A Novel Framework for Ranking Cloud Service Providers Using Security Risk Approach

Jamal TALBI[1], Abdelkrim HAQIQ[1,2]

[1]Computer, Networks, Mobility and Modeling laboratory, Department of Mathematics and Computer, FST, Hassan 1st University, Settat, Morocco
Emails: {talbi85@gmail.com, ahaqiq@gmail.com}

[2]e-NGN Research group, Africa and Middle East

Abstract—**Cloud computing is becoming a key factor in computer science. It represents a new paradigm of utility computing and enormously growing phenomenon in the present IT industry and economy hype. The cloud users (CUs) increase and require secure, reliable and trustworthy cloud service providers (CSPs) from the market. It's a challenge for a new customer to choose the highly secure provider. In this paper, we propose a cloud broker that analyze and rank the cloud service providers based on measuring the risks of confidentiality, integrity and availability. This model uses a CSP Rank Framework for the group of cloud providers by assessing security metrics which make decision of the more secure provider among all providers and justify the business needs in terms of security and reliability.**

Keywords—**Cloud broker, Security Risk, Confidentiality, Integrity, Availability.**

I. 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, 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 and availability 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 [3].

In this work, our aim is to help the new customer to find the most reliable and secured CP in terms of security and trust through a cloud broker that can define, analyze, measure and rank the cloud service providers based on a risk analysis approach 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 proposed model. Section IV describes the CSP Rank Framework. Section V presents an implementation of the model. Section VI gives a conclusion.

II. 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. Our motivation in this paper is to promote a novel approach for ranking 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 [2] 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 [3], 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 [4] 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 [5] 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 [6] 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 [7] 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 [8] had done a survey on quality of service ranking cloud computing. Here the author considered few quality of service parameters and ranked providers based on that.

Cloud Rank [9] 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 [10] 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.

III. THE CONCEPTUAL MODEL OF THE CSP RANK FRAMEWORK

We propose a broker 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 our cloud broker has an important role to find out the secure cloud service providers existing in the database of our cloud broker. The proposed model is described in the following, in terms of its architecture.

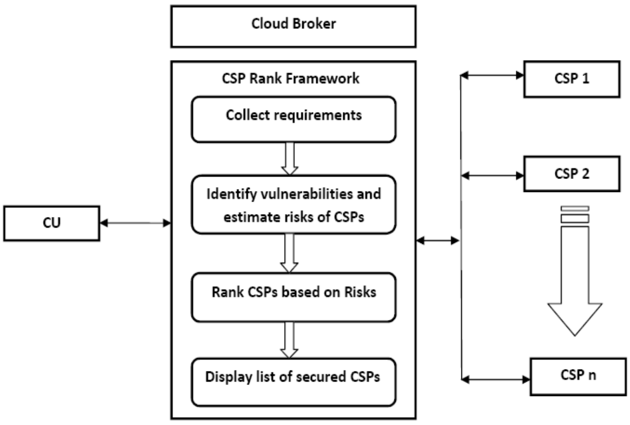


Fig. 1. The structure of the proposed CSP Rank Framework Model

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.

A. Requirements requested

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

B. Vulnerability identification and risks 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.

C. Ranking secured cloud systems

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, we proposed an architecture based on the 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.

IV. DESCRIPTION OF THE CSP RANK FRAMEWORK

Probably all cloud service providers have a Service Level Agreements (SLA), 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 scans and security risk assessment. The obtained results were fed into the security ranking system that offer a list ranked of the secure providers.

Fig. 2 shows our approach for model construction of the cloud broker for ranking secured CSPs taking into account some conditions that should be considered [11]:

- 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.
- 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.
- We consider that a CSP provide 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 cloud broker to see the ranked results.

