Journal of Physics: Conference Series

A Comprehensive Review of Existing Risk Assessment Models in Cloud Computing

To cite this article: Ahmad Amini and Norziana Jamil 2018 *J. Phys.: Conf. Ser.* **1018** 012004

IOP Conf. Series: Journal of Physics: Conf. Series **1018** (2018) 012004 doi:10.1088/1742-6596/1018/1/012004

A Comprehensive Review of Existing Risk Assessment Models in Cloud Computing

Ahmad Amini, Norziana Jamil

Institute of Informatics and Computing in Energy (IICE), Universiti Tenaga Nasional,
Jalan IKRAM-UNITEN,Selangor, Malaysia.
Email: Ahmad.Amini2015@gmail.com, Norziana@uniten.edu.my

Abstract. Cloud computing is a popular paradigm in information technology and computing as it offers numerous advantages in terms of economical saving and minimal management effort. Although elasticity and flexibility brings tremendous benefits, it still raises many information security issues due to its unique characteristic that allows ubiquitous computing. Therefore, the vulnerabilities and threats in cloud computing have to be identified and proper risk assessment mechanism has to be in place for better cloud computing management. Various quantitative and qualitative risk assessment models have been proposed but up to our knowledge, none of them is suitable for cloud computing environment. This paper, we compare and analyse the strengths and weaknesses of existing risk assessment models. We then propose a new risk assessment model that sufficiently address all the characteristics of cloud computing, which was not appeared in the existing models.

1. Introduction

During these few years the use of cloud computing by organizations and individuals have increased as they gain access to a shared resources. Cloud computing enables the adoption of on-demand services with virtualized resources through minimal management effort and service provider's interaction [1] . The flexibility and elasticity of this new paradigm can be seen when different cloud services can be integrated using computing resources that benefits users especially when they face restricted economy resources. On the other hand, cloud computing by outsourcing resources that beyond organization boundaries, enforces users to host strategic assets in an inaccessible area. This becomes the main source of risk, which needs to be mitigated in order to guarantee the service's assurance [2]. The lack of control and trust, and the concern of data confidentiality and data integrity, has forced organizations to perform risk assessment to determine their privacy and security. This is done by assessing threats and analysing vulnerabilities. Risk assessment is an integral part of risk management and it is aimed to assess the threat's impacts [3]. The circumstance of assessing risk depends on different factors which are cloud's services, cloud's models, and the required information security (accessibility, availability, integrity, confidentiality).

These challenges lead many researches to develop quantitative or qualitative based assessment models to produce evaluated results to be used by organization as a guide to secure and protect their outsourced assets. However, cloud computing still lacks of standardized information security framework, which applies to risk assessment as well [1]. This paper focuses on a specific aspect of risk assessment such as threat, vulnerability, assets identification and cloud computing characteristics such as rapid elasticity, on-demand self-services, resource pooling, broad network access, and measured service. The result of this research leads to the development of a quantitative risk assessment model to aid organizations in establishing an accurate security risk plan to protect critical assets and gather requirements before applying risk assessment. This paper is organized as follows: Section 2 overview risk assessment in general to give an idea the fundamental steps involved in risk assessment. The understanding of risk assessment framework is important so that it helps to minimize the risk of threats. We detailed out the methodology that we used to conduct this study in Section 3 and our proposal of risk assessment framework is given in Section 4.

2. Risk Assessment

In terms of information security, due diligence should be undertaken to ensure risks are managed properly that includes a process of identifying and assessing security risks [4]. The whole aim is to protect organization's assets. This process is known as security risks management that involves identifying critical assets and threats, and assessing vulnerability and security risk [5] . Risk management framework in cloud computing consists of five stages: user requirement self-assessment, cloud service provider desktop assessment, risk assessment, third party agencies review, and continuous monitoring [6]. This study is only focusing on the third stage of risk management framework, which is risk assessment. This stage is considered to be the most crucial stage in risk management. We reviewed existing models of risk assessment to determine potential threats and risks that are associated with cloud computing. On the other word, on-demand nature of cloud computing is the source of critical threat's impacts such as data lose or leakage, account or service hijacking, denial of service, and data breaches [7]. Risk assessment aims to analyse potential risk of information systems and supply effective strategies for risk reduction through recognizing assets, threats and vulnerabilities [8].

