UDC 004.052.2:004.054

Olena Chebanyuk, D,Sc, Anton Stadnychenko, PhD student
(National Aviation University, Ukraine)

Risk assessment models in cloud computing

Paper investigates various risk assessment models applicable to cloud computing and provides a comparative analysis of their strengths and weaknesses. The models analyzed include OCTAVE, CVSS, NIST, FAIR, CRAMM, STRIDE, and DREAD. Based on the analysis, the FAIR model is found to be the most suitable for cloud software, tailored to the characteristics of cloud computing.

Introduction.

In recent years, the adoption of cloud computing has seen exponential growth as businesses and organizations look to leverage the benefits of on-demand resources, scalability, and cost savings. However, as with any technology, there are inherent risks that need to be managed and mitigated. Cloud computing introduces a unique set of challenges in terms of risk assessment and management due to the shared responsibility model between cloud service providers and customers. 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 [1]. Risk assessment models allow to organizations to quantify and prioritize risks based on their impact and severity on critical assets. These models help businesses to make informed decisions about which risks to mitigate and which to accept based on a thorough understanding of the potential consequences. Paper will investigates various risk assessment models that are applicable to cloud computing environments and provides a comprehensive analysis of their strengths and weaknesses. Based on the comparison a risk assessment model tailored to the characteristics of cloud computing is proposed.

Review of risk assessment models

Risk assessment is a critical aspect of ensuring the security and resilience of cloud computing systems. It is essential for organizations to have a comprehensive understanding of the risks associated with cloud computing, and to take appropriate measures to mitigate these risks. Risk assessment models provide a framework for identifying, analysing, and evaluating the risks associated with cloud computing. There are several risk assessment models that have been developed specifically for cloud computing environments. These models vary in their approach and complexity, but they all aim to provide organizations with a structured approach to identifying and mitigating risks.

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation [1] - This model focuses on identifying and prioritizing critical assets and assessing the impact of potential threats on those assets. It emphasizes a collaborative approach involving both technical and non-technical stakeholders.

CVSS: Common Vulnerability Scoring System [3] - This model is designed to provide a standardized method for assessing and rating the severity of vulnerabilities in software or systems. It uses a numerical score based on various factors such as exploitability, impact, and complexity.

NIST: National Institute of Standards and Technology - This model provides a comprehensive framework for managing cybersecurity risks [2]. It includes guidelines and best practices for risk assessment, risk management, and security controls, and is widely used in both public and private sector organizations.

FAIR: Factor Analysis of Information Risk - This model uses a quantitative approach to risk assessment, focusing on factors such as asset value, threat frequency, and loss magnitude to calculate the probable financial impact of a security incident.

CRAMM: Computer Risk Assessment Methodology [1] - This model is a comprehensive risk assessment framework that includes a detailed questionnaire to assess potential risks and vulnerabilities. It also provides guidance on risk management and mitigation strategies.

STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege[4] - This model is a threat modeling approach that focuses on identifying and mitigating potential security threats. It provides a structured method for analysing threats and developing countermeasures.

DREAD: Damage, Reproducibility, Exploitability, Affected Users, and Discoverability[4] - This model is another threat modeling approach that focuses on identifying and prioritizing potential threats based on their severity and impact. It uses a numerical scoring system to rate each threat based on various factors.

Comparative analysis of risk assessment models.

To select the most appropriate model, it is necessary to conduct a comparative analysis. We need criteria to consider the fundamental aspects of cloud computing, such as resource pooling, rapid elasticity, and measured services. Additionally, the criteria should focus on critical aspects of risk assessment, such as threat identification and classification, vulnerability identification, and asset value estimation. These criteria are:

Cloud suitability - because not all risk assessment models are well-suited for the unique characteristics and requirements of cloud environments, such as on-demand self-services and rapid elasticity.

Ease of use - because risk assessment models that are too complex or difficult to use may not be adopted by organizations or may be used incorrectly, leading to ineffective risk management.

Risk factor coverage - because a good risk assessment model should cover a wide range of potential risks and vulnerabilities that are relevant to cloud environments, such as data breaches, insider threats, and system downtime.

Adaptability - because cloud environments are dynamic and constantly changing, and risk assessment models need to be able to adapt to new threats and vulnerabilities as they emerge.

Scalability - because cloud environments can scale rapidly and risk assessment models need to be able to handle large volumes of data and resources in a scalable and efficient manner.

Having criteria and models, we built a table for comparing models according to the given criteria. Characteristics are classified into three levels: low, medium, and high.

