and its essential goal is to decrease the identified risks to a satisfactory level. ENISA has distinguished technical, legal and organizational risks that need to be assessed before the cloud adoption.

The risk management is the next logical step after the risk assessment. In traditional IT systems, risks were identified based on critical areas, quantified, evaluated and addressed accordingly. Cloud has added a layer of complexity that has yet to be solved. There are still unanswered questions regarding the segregation of duties between the cloud provider and clients.

In [6] a framework is proposed that uses an incremental approach that can enable, plan, screen and manage information security in cloud services. The framework uses a model that is based on multiple criteria that incorporates static and dynamic measurements. The main objective of this framework is to make the security administration a continuous process.

Another proposal for a risk assessment framework can be found in [7] where the authors include the cloud users in the overall risk assessment by applying a so-called analytic hierarchy process that quantifies the risk.

The starting point for an organization can be any type of these frameworks and an effort should be made to investigate and utilize methods from more than one and create and adapt according to the organization's unique needs.

Moreover, existing frameworks are less prescriptive about internal controls suitable for hybrid cloud setups and center around controls that the cloud suppliers usually set up inside their infrastructures. During the overall risk management, it's important that the information security controls such as encryption and key administration, authentication, data breach warnings and legal controls are performed, and they should also be specified in the service agreements with the cloud providers.

The risk appetite of a company represents a concept that is opposite to risk management. It's basically a measure of the amount of risk that a company is willing to take to pursue its business initiatives. Cloud computing is relatively new in terms of adoption and presents a unique set of risks. Due to the rapid evolution of the technologies in this area, the awareness over a company's risk tolerance can have a strategic importance.

The assessment of a cloud risk appetite needs to take several factors into consideration. The risk tolerances of similar businesses need to be evaluated to have a good balance between risk and innovation on the market. For businesses that are moving to cloud, there is a possibility that risk assessment has already been done in the past and that there are items that can be reused and adapted to the new cloud paradigm. Technology and the future strategy of the company also need to be taken to consideration when assessing the risk tolerance.

The final step is the formal documentation of the risk appetite. This document should be made available to the organization's staff so that they act accordingly.

4. Framework proposal

Cloud access security brokers are cloud-based or on-premises security policy enforcement points, placed between cloud service providers and cloud consumers. CASBs consolidate multiple types of security policy enforcement [8]. One of the features of CASBs is the comparison between different SaaS vendors highlighting different aspects regarding security. There are several CASBs vendors on the market and each one of them has its own set of features. For an organization that wants to adopt different SaaS solutions for its business, it's difficult to assess the risk for different SaaS vendors and it's difficult to choose a CASB vendor to address those risks. This leads to the conclusion that there is a need for a standardized way of assessing risk in cloud which has been proved to be difficult as we have seen in the previous sections of this paper. As a solution, we propose a unified framework for quantifying risk to resolve this issue. These are its core principles:

- Usage of the CSA approved list of cloud risks
- Transparency to stakeholders
- Ease in assessing CASBs
- Cloud community participation to the framework
- Anonymous submission of reported losses
- Cost efficiency

The accurate communication regarding the cyber risk involved with the cloud adoption represents the main challenge that chief information security officers face when dealing with upper management boards. One obvious way to quantify a risk represents the loss in money. This is a familiar concept to stakeholders, it's easy to understand and allows key people to make informed decisions about the SaaS that they want to adopt, evaluate the costs involved and balance the risk and opportunity [9].

Table 2. Quantification example of cloud risks associated with a SaaS solution

Cloud Risk	CASB Costs	Risk Mitigation	Total Investment	Risk Value	Risk Tolerance
Data Loss	€3000	€5000	€9000	€300000	0%
Data Breaches		€1000		€10000	0%
Account hijacking	€1000	€2000	€3000	€10000	10%
Insecure APIs	€5000	€2000	€17000	€20000	30%
Denial of Service		€3000		€3000	30%
Cloud abuse		€5000		€12000	50%
Malicious insiders		€2000		€20000	10%
Shared technology	€0	€1000	€1000	€6000	10%
Insufficient due diligence	€0	€1000	€1000	€6000	10%
Total	**€8000**	**€22000**	**€30000**	**€117000**	**N/A**

In table 2 we can observe an example where risks are assessed for the adoption of a SaaS solution. The CASB Solution can offer discount packages as part of the offer, for example data loss and data breach mitigation security products are bundled together. Although CASB products are advanced, additional security measures need to be implemented on-premise and their costs should be taken into consideration.

