Towards a Cybersecurity Model for Selecting the Secured Cloud Service Provider using Security Risk Approach

Jamal Talbi
Computer, Networks, Mobility and Modeling laboratory
Department of Mathematics and Computer,
FST, Hassan 1st University, Settat, Morocco
e-NGN Research group, Africa and Middle East

Abdelkrim Haqiq
Computer, Networks, Mobility and Modeling laboratory
Department of Mathematics and Computer,
FST, Hassan 1st University, Settat, Morocco
e-NGN Research group, Africa and Middle East

ABSTRACT

Cloud computing is a rising field providing computation resources. It represents a new paradigm of utility computing and enormously growing phenomenon in the present IT industry and economy hype. The companies which provide services to customers are called as cloud service providers. The cloud users (CUs) increase and require secure, reliable and trustworthy cloud service providers (CSPs) from the market. So, it's a challenge for a new customer to choose the highly secure provider. In this paper, we propose a cybersecurity model to analyze and select the secured cloud service provider. This model uses a CSP Rank Framework for the group of cloud providers by assessing security risks in terms of confidentiality, integrity, availability, non-repudiation and authenticity which make decision of the more secured provider among the available providers list and justify the business needs of users in terms of security and reliability.

Keywords

Cloud Computing, Cybersecurity Model, CSP Rank Framework, Security Risk.

1. INTRODUCTION

Cloud computing [1] is an active research subject as the information industry sees it as the new model. Many companies, enterprises and organizations outsource some of their information systems to benefit from the cloud services which are Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). The main interesting features of a cloud are the cost decrease and a faster time to market. Based on sharing resources, the cloud computing changes the user concerns from managing an infrastructure to only focusing on their core business. Currently there are many numbers of providers [2], but finding the best cloud service provider among the available cloud service providers is difficult. Thus, it is a challenge for the users to choose the best secured cloud provider for fulfilling their requirements. Presently, there is a lack of frameworks that can permit customers to evaluate cloud offerings and rank them based on their ability to meet the user's quality of service (QoS) and security requirements. This is a major problem for every user, especially those who are more concerned about data security and privacy from CSP.

A secure computer system provides guarantees regarding the confidentiality, integrity, availability, non-repudiation and authenticity of its objects (such as data, processes or services). Security is related to vulnerabilities in software, and these are hard to foresee or detect before an actual attack; security involves personal aspects (e.g., user or operator issues) and aspects of the operational environment that are often beyond the control of the development teams. Thus, it is necessary to assess and contain risk using precautionary measures that are commensurate. Accordingly, we have to dispose a system that measure and rank the secured cloud service providers and then, the cloud services can make a major impact and will craft a healthy competition among cloud providers to satisfy their service level agreement (SLA) and improve their QoS and trustworthiness.

The principle aim of this work is to help a new customer to find the most reliable and secured CP in terms of security and trust through a broker framework that can define, analyze, measure and rank the cloud service providers based on a security risk analysis that calculate some metrics. Thus, the obtained results make decision of the best option of CP and justify the business needs in terms of security and reliability.

The paper is organized as follows: the next section discusses related work, Section III introduces the architecture of the proposed model. Section IV describes the CSP Rank Framework. Section V presents an implementation and experimentation of the model. Section VI gives a conclusion.

2. RELATED WORK

Security metrics are one of criteria that play a major role in ranking service providers. A cloud user may require an efficient, cost effective and basically more secure provider for his application. Since there are many providers who will provide same type of services with different level of security, so it will be a challenge for the user to select the best choice. Thus, the motivation is to promote a novel approach for selecting the secured providers based on measuring security metrics of cloud services.

In the same context, many researchers have proposed different approaches to help customer in this mission to select the appropriate cloud service. A collaborative filtering approach [3] rank the items based on similar users preferences. This algorithm aggregates all the items purchased by the users and eliminate those items and ask users to rate the remaining services. In [4], cloud rank approach proposed greedy algorithm. It gives a method to rank cloud providers based on existing customer's feedback. It ranks component rather than service of providers. But there is no guarantee that all explicitly rated items by customers are ranked properly.