Unfortunately, most proposed risk security assessment models do not guarantee obtaining risks in novel and intangible environments. Cloud computing characteristics are the same as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service which make it attractive and also tend to make it hard to assess its security risks [9] . Accordingly, through cloud computing evaluation, new risks are different from one organization to another. For this reason, risk assessment strategies have been developed and integrated into cloud organization based on business aspects. In this manner, the level of risk in many cases, vary significantly with the type of cloud environment being considered [10]. Nowadays, several numbers of risk assessment, framework, and methodology are available to eliminate the possible risks and potential threats that are associated with an IT systems [11]. The risk identification is the first step of risk assessment process. In cloud computing the main source of risks are malicious threats to exploit vulnerabilities. These threats are divided into general threats that are applicable to any type of information system and unique threats that can affect cloud's users and providers. These threats are associated with virtualization technology, data protection, controlling and allocating resources. The next step is analysing risk to determine the impact and likelihood of each risk. Measuring and assigning value to each risk is the last step of risk assessment approach that is done through quantitative, qualitative or integration of both methods. However, the list of risks and their value can be different base on services, models, or other characteristics of cloud computing.

3. Research Methodology

The methodology of this research is divided into four phases namely Phase 1: review cloud computing characteristics and risks, Phase 2: review existing risk assessment models in cloud computing, Phase 3: compare advantage and disadvantages of existing risk assessment models, and Phase 4: define risk assessment approaches. In Phase 1, we review cloud computing characteristics and different risks that organizations encounter when adopting cloud computing. Different risk assessment models are then reviewed in Phase 2. All models were chosen based on their possibility to be adopted into cloud computing. The details of every phase is given below.

3.1. Phase 1: Define Cloud Computing (CC) characteristics

For assessing the security risks that could affect cloud computing environment, we have a closer look at cloud computing characteristics which affect the risk assessment process.

- ***On-demand services****:* A user can request and manage one or more services whenever he/she needs and pay as “pay-and-go” without any human interaction with a Cloud Service Provider (CSP) [12].
- ***Rapid elasticity****:* Resources can elastically and rapidly provisioned as customer’s demands and they can have unlimited resources to be purchased based on their requests [13].
- ***Broad access network:*** The availability of resources and customer’s data that are located in different virtual machines creates a dynamic collection of resources that can be harmed by unauthorized users.
- ***Resource pooling:*** Computing resources are combined to serve multi customers by different physical and virtual resources which are dynamically assigned and reassigned based on demands [14] .
- ***Metered services:*** Measuring and reporting the usage of system dynamically, is a major abstraction in cloud computing in pay-as-you-use manner.

The above five properties of cloud computing, highlight the dynamic nature of cloud computing that requires a dynamic and cloud-oriented risk assessment approach to identify the risks of cloud adopted assets.

3.2. Phase 2: Reviewing existing Risk Assessment Models

Assessing risks in cloud computing as a complex and dynamic environment has additional challenges. The lack of undefined clear boundaries between cloud services, enforce businesses to develop dynamic risk assessment instead of statistic approaches in cloud computing. Consequently, different models have been developed to modify risk assessment models and prevent users and providers from hazardous risks. The existing Risk Assessment models reviewed are briefed in the following sections.

3.2.1. OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is the methodology to identify and evaluate information security risks by developing qualitative risk evaluation criteria and identifying assets, vulnerabilities and risks. This approach consists of eight steps that are organized into four groups (Figure 1). The primary benefit of OCTAVE is connecting organizational objectives to information risk assessment and vulnerability management. For this reason, OCTAVE is developed as flexible and self-modified approach to be customized for different organizations by their small teams of IT and the business. However, this model can be integrated by other models and used as a hybrid model that it seems as a big opportunity for cloud computing. But unfortunately, documenting all requirements and characteristics of this integrated approach, makes this model more complex for distributed and massive computing environments. The method of threat classification and identification is another disadvantage of OCTAVE model.