Table 1

Risk assessment models comparison

Risk Assessment Model	Cloud Suitability	Ease of Use	Risk Factor Coverage	Adaptability	Scalability
OCTAVE	Medium	Low	High	Low	Medium
CVSS	Low	High	Medium	Medium	High
NIST	Medium	Medium	Medium	High	High
FAIR	High	Medium	High	High	Low
CRAMM	Low	Low	Medium	Low	Medium
STRIDE	Medium	High	Low	Medium	High
DREAD	Low	High	Low	Medium	High

Proposed model for cloud software risk assessment

Based on the comparative analysis of the seven risk assessment models for cloud computing, the FAIR model seems to be the most suitable for cloud software. The FAIR model excels in its ability to provide a quantitative analysis of risk, allowing for a more precise and objective understanding of the risk involved. It also includes a comprehensive taxonomy of threat actors and threat events, enabling organizations to identify potential threats and better allocate resources towards risk management. Furthermore, FAIR includes a well-defined process for risk assessment, which helps organizations to ensure consistency and accuracy in their risk management efforts. It also has the ability to support a wide range of risk scenarios, making it a flexible model that can be applied to different types of cloud software. The FAIR model's strengths in quantitative analysis, comprehensive threat taxonomy, and well-defined risk assessment process make it the best choice for risk assessment in cloud software.

Proposed model is based on avoiding drawbacks of FAIR model. We are concentrating on minimization such types a risks as scalability of resources that are used when application grows.

Explanation of the proposed model

During analysis of risk factors for development of software with cloud services are defined. Key idea of the proposed model that different types of risks depend upon different resources (Figure 1). Package diagram with main components of the model is represented on the figure 1. Dependency relationship between two packages shows that risks depends upon resources. In order to manage some risks some resource or collaboration of them is used. Corresponding compositions of required resources and risks are represented as pair of required and provided interfaces.

For example, component “Risks of architectural solutions designing” depend upon people resources. For example, community that recommends architectural templates, or design patterns, used for design architectural solutions in cloud. Also this risk depend upon qualification of software architectures, involved in project designing.

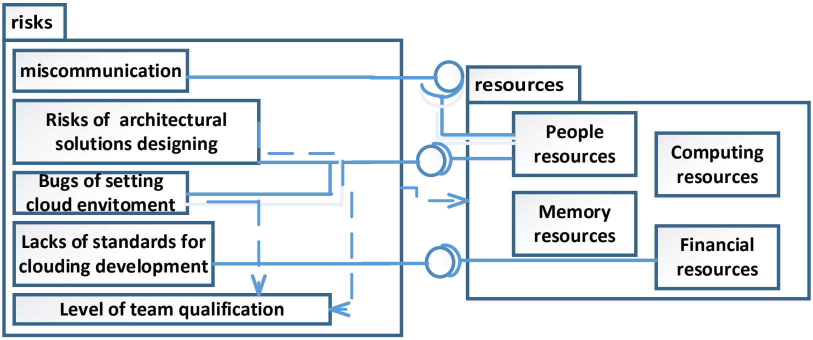
risks
miscommunication
Risks of architectural solutions designing
Bugs of setting cloud envitoment
Lacks of standards for clouding development
Level of team qualification
resources
People resources
Computing resources
Memory resources
Financial resources

Figure 1 Component diagram of model for risk assessment in development using cloud services.

Conclusion

Adopting cloud computing to software development has brought challenges to managing risks, making risk assessment models essential tools for businesses and organizations. Several risk assessment models may used for cloud computing environments, including OCTAVE, CVSS, NIST, FAIR, CRAMM, STRIDE, and DREAD. A comparative analysis of these models shows that the FAIR model is the most suitable for cloud software as it offers a quantitative analysis of risk, allowing for a more precise and objective understanding of the risk involved. With the proposed FAIR model, organizations can make informed decisions about which risks to mitigate and which to accept, contributing to developing best practices for risk assessment in cloud computing.

Overall, this thesis provides insights into the importance of risk assessment in cloud computing and proposes a model that can assist businesses in making informed decisions to maintain the security and integrity of their data and systems.

References

1. Amini, Ahmad, and Norziana Jamil. "A comprehensive review of existing risk assessment models in cloud computing." Journal of Physics: Conference Series. Vol. 1018. No. 1. IOP Publishing, 2018.
2. Force, Joint Task. "Risk management framework for information systems and organizations." NIST Special Publication 800 (2018): 37.
3. Mell, Peter, Karen Scarfone, and Sasha Romanosky. "Common vulnerability scoring system." IEEE Security & Privacy 4.6 (2006): 85-89.
4. Zhang, Lu, et al. "A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces." International Journal of Information Security (2021): 1-17.