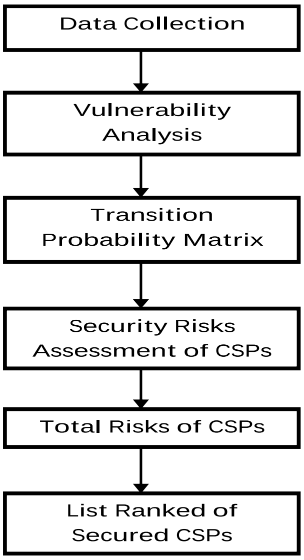

Data Collection
Vulnerability Analysis
Transition Probability Matrix
Security Risks Assessment of CSPs
Total Risks of CSPs
List Ranked of Secured CSPs

Fig. 2. Conceptual model of CSP Rank Framework

A. Vulnerability analysis in CSPs

Vulnerability is a software defect or weakness in the security system which might be exploited by a malicious user causing loss or harm [12]. The identification of these vulnerabilities has been used by several approaches and researchers to estimate risks of the systems.

The Common Vulnerability Scoring System (CVSS) [13] [14] framework allows to assess the severity level of IT vulnerabilities. It associates a severity score (CVSS score) to each IT vulnerabilities, which ranges from 0.0 to 10.0. CVSS [15] is composed of three major metric groups: Base, Temporal and Environmental.

The Base metric represents the intrinsic characteristics of vulnerability, and is the only mandatory metric. The optional Environmental and Temporal metrics are used to augment the Base metrics, and depend on the target system and changing circumstances. The Base metrics include two sub-scores termed exploitability and impact. In the last sub-group, we find three metrics, representing the impact of the attack on the three classical security properties: Confidentiality Impact, Integrity Impact and Availability Impact which we are interested in the next sub-section.

Risk is the potential that something will go wrong [16]. In other words, risk is the possibility of the occurrence of a harmful event. Risk can be formally defined [17] in (1) as:

Risk= Likelihood of an adverse event × Impact of the adverse event (1)

The likelihood of the exploitation of vulnerability depends not only on the nature of the vulnerability but also how easy it is to access the vulnerability. Researchers have developed a stochastic model describing the life cycle of a single vulnerability and containing state transitions [15] as shown is Fig. 3.

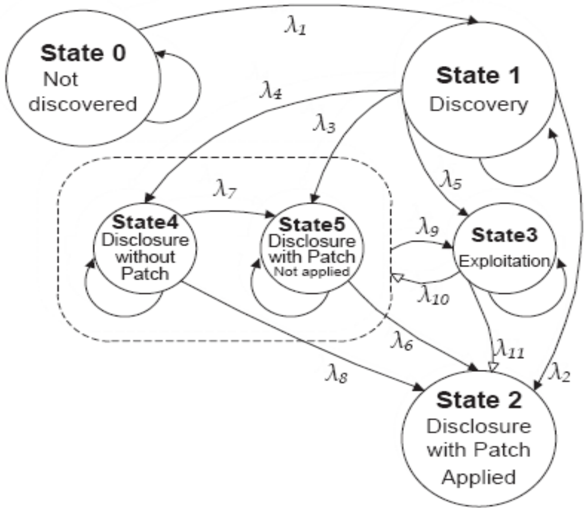


Fig. 3. Stochastic model representing the life cycle of a single vulnerability

The vulnerability life cycle begins with State 0 in which the vulnerability is not yet discovered. State 1 represents the next state when the vulnerability is discovered but it is yet to be disclosed. When the vulnerability is disclosed with the release and application of the patch, it is said to be in State 2. State 4 represents scenario wherein the vulnerability is disclosed without a patch. At State 5, the vulnerability is disclosed with the patch, but the patch is not applied. In State 3, the vulnerability is being exploited. Thus, each vulnerability found after the penetration test by using a scan process [15] on all providers, follows this model that contains 11 possible transitions between the states.

B. Measuring security risk assessment

The security risk can be measured using the risk definition in (1), the model in Fig. 3 and based on the CVSS exploit and impact scores taking into account that the vulnerability must be exploited. Hence, the cumulative risk [18] of a vulnerability being exploited is the likelihood of vulnerability being in State 3.

We consider that Lh_3 as the likelihood of the vulnerability to be in State 3. In this context, we based on Markov chain to compute the Lh_3 for the vulnerability.