But similar users will experience the same with same cloud providers so for them this approach will be helpful.

QoS-aware web by collaborative filtering [5] proposed a collaborative approach to rank providers on the basis of its web services. This method is useful for the customers who want to get an appropriate cloud provider which provides suitable web services. Thus, this method includes experience of users who used the services already and a hybrid collaborative filtering approach for evaluating web service QoS parameters.

Parveen Dhillon [6] proposed an effective and efficient method to select best cloud service. In order to select the best provider, three parameters are considered. Instead of taking all three parameters together applied. They made a ranking in where the best provider obtained is selected.

Zibin Zheng [7] proposed an approach for ranking equivalent cloud service providers by providing the similar kind of services which will help users to select suitable providers without spending much time for it. This method uses some QoS parameters for predicting best provider.

Deepak Kapgate [8] proposed a predictive broker algorithm based on Weighted Moving Average Forecasting Model (WMAFM). It proposes a new method to balance load on data centers and also minimizes response time. So for end users, they can get their requested service within few seconds.

Subha [9] had done a survey on quality of service ranking cloud computing. Here the author considered few qualities of service parameters and ranked providers based on that.

Cloud Rank [10] approach measures and ranks cloud services for the users. It takes the feedback or rating of users who had used the services already.

An efficient approach [2] find the best cloud provider by using a system for ranking cloud services based on QoS parameters such as service response time, cost, interoperability and suitability. It uses a broker algorithm that classify the existing providers and find out the more effective and efficient provider.

A sophisticated study [11] proposed ranking frameworks in cloud computing based on QoS parameters to select the best possible service provider.

Gani [12] proposed a conceptual model of federated third party cloud ranking and monitoring system (CMFCSPRS) that assures and boosts up the confidence to make a feasible secure and trustworthy market of CSPs.

3. THE PROPOSED MODEL

This paper proposes a CSP Rank Framework (see Figure 1) which can act as a middleware between customer and cloud service provider. It can get the needed requirements from customer and help the customer by listing out suitable cloud providers. So this model has an important role to find out the secured cloud service providers existing in the database of the broker. The proposed model is described in the following, in terms of its architecture.

This system develops a model to find out the secured cloud service providers based on a security risk assessment approach by determining the vulnerabilities and computing the risks related to cloud service providers list.

3.1 Requirements Requested

The broker collects security requirements from user. It may be infrastructure requirements, platform requirements or software requirements.

3.2 Threat Identification and Risk Assessment

All the registered cloud service providers give all the services which they are providing. Cloud broker contains the level of security of cloud providers. So the client gives requirements to broker, it checks the provider’s performance based on criteria that are risks computed.

3.3 Ranking Secured Cloud Service Providers

The CSP Rank Framework using a broker provides optimal cloud service provider selection from the more numbers of CSPs based on security metrics, especially risks which provides better selection of providers among many. Thus, the proposed architecture uses evaluation of risks related to systems caused by vulnerabilities and threats for making a decision to rank and select the right provider in terms of reliability and security.

4. DESCRIPTION OF THE CSP RANK FRAMEWORK

Normally all cloud service providers have a Service Level Agreements (SLA) [13], but most of these SLAs were written to protect the vendors as opposed to being customer-centric. That has to change, and customers have to demand more with regard to service and the assurance of it. In the same time, cloud providers should protect their data or services from risk and harm. For this aim, the CSP Rank Framework will conduct vulnerability and threat scans of components and services of the existing providers. The obtained results were fed into the security ranking system that offer a list ranked of the secure providers.

The conceptual model of the broker for selecting secured CSPs (see Figure 2) contains four stages in the process to select the secured providers. For this aim, some assumptions and conditions should be considered as follows [12]:

- The CSP Rank Framework must maintain the trust and reliability.
- The CSP Rank Framework has enough resources to provide for processing and executing their own work.