Also, the threat tree as a guide for identifying threats in OCTAVE is not suitable for massive computing environment because the users are faced with a huge and unclear tree by many paths where each path presents a real-word scenario. This threat identification approach is a single-dimension and furthermore static in that it cannot support different criteria (agent, source, impact and motivation) of threat classification and identification in cloud computing. The elimination of vulnerability identification tool is another issue in OCTAVE Allegro. It seems this function of OCTAVE is more suitable for static environment that company can integrate their own vulnerability classification tool. Classification of vulnerabilities in cloud computing has to follow principles such as public acceptance, comprehensibility, competence, determinism, mutual exclusion, and repeatability [15] by respecting Web Service (WS), Service-Oriented-Architecture (SOA), and virtualization as the main core of cloud computing. By considering all the above mentioned criteria and functionalities of vulnerability assessment, it seems is more appropriate and efficient to integrate vulnerability identification into cloud services.

3.2.2. Semi-quantitative BLO-oriented cloud risk assessment (SEBCRA)

This model as depicted in Figure 2 evaluates the impact of risks on an organization's global Business-Level Objectives (BLO) rather than considering the effect on different single assets of organization [10]. Semi-quantitative or hybrid is the primary method to assess risk in this model, which is less numerical than quantitative methods and risks have been classified based on their probability. The core concept is based on risk level estimation for each BLO that is proportional to the probability of a given risk and its impact on the BLO [16]. The qualitative part is risk level estimation by risk-level matrix that includes probability of risk occurrence (very unlikely, possible, likely, and frequent) and impact of each risk (very high, high, medium, low, and very low).

The outcome of this matrix is a list of prioritized risk that is obtained by multiplying probability with impact of risk to maximize profit and user satisfaction. Known and unknown risk identification is the most critical part of risk assessment method used in this model. It is so because the risk identification is based on service provider and impact of risks that is so narrow. This indicates that additional factors have to be investigated such as motivation and source of risks. On the other hand, multi dimensions model is more efficient for on-demand and massive computing environment to identify and classify risks. Measuring the impact of each risk is related to main information security principles such as integrity, confidentiality and availability. These impact metrics allow provider to calculate accurately the cost of each risk for the system. In this model, it is more important to measure the cost of threat quantitatively by considering security metrics rather than classifying them by qualitative matrix.

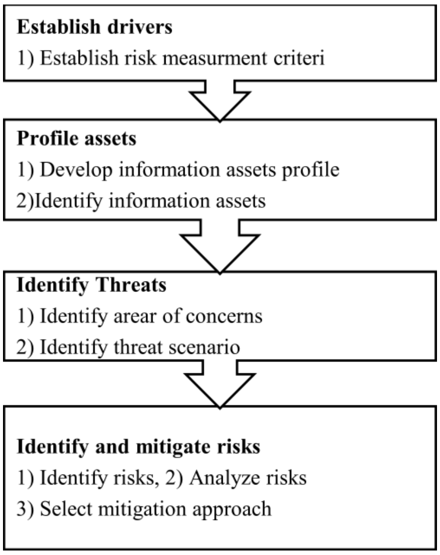
Establish drivers
1) Establish risk measurment criteri
Profile assets
1) Develop information assets profile
2)Identify information assets
Identify Threats
1) Identify arear of concerns
2) Identify threat scenario
Identify and mitigate risks
1) Identify risks, 2) Analyze risks
3) Select mitigation approach

Figure 1: OCTAVE Model

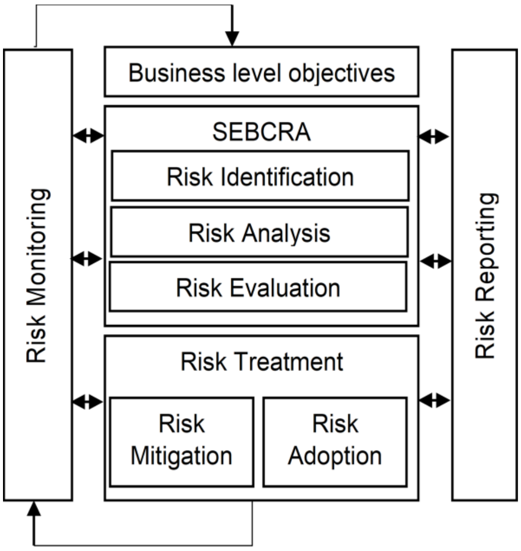

Figure 2: LO driven cloud risk management

3.2.3 A cyber security model

This model proposes security metrics (stakes, dependency and impact matrix, security requirements, component and services, security threats) that are quantified in economic terms to enable service provider and service subscriber to quantify the risks that they incur as a result of prevailing security threats and system vulnerabilities [17]. This quantitative model, summarized all metrics in matrix of mean failure cost to measure threats. On the other hand, the discussed model allows providers and subscribers to make security decision based on quantitative analysis.