The process starts at State 0 for each vulnerability, thereby the vector giving the initial probabilities is V1= [1 0 0 0 0 0]. We define also for a single vulnerability, the state transition matrix M as shown below:

$$\begin{bmatrix} (1-\lambda_1) & \lambda_1 & 0 & 0 & 0 & 0 \\ 0 & (1-\lambda_2-\lambda_3-\lambda_4-\lambda_5) & \lambda_2 & \lambda_5 & \lambda_4 & \lambda_3 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_{11} & (1-\lambda_{10}-\lambda_{11}) & 0 & \lambda_{10} \\ 0 & 0 & \lambda_8 & 0 & (1-\lambda_7-\lambda_8) & \lambda_7 \\ 0 & 0 & \lambda_6 & \lambda_9 & 0 & (1-\lambda_6-\lambda_9) \end{bmatrix}$$

Using the initial probabilities V1 and the state transition matrix M, we obtained the state probabilities V3 after two steps as calculated in (2).

$$V3 = V1 \times M^2 \qquad (2)$$

Thus, Lh_3 is the third element of the matrix V3 and represents the cumulative risk of a vulnerability being exploited. According to (1), we can assess the risk for a possible vulnerability i as:

$$Risk_i = Lh\_3 \times Impact\ of\ exploitation_i \qquad (3)$$

Next we compute Confidentiality risk, Integrity risk and Availability risk. According to the National Vulnerability Database (NVD) database, we used Confidentiality Impact, Integrity Impact and Availability Impact values of the vulnerability as the impact of exploitation for the three types of risk. Based on (3), the risk expressions for a single vulnerability are given in (4).

$$CRVu_i = Lh\_3 \times ConfidentialityImpact_i$$

$$IRVu_i = Lh\_3 \times IntegrityImpact_i$$

$$ARVu_i = Lh\_3 \times AvailabilityImpact_i \qquad (4)$$

The CRVu represents the Confidentiality risk of the vulnerability, IRVu is the Integrity risk of the Vulnerability and ARVu refers to the Availability risk of the vulnerability. Finally, the broker calculates the total risk for each cloud service provider by summing the risks of the individual vulnerabilities detected in this provider. Thereby, the risks related to a cloud service provider j from n providers with m vulnerabilities are expressed in (5).

$$CR\_CSP_j = \sum_{i=1}^{m} CRVu_i$$

$$IR\_CSP_j = \sum_{i=1}^{m} IRVu_i$$

$$AR\_CSP_j = \sum_{i=1}^{m} ARVu_i \qquad (5)$$

Where *CR_CSP*$_j$ is the Confidentiality risk of a selected provider j, *IR_CSP*$_j$ is the Integrity risk of a selected provider j and *AR_CSP*$_j$ is the Availability risk of a selected provider j.

C. Final ranking of CSPs

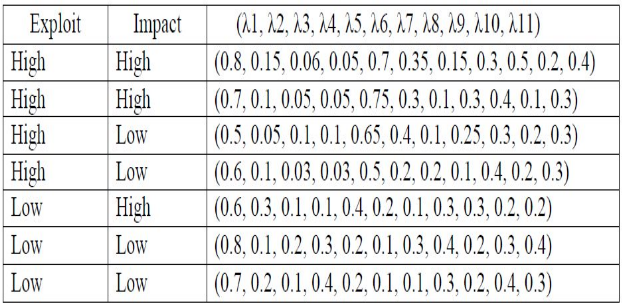
Based on the calculation of the total risks CR_CSP, IR_CSP and AR_CSP of each cloud service provider from all providers, our framework provides a list ranked of the secure CSPs starting with the providers having the minimum security risks in terms of confidentiality, integrity and availability.

V. IMPLEMENTATION OF THE CSP RANK FRAMEWORK

We illustrate the use of our CSP Rank Framework ins a practical application; we consider three cloud providers X, Y and Z under a number of vulnerabilities.

After the data collection step, a vulnerability analysis quantified the vulnerabilities of our clouds by using the CVSS framework and the NVD website as shown in TABLE I. These vulnerabilities are categorized into in four groups: High exploit and High impact, High exploit and Low impact, Low exploit and High impact, Low exploit and Low impact based on CVSS exploit score and CVSS impact score that are qualified as Low if their score is less than or equal to 5.0 and High if this score is greater than 5.0.