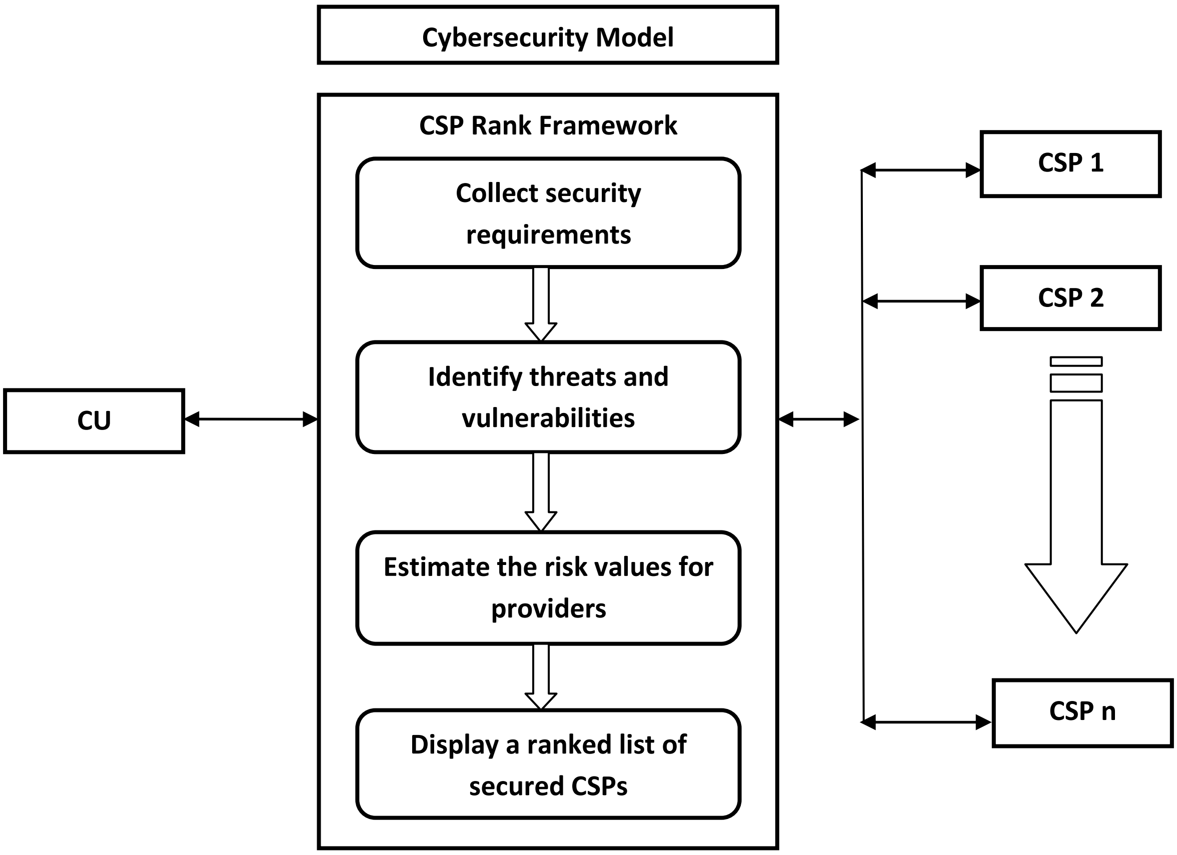
Cybersecurity Model
CSP Rank Framework
Collect security requirements
Identify threats and vulnerabilities
Estimate the risk values for providers
Display a ranked list of secured CSPs
CU
CSP 1
CSP 2
CSP n