3.2.4. Scalable Risk Assessment method using game theory (CCRAM)

Game theory is an interdisciplinary approach to inspect the behaviour between two players or groups and find optimal strategies to increase outcome or decrease damage of risks [18] .The main purpose of CCRAM model is to allow defender to choose a defence strategy against attacker's action. For modelling risk assessment, Confidentiality, Integrity, and Availability (CIA) are considered to calculate the impact of attack on the system. This is assuming virtualization and live migration of resources and assets in cloud computing affect the value of CIA from one system to another. However, in CCRAM model, the quantitative values are used to calculate the risk's effects and determine which one is more important. The three main characteristics of risk assessment model are listed as impact of threat, likelihood, probability and value of assets. The total value of asset and the level of damage by risks are represented in this model but the level of system's vulnerabilities to calculate the probability or likelihood is not mentioned in the above model.

3.3. Phase 3: Comparing the advantages and disadvantages of presented risk assessment approaches

The comparison of different discussed models is summarized in Table 1. The advantages and disadvantages of different risk assessment models are based on risk assessment and cloud computing characteristics. The first step of this comparative study is to specify the main characteristics of all risk assessment methodologies. In the early stage, organizations should clarify which assets are more important and critical for them which could be classified such as private-classified, financial-classified and application assets-classified [19].

The next step is to identify threats and vulnerabilities and to consider how threats can exploit vulnerabilities. For this reason, effective security classification is necessary to identify threats and vulnerabilities into classes based on the intended effect of attacks and develop solutions to prevent system from hazardous threats [20]. In this situation, organization which are interested to adopt cloud computing have to modify and present the combination list of threats and map them to indicate vulnerabilities and clarify the security concerns that are effected by each threat. Finally, the presented list have been used to estimate the security risk based on impact and likelihood.

However, comparison of the risk assessment models presents great opportunities to look at similarities in model's infrastructure and develop a novel risk assessment model. The next step of the comparative study is about sub-characteristics of main risk assessment characteristics. Each sub-feature has been presented as the main objective of a novel risk assessment in cloud computing. Furthermore, we try to carry the comparison among elements and cross-checked and marked against all proposed models in the table 2. Nonetheless, all the compared results are very useful to quantify the security risk assessment for each organization and translate them to a homogenized risk analysis result.

3.4. Phase 4: define the risk assessment approaches

For migrating organizations' information to the cloud the optimal rules have to be investigated to apply some approaches in order to reduce cost and improve security. Most of the risk assessment models in our comparison are not suitable for assessing risk in complex and dynamic environments such as cloud computing. The most important holistic approaches to address the above challenges are discussed below:

- Organization that are interested to adopt cloud computing into their business must rely essentially on automated mechanisms. In fact, based on cloud computing's promises automated control mechanisms are supposed to be more effective. As a result, the risk assessment model has to be an automated system with less training and better risk managing and privacy monitoring.

- The integration of different dynamic computing environments by different properties and characteristics, supporting virtualization and resource pooling are challenges and concerns for assessing risks in traditional assessment methodologies. In this situation, defining boundaries and controlling the access to virtual resources can be defined as risk assessment approaches to aid organization to protect system from cyber threats when adopting it into the cloud computing.

By sharing physical and virtual resources between different consumers in cloud computing, a traditional risk assessments have to be updated to support resource pooling and multi-tenancy. In this shared resources environment, each consumer can carry out malicious activities that may affect other consumers. Therefore, controlling the access to different resources and automated resource allocation have to be considered in order to develop and adopt risk assessment in cloud computing.