We propose that the value for a specific cloud risk be calculated using the following formula:

$$Rc = \frac{\left(\frac{Li}{Vi} + .. + \frac{Ln}{Vn}\right)}{n} \times Vc \times (1 - Tc)$$

The risk is expressed in an actual amount of money, $\boldsymbol{Rc}$. First, we calculate an average of the monetary losses caused by attacks relative to the respective values of the companies. There are multiple ways to assess the value of a company: Market Capitalization, Times Revenue, Earnings Multiplier, Discounted Cash Flow, Book Value, Liquidation Value and for accurate results we note that the same method should be used for one calculation. $\boldsymbol{Li}$ represents the loss associated with a cloud risk experienced by a company that has the value $\boldsymbol{Vi}$**.** The average result expressed as a percentage is then multiplied by the value of the company $\boldsymbol{Vc}$ that addresses a cloud risk. $\boldsymbol{Tc}$ represents the risk tolerance of the company to that specific cloud risk, expressed as a percentage. For example, if the company's tolerance towards data loss is 10% the value obtained after taking in consideration the company's value will be multiplied by 90% (1-10%).

The value obtained should be a starting point for the quantification of the risk [10] since it expresses real losses that can occur in the case of a security event and can be altered if the CISO for example decides that the respective case is not applicable to the business that he is trying to protect.

Getting the correct loss values and valuating the companies are the most difficult steps. We believe that a platform that would ease the reporting of such events and make the cost transparent is necessary. This would need the participation of the whole cloud community and companies should be transparent about the attacks they suffer which is not an easy thing to do since even news about the attacks would cause financial losses to their business. Multi-party computation (MPC) is used to describe a form of computation that can be performed over a series of private inputs. In an MPC scheme several participants want to compute the value of a public function on their private data while keeping their inputs secret. The goal of MPC is to build an algorithm where the participants can obtain the result of the function without having to rely on a third-party entity. We hope that this will be a subject for future work since it's a plausible way to deal with the anonymous submission of losses.

Once we have an assessment of all the risks applicable to the business and the associated monetary losses attached to them, a comparison can be made between the different security brokers considering the points where the CASBs will address those risks. In some cases, additional security measures will have to be put in place by the CISO department and they should also be quantified.

Once they are presented an overall view of the costs involved, board members can make a cost decision regarding the adoption of a particular SaaS solution and regarding the risks involved and the cost of their mitigation. The assessment part and the valuation of the companies are not easy to perform but we envision a collaboration of the cloud community for this common scope.

5. Conclusions

Although cloud computing has brought many advantages to companies, it has opened the doors for new security issues. The use of traditional models for risk assessment is not suitable for the new cloud computing landscape due to the new types of threats and new attack surfaces. In this paper we have analyzed several risk assessment methods and we have proposed a framework that helps the risk assessment of SaaS solutions in a manner that is easy to communicate to non-technical people. The SaaS market has experienced significant growth and the security breaches continue to fuel cybersecurity market growth as well. CASB's are just one of the technologies that have emerged in this new cloud security landscape. In this context, a method for assessing security risks is essential for a company that wishes to implement several SaaS solutions and wants to take advantage of a CASB. The proposed framework is designed to close the communication gap between the CISO department and the board members of a company. A clear understanding of the cloud risks impact over time can help companies to tolerate a higher level of risk in an efficient way.

6. References

[1] Răcuciu C and Eftimie S 2015 Security threats and risks in cloud computing *Mircea cel Bătrân Naval Academy Scientific Bulletin*, vol **18**, pp. 105-108

[2] Belbergui C, Elkamoun N and Hilal R 2017 Cloud Computing: Overview and Risk Identification Based on Classification by Type *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), Rabat, 2017,* pp. 1-8

[3] Maneerattanasak U and Wongpinunwatana N 2017 A Proposed Framework: An Appropriation for Principle and Practice in Information Technology Risk Management *2017 International Conference on Research and Innovation in Information Systems (ICRIIS), Langkawi, 2017,* pp. 1-6.

[4] ISACA 2009 The risk IT Framework *Information Systems Audit and Control Association*

[5] Madria K 2009 Cloud Computing Risk assessment *Missouri University of Science and Technology*

[6] Djemame K, Armstrong D, Guitart J and Macias M 2016 A risk assessment framework for cloud computing *IEEE Transactions on Cloud Computing*, pp. 265-278

[7] Cayirci E, Garaga A, Oliveria A and Roudier Y 2016 A risk assessment model for selecting cloud service providers Journal of Cloud Computing, p.14

[8] Eftimie S, Dumitru L and Opriș V 2016 Cloud Access Security Brokers *Education and creativity for a knowledge-based society International conference 2016*

[9] Deloitte 2016 The value of cyber risk quantification, pp. 1-7

[10] Filkins B 2016 Quantifying risk: closing the chasm between cybersecurity and cyber insurance *SANS Institute, 2016*, p.3