Fig 1: The structure of the proposed CSP Rank Framework Model

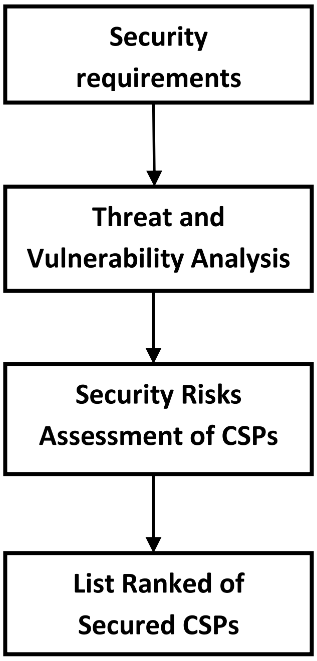
Security requirements
Threat and Vulnerability Analysis
Security Risks Assessment of CSPs
List Ranked of Secured CSPs

Fig 2: Conceptual model of CSP Rank Framework

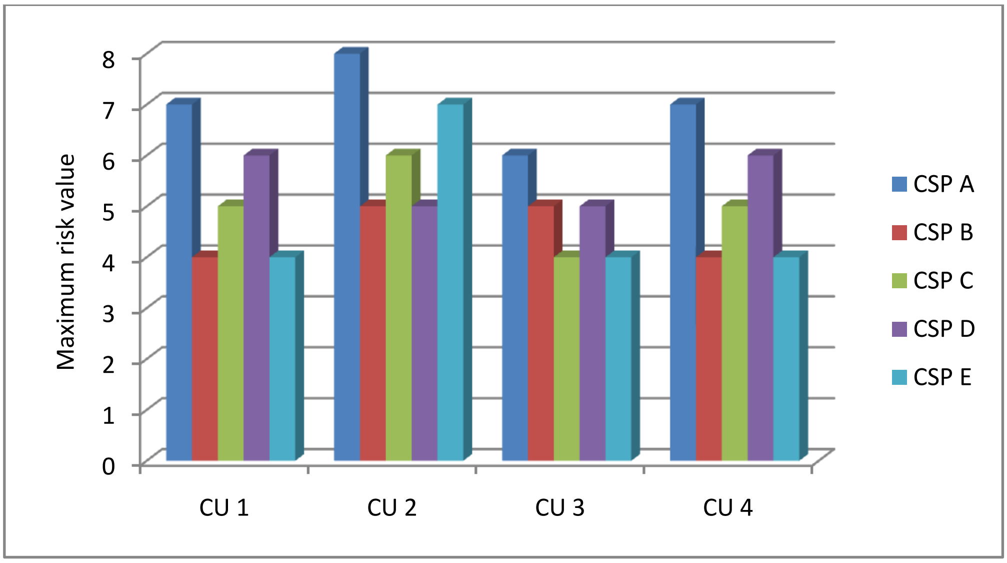

Fig 3: Comparison of risks in cloud users for the five cloud providers

- The broker must be maintained and regulated by strict laws and transparent policies.
- Both the broker and CSPs mutually agree before executing the software penetration test.
- The CSP provides IaaS, PaaS and SaaS of its own.
- The CSP Rank Framework is only the responsible of computing security metrics from sources and processes these measures for ranking results.
- A new cloud user looking for security and reliability should pay to the broker to see the ranked results.

4.1 Security Requirements

The CSP Rank Framework uses the five CIANA objectives (Confidentiality, Integrity, Availability, Non-Repudiation, and Authenticity) to define the security need of each cloud user. If the customer needs the objective, the value is equal to 1, otherwise to 0.

4.2 Threat and Vulnerability Analysis

Vulnerability is a software defect or weakness in the security system which might be exploited by a malicious user causing loss or harm [14]. The identification of these vulnerabilities has been used by several approaches and researchers to estimate risks of the systems. In this case, we take into account five cloud security threats given by the Cloud Security Alliance (CSA) [15] to evaluate the risks. These threats are each related to the 5 CIANA objectives:

- Data Breaches = {Confidentiality}
- Data Loss = {Availability, Non-Repudiation}
- Account Hijacking = {Confidentiality, Integrity, Availablity, Non-Repudiation, Authenticity}
- Insecure Interfaces = {Confidentaility, Integrity, Authenticity}
- Denial of Service = {Availability}

These relations with the security needs of each cloud user are combined to obtain a function called harm. This later is defined on each customer, for each threat through the sum of the affected security needs. For example, the Insecure Interfaces threat (t) has the following harm on the cloud user (k) with the security needs (Confidentiality, Integrity, Non-Repudiation):

$$Harm(t,k) = (1\times1) + (1\times1) + (0\times0) + (0\times1) + (1\times0) = 2$$

where the first value of each bracket is equal to 1 if the threat correpond to the objective, 0 otherwise, and the second value is related to the security need.