Table 1. Comparing risk assessment models based on cloud computing characteristics

RA models	**Risk assessment characteristics**		**Cloud computing charactristics**			
	Threat identification and classification	**Measured services**	**On-demand self-services**	**Broad network access**	**Resource pooling**	**Rapid elastisity**
OCTAVE	Use threat tree as a single dimension	The lack of suitable threat and vulnerability identification	customized model	lack of clearly-defined bounderies	Need more modification for multi-tenancy environment and addressing unknown location	Slightly strong to migrate by another risk assessments
SEBCBRA	use risk level matrix	costing and measuring VMs follows pay-as-you-go model	Use Business-Level Agreement	Mean Time Between Failure (MTBF) and Mean Time to repair (MTTF) to assess the availability of resources	Offer round-robin schaduler to ensure equitable distribution of VMs	Use workload pattern for real access to resources
A cyber security model	Use main failure cost matrix	Calculate the security gain cost	self-managed purpose	access to a computational resources	provide allocation mechanisms	resource migration, communication,and mobility
CCRAM	Formulate CIA value to measure the impact of	The lack of pay-as-you-use	out of self-managed process and need expert	Support live migration	lack of resource housting and multi-tenancy	Identify cloud live migration

Asset's value estimation	**Vulnerability identification and classification**
Identify and develop profile of asset's information	Lack of suitable tool to identify vulnerability
Consider the business and IT-level objective as assets	Lack of vulnerability assessment
Estimate the asset's value	Define virtualization as the source of major security risks
The damage level of assets is formulated in this model based on CIA form	Miss the evaluation of vulnerabilities

- By giving opportunity to users to scale up and down resources elasticity and rapidly, the effective risk assessment model must cover providers, sub-providers, and consumers to optimize the use of available and shared resources. For this reason, risk assessment has to be able to migrate to another risk assessment models and control the live migration of physical and virtual resources dynamically.
- Controlling and optimizing the used resource by consumers, enforce organizations to deploy risk assessment model to control the collected confidential data of users that are potentially vulnerable. In this situation, protecting and monitoring the metering information of each individual user is an important approach for adopting risk assessment into cloud computing.

Table 2. Comparative of sub characteristics among different risk assessment models

Risk assessment		**Risk assessment models**			
Characteristics	**Sub-characteristics**	**OCTAV**	**SEBCBRA**	**A cyber security**	**CCRAM**
1. On-demand self-services	Simple and self-service user portal	✓	✓	×	×
2.Broad network access	Clearly-defind boundry	×	✓	?	?
	Access to resources as virtual	×	✓	✓	✓
	Identity and Access Management	✓	✓	✓	✓
	Federated differend services	✓	?	?	✓
3.Resource pooling	Access of user to different resource	?	?	✓	?
	Automated allocation and re-	✓	?	?	✓
4.Rapid elastisity	Live migration	✓	✓	✓	✓
	Control Physical and virtual resource	×	?	✓	×
	Risk assessment migration	✓	×	×	×
	Resource migration and	×	✓	✓	×
5.Measured services	Used-resource calculation and	×	✓	✓	×
6. Threat identification and classification	Threat identification	✓	✓	✓	✓
	Threat impact measurement	×	✓	✓	✓
7. Vulnerability identification and	Vulnerabilities identification	✓	×	✓	×
8. Asset's value estimation	Assets identification and value	✓	✓	✓	✓

Full fill requirements: ✓, doesn't full fill : ✗ , couldn't find documentation: ?

4. Conclusion

The adoption of cloud computing provides continuous benefits such as access to unlimited virtualized resources, management and maintenance of system professionally, access to on-demand services and billing through as pay-as-you-need. Unfortunately, these advantages do not offer better security in terms of integrity, confidentiality, and availability. For this reason, risk assessment models have been developed to enable service providers and users to quantify risks based on their impact and severity on critical assets. Moreover, developing risk assessment for cloud computing in a complicated environment requires comprehensive quantitative and qualitative metrics. The most of the risk factors and metrics will rely on decision maker's or expert's judgments. In this work, we investigate different risk assessment models by carefully considering cloud computing characteristics and considering the main features of risk assessment model. We do a classification of risk and obtain a generic baseline to develop a new risk assessment model that suits well in cloud computing. We envision to extend this work to refine a quantitative and qualitative risk assessment approach for measuring and ranking risks for cloud computing environment.

Acknowledgement

First I would like to thank to my supervisor Dr. Norziana Jamil for her guidance and her advice. This study is partly funded by TNB Seed Fund 2016 under a project 'R&D of Micro Cryptographic Engine for Protecting Data in SCADA Link'. I would specially thank my family who has supported me through the ups and downs in completing this study. Without helps of the person mentioned above, I couldn't be succeed in this research.