TABLE I. CLASSIFICATION OF VULNERABILITIES



Exploit	Impact	(λ1, λ2, λ3, λ4, λ5, λ6, λ7, λ8, λ9, λ10, λ11)
High	High	(0.8, 0.15, 0.06, 0.05, 0.7, 0.35, 0.15, 0.3, 0.5, 0.2, 0.4)
High	High	(0.7, 0.1, 0.05, 0.05, 0.75, 0.3, 0.1, 0.3, 0.4, 0.1, 0.3)
High	Low	(0.5, 0.05, 0.1, 0.1, 0.65, 0.4, 0.1, 0.25, 0.3, 0.2, 0.3)
High	Low	(0.6, 0.1, 0.03, 0.03, 0.5, 0.2, 0.2, 0.1, 0.4, 0.2, 0.3)
Low	High	(0.6, 0.3, 0.1, 0.1, 0.4, 0.2, 0.1, 0.3, 0.3, 0.2, 0.2)
Low	Low	(0.8, 0.1, 0.2, 0.3, 0.2, 0.1, 0.3, 0.4, 0.2, 0.3, 0.4)
Low	Low	(0.7, 0.2, 0.1, 0.4, 0.2, 0.1, 0.1, 0.3, 0.2, 0.4, 0.3)

Hence, the obtained risks values as shown in TABLE II can be grouped into three classes: High Risk (≥ 0.5), Medium Risk (≥ 0.3 and < 0.5) and Low Risk (< 0.3).

TABLE II. THE LH_3 VALUES

Exploit	Impact	Lh_3
High	High	0.560
High	High	0.525
High	Low	0.325
High	Low	0.300
Low	High	0.240
Low	Low	0.160
Low	Low	0.140

Fig.4 illustrates the comparison of the Availability risk for the three clouds. We conclude that the high risk and medium risk groups are dominated by the clouds X and Y whereas the low risk group is dominated by the cloud Z.

Fig. 5 and Fig. 6 show the Confidentiality risk and Integrity risk comparison respectively between the providers X, Y and Z.

Thus, we see that the providers X and Y dominate the High risk and Medium risk categories where the cloud Z dominates the Low risk category.