4.3 Measuring Security Risk Assessment

Once the harm of the threats on each cloud user is calculated, the response to these threats for each cloud provider has to be determined. For this aim, it's necessary to use the STAR Registry and the matrix defined by the CSA [15].

The CSA matrix defines a list of security controls that a cloud provider should implement to reduce security risks. Each of these controls can be related to one or multiple threats. In addition, the STAR Registry publishes the list of implemented controls for providers willing to follow these recommendations.

In this case, two information are used as binary values (a control mitigates a threat or not / a control is implemented by a provider or not) to calculate the coverage score, which indicates the response of a provider to a given threat. This value is a percentage, if the provider implements all controls mitigating a threat, it gets a coverage for this threat of 100%. Thus, this percentage is brought to a score on a scale of 0 to 5 (with 5 equivalent to 100%).

Usually, the vulnerability are assessed and used to calculate a risk value of an information system [16]. But in a cloud context, providers may be tempted to conceal their vulnerabilities for security reasons. This is why we use the coverage based on the security controls. By using the maximum possible coverage value $Covg_{max}$ (in this case 5), it is possible to get an equivalent to the vulnerabilities. Therefore, by combining this value with the harm, the risk formula can be defined for a threat t, a cloud user k and a provider CSP p as follows:

$$Risk(t,k,p) = Harm(t,k) + (Covg_{\max} - Covg(p,t))$$

4.4 List Ranked of the Secured CSPs

The CSP Rank Framework provides optimal cloud service provider selection from the more numbers of CSPs based on security risk values estimated in the last step which provides a list ranked of the more secured CSPs for each customer want to see the ranked results.

5. IMPLEMNTATION AND EXPERIMENTATION OF THE CSP RANK FRAMEWORK

To demonstrate the feasibility and the efficiency of the cybersecurity model, it’s proposed an illustration of the CSP Rank Framework in a practical application with four cloud users CU 1, CU 2, CU 3 and CU 4 under some threats related to the CIANA objectives requesting services from five cloud providers A, B, C, D and E.

Table 1: Security needs of the four cloud users

	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity
CU 1	1	1	0	1	0
CU 2	0	1	1	1	1
CU 3	1	0	1	0	0
CU 4	1	0	0	1	1

Table 2: Calculation of the harm values on each cloud user

	CU 1	CU 2	CU 3	CU 4
Data Breaches	1	0	1	1
Data Loss	1	2	1	1
Account HIjacking	3	4	2	3
Insecure Interfaces	2	2	1	2
Denial of Service	0	1	1	0

Table 3: Coverage of the cloud providers for the 5 cloud threats

	CSP A	CSP B	CSP C	CSP D	CSP E
Data Breaches	3	5	4	1	2
Data Loss	5	3	4	4	2
Account Hijacking	1	4	3	2	5
Insecure Interfaces	2	5	5	1	3
Denial of Service	3	1	4	1	4

Table 4: Maximum risk values of the CUs for each provider

	CSP A	CSP B	CSP C	CSP D	CSP E
CU 1	7	4	5	6	4
CU 2	8	5	6	5	7
CU 3	6	5	4	5	4
CU 4	7	4	5	6	4

The comparison of the risks in cloud customers for the five cloud providers (see Figure 3) shows the difference in level of risk value between the five providers. Thus, the user can request services by starting with the providers having the minimum security risks [17].