References

[1] Theoharidou, M., N. Tsalis, and D. Gritzalis, *In Cloud We Trust: Risk-Assessment-as-a-Service*, in *Trust Management VII*, C. Fernández-Gago, et al., Editors. 2013, Springer Berlin Heidelberg. p. 100-110.

[2] Rebollo, O., et al., *Empirical evaluation of a cloud computing information security governance framework.* Information and Software Technology, 2015. **58**: p. 44-57.

[3] Peiyu, L.I.U. and L.I.U. Dong, *The New Risk Assessment Model for Information System in Cloud Computing Environment.* Procedia Engineering, 2011. **15**: p. 3200-3204.

[4] Humphreys, E., *Information security management standards: Compliance, governance and risk management.* Information Security Technical Report, 2008. **13**(4): p. 247-255.

[5] Bajpai, S., A. Sachdeva, and J.P. Gupta, *Security risk assessment: Applying the concepts of fuzzy logic.* Journal of Hazardous Materials, 2010. **173**(1–3): p. 258-264.

[6] Khrisna, A. and Harlili. *Risk management framework with COBIT 5 and risk management framework for cloud computing integration*. in *Advanced Informatics: Concept, Theory and* Application (ICAICTA), 2014 International Conference of. 2014.

[7] Amini, A., et al., *A Fuzzy Logic Based Risk Assessment Approach for Evaluating and Prioritizing Risks in Cloud Computing Environment*, in Recent Trends in Information and Communication Technology: Proceedings of the 2nd International Conference of Reliable Information and Communication Technology (IRICT 2017), F. Saeed, et al., Editors. 2018, Springer International Publishing: Cham. p. 650-659.

[8] Guan, J.-z., et al., *Knowledge-based information security risk assessment method.* The Journal of China Universities of Posts and Telecommunications, 2013. 20, Supplement 2: p. 60-63.

[9] Burton S. Kaliski, J. and W. Pauley, *Toward risk assessment as a service in cloud environments*, in *Proceedings of the 2nd USENIX conference on Hot topics in cloud computing*2010, USENIX Association: Boston, MA. p. 13-13.

[10] Fitó, J.O. and J. Guitart, *Business-driven management of infrastructure-level risks in Cloud providers.* Future Generation Computer Systems, 2014. **32**: p. 41-53.

[11] Saleh, M.S. and A. Alfantookh, *A new comprehensive framework for enterprise information security risk management.* Applied Computing and Informatics, 2011. **9**(2): p. 107-118.

[12] Jula, A., E. Sundararajan, and Z. Othman, *Cloud computing service composition: A systematic literature review.* Expert Systems with Applications, 2014. **41**(8): p. 3809-3824.

[13] Ali, M., S.U. Khan, and A.V. Vasilakos, *Security in cloud computing: Opportunities and challenges.* Information Sciences, 2015. **305**: p. 357-383.

[14] Sher DeCusatis, C.J. and A. Carranza, *Chapter 15 - Cloud Computing Data Center Networking*, in *Handbook of Fiber Optic Data Communication (Fourth Edition)*, C. DeCusatis, Editor. 2013, Academic Press: Oxford. p. 365-386.

[15]Rabai, L.B.A., et al., *A cybersecurity model in cloud computing environments.* Journal of King Saud University - Computer and Information Sciences, 2013. **25**(1): p. 63-75.

[16]Djemame, K., et al., *A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems*, in *The Second International Conference on Cloud Computing, GRIDs, and Virtualization*2011, IARIA. p. 119-126.

[17] Rabai, L.B.A., et al., *A cybersecurity model in cloud computing environments.* Journal of King Saud University - Computer and Information Sciences, 2013. **25**(1): p. 63-75.

[18] Furuncu, E. and I. Sogukpinar, *Scalable risk assessment method for cloud computing using game theory (CCRAM).* Computer Standards & Interfaces, 2015. **38**: p. 44-50.

[19] Amini, A., et al., *Threat Modeling Approaches for Securing Cloud Computin*. Vol. 15. 2015. 953-967.

[20] Jouini, M., L.B.A. Rabai, and A.B. Aissa, *Classification of Security Threats in Information Systems.* Procedia Computer Science, 2014. **32**: p. 489-496.