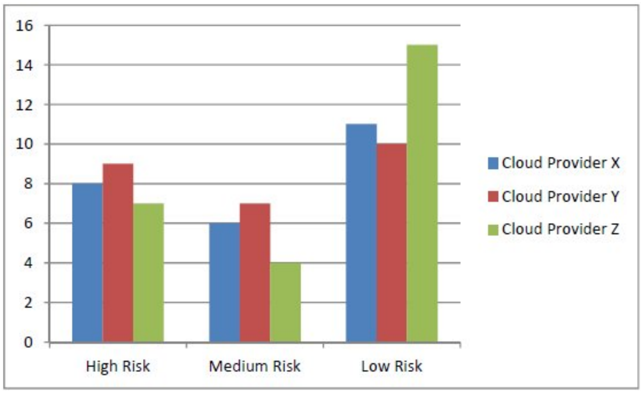


Fig. 4. Comparison of Availability Risk between the Clouds X, Y and Z

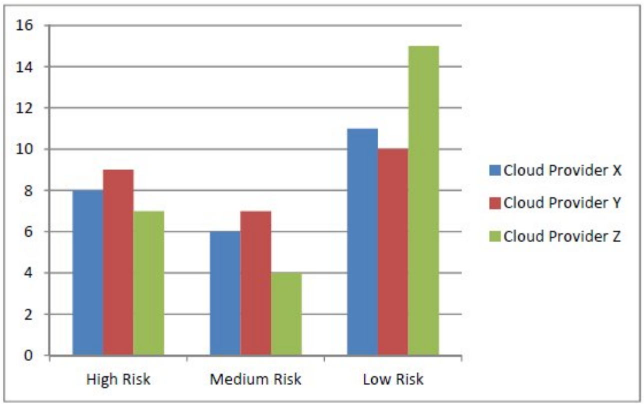


Fig. 5. Comparison of Confidentiality Risk between the Clouds X, Y and Z

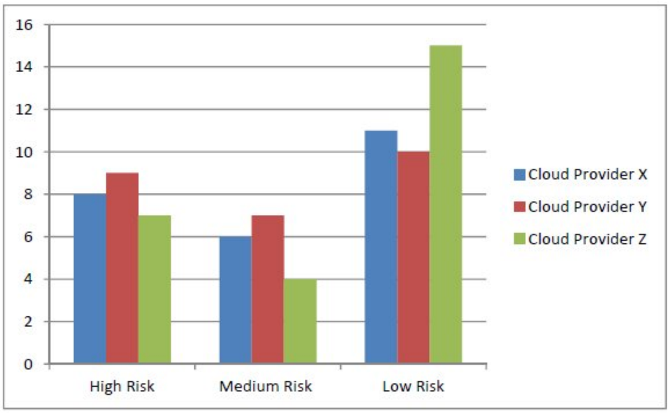


Fig. 6. Comparison of Integrity Risk between the Clouds X, Y and Z

VI. CONCLUSION

Cloud Computing became 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 cloud broker based on CSP Rank Framework that identifies vulnerabilities and measures the security risks. This model represents a raking system helping users to find out the best providers in terms of security and trust, and also satisfy their requirements.

REFERENCES

[1] E. Caron, A. Duang Le, A. Lefray, and C. Toinard, "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] G. Linden, B. Smith and J. York, "Amazon.com Recommendations: Item-to-Item Collaborative Filtering", IEEE Internet Computing, vol. 7, no. 1, pp. 76-80, Jan. /Feb. 2003.

[3] Z. Zibin, Z. Yilei, and M. R. Lyu, "Cloud Rank: A QoS-Driven Component Ranking Framework for Cloud Computing" in Reliable Distributed Systems, 29th IEEE Symposium on 2010, pp. 184-193.

[4] Z. Zheng, H. Ma, M. R. Lyu and I. King, "QoS- Aware Web Service Recommendation by Collaborative Filtering", IEEE Trans. Service Computing, vol. 4, no. 2, pp. 140-152, Apr.-June 2011

[5] P. Dhillon, V. Arora, "A Compositional Approach of Reliable and Efficient Cloud Service Selection", Volume 2, Issue 8, August 2012 ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering.

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

[7] D. Kapgate, "Weighted Moving Average Forecast Model based Prediction for Service Broker Algorithm for Cloud Computing", International Journal of Computer Science and Mobile Computing, vol. 3, Issue. 2, February 2014.

[8] M. Subha, M. U. Banu, "A Survey on QoS Ranking in Cloud Computing", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 2, February 2014.

[9] R. Yuvarani, M. Sivalakshmi, "Achieve Ranking Accuracy Using Cloud Rank Framework for Cloud Services", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Special Issue 1, March 2014.

[10] 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 4(7), pp. 943-946, July 2014.

[11] M. Whaiduzzaman, A. Gani, "Measuring Security for Cloud Service Provider: A Third Party Approach", International Conference on Electrical Information and Communication Technology (EICT), pp. 1-6, 2013 IEEE.

[12] C. P. Pfleeger, S. L. Pfleeger, "Security in Computing, 3rd edition", Prentice Hall PTR, 2003.

[13] P. Mell, , K. Scarfne, and S. Romanosky, "A Complete Guide to the Common Vulnerability Scoring System (CVSS) Version 2.0", Forum of Incident Response and Security Teams (http://www.first.org/cvss/cvss-guide.html), June 2007.

[14] L. Gallon, J-J. Bascou, "Using CVSS in attack graphs", Sixth International Conference on Availability, Reliability and Security, 2011 IEEE.

[15] H. Joh, Y. K. Malaiya, "Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics", International Conference n Security and Management (SAM'11), Las Vegas, 2011.

[16] B. S. Blanchard, W. J. Fabrycky, "Systems Engineering and Analysis", Pearson Prentice Hall, 2006.

[17] G. Stoneburner, A. Gorguen and A. Fertinga, "Risk Management Guide for Information Technology Systems", in National Institute of Standards and Technology Special Publication, 2002.