6. CONCLUSION

Cloud computing is becoming a key factor in computer science and an important technology for many organizations to deliver different types of services. So, the multiple cloud service providers make a dilemma for a cloud user to choose each provider which is more secured and has the minimum security risk. Hence, in this paper, we propose an effective and efficient cybersecurity model based on CSP Rank Framework that identifies threats and vulnerabilities, and measures the security risks of the existing cloud providers. This model represents a raking system helping consumers to find out the best providers in terms of security and trust, and also satisfy their requirements. As a future work, we will improve this approach by integrating an autonomous and flexible agents using a multi-agent system (MASs) that are capable of intelligent behavior and suitable tools for helping the model to automate the collection of business needs in terms of security and reliability, the computation and the raking function of the security risks for the group of cloud providers which make decision of the more secured providers.

7. REFERENCES

[1] Caron, E., Duang Le, A., Lefray, A. and Toinard, K. 2013. Definition of security metrics for the cloud computing and security-aware virtual machine placement algorithms, International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2013 IEEE.

[2] K. Amrutha, B. Madhu, "An efficient approach to find best cloud provider using broker", International Journal of Advanced Research in Computer Science and Software Engineering, 2014.

[3] Linden, G., Smith, B. and York, J. 2003. Amazon.com Recommendations: Item-to-Item Collaborative Filtering, IEEE Internet Computing, vol.7, no.1, pp.76-80,Jan./Feb.2003.

[4] Zibin, Z., Yilei, Z. and Lyu, M. R. 2010. Cloud Rank: A QoS-Driven component ranking framework for cloud computing. In Reliable Distributed Systems, 29th IEEE Symposium on 2010, pp.184-193.

[5] Zheng, Z., Ma, H., Lyu M.R. and King I. 2011. QoS-Aware web service recommendation by collaborative filtering. IEEE Trans. Service Computing, vol.4, no.2, pp.140-152, Apr.-June 2011.

[6] P. Dhillon, V. Arora, "A compositional approach of reliable and efficient cloud service selection", International Journal of Advanced Research in Computer Science and Software Engineering, 2012.

[7] Zheng, Z., Wu, X., Zhang, Y., Lyu, M.R., Wang, J. 2013. QoS Ranking prediction for cloud services, Parallel and Distributed Systems, IEEE Transactions on, vol.24, no.6, pp.1213-1222, June 2013.

[8] D. Kapgate, "Weighted moving average forecast model based prediction for service broker algorithm for cloud computing", International Journal of Computer Science and Mobile Computing, 2014.

[9] M. Subha, M.U. Banu, "A survey on QoS ranking in cloud computing", International Journal of Emerging Technology and Advanced Engineering, 2014.

[10] R. Yuvarani, M. Sivalakshmi, "Achieve ranking accuracy using cloud rank framework for cloud services", International Journal of Innovative Research in Computer and Communication Engineering, 2014.

[11] P. Bathla, S. Vashit, "A sophisticated study of QoS ranking frameworks in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, 2014.

[12] Whaiduzzaman, M. and Gani, A. 2013. Measuring security for cloud service provider: A third party approach, International Conference on Electrical Information and Communication Technology (EICT), 2013 IEEE.

[13] Salam, A., 2012. What is the key criterion for selecting a cloud service provider?, CloudTweak.

[14] Pfleeger, C.P. and Pfleeger, S.L. 2003. Security in Computing, 3rd edition, Prentice Hall.

[15] Cloud Security Alliance. Cloud Control Matrix / Security, Trust & Assurance Registry / Consensus Assessments Initiative Questionnaire. Technical report.

[16] Elio, G., Dahman, K., Gateau, B. and Godart, C. 2014. A broker framework for secure and cost-effective business process deployment on multiple clouds, CAiSE 2014 Forum/Doctoral Consortium, Thessaloniki, Greece. June 2014.

[17] Lenkala, S. R., Shetty, S. and Xiong, K.2013. Security risk assessment of cloud carrier, International Symposium on Cluster, Cloud, and Grid (CCGrid), pp.442-449, 2013 IEEE/ACM.