Optimized Off-line Risk Assessment Framework for Cloud Service Providers

REU Students: Ashley Painter*, Joshua Haupt˜, Matthew Hall ° **PhD Student**: Amartya Sen*

* Computer Science, MS&T °Computer Science, Humboldt State University ˜Computer Science, Southern Illinois University Edwardsville

Faculty Advisor: Dr. Sanjay Madria*

INTRODUCTION

To determine whether or not an application should be migrated on to a cloud service provider (CSP) there are three things that are needed

- An analysis of an application
- An analysis of the various aspects of services provided by a CSP
- A cost benefit tradeoff analysis to evaluate the efficiency of migration in terms of security and monetary benefits

OBJECTIVES

- To develop security rating framework to rate each entities of an application along the lines of Confidentiality(C), Integrity(I), & Availability(A), along with the introduction of a new attribute, "*criticality*"(Cr).
- To break down an SLA based on certain categories like, security & privacy, availability, and to *grade* them on a point based scale as per the information presented in an SLA.
- To perform *a cost-benefit tradeoff* analysis considering the different available CSPs with regards to the cost and security benefits gained from hosting different entities of an application on them.

BACKGROUND

This work stems from the previous work of offline risk assessment of Cloud Service Provider [1]. The previous work however did not recommend a final migration strategy for an application or a way to evaluate entities in a DFD with their relationships to other entities and the type of information they handle. It also did not recommend a way to rate CSP's by their SLA's.

Application Analysis Framework

•The framework evaluates each entity in a DFD of an application for C,I,A,Cr in two directions data flowing into and out of the entity [3].

•It does this by translating the DFD into a weighted directed graph with several *specialized types of nodes* based off what the entity is doing with the data.

•It evaluates the individual nodes with respect to the type of data they're handling, the type of node, and its relationship with other nodes.

SLA Grading Framework

The proposed methodology relies on a framework consisting of eight categories [2] which are listed below,

•Availability
•Compensation
•Scalability
•Security and Privacy
•Performance
•Understanding of Costs
•Ease of configuration
•Compatibility

Each category is scored on a point based system from *0 to 5* based on how it is presented in the SLA.

Figure. 1: Depicts the different aspects of the Optimized Offline Risk Assessment Framework

Cost benefit tradeoff Analysis Framework

•First Record the cost difference for Total Cost of Ownership (TCO) and Cost of Cloud Storage (CCS) for all components of an application on all the perspective CSPs [4].

•A cost matrix *A* is *m*X*n*
  - *m* is the number of storage option for a component (Cloud A, Cloud B, etc..) and the last row (A_m) has TCO for each component.
  - *n* is the number of different entities in the application.

•A_{ij} *is the price of storing entity* i *on cloud* j

•Difference matrix D comes from $T: A \rightarrow D$ *where* $D_{ij} = A_{im} - A_{ij}$

$$for\ 0 \leq i \leq m; 0 \leq j \leq n$$

•Now consider security coverage differences of each component on a cloud versus stored on private hardware in: *technical impact, required privilege, business impact*.

•With these attributes scored for each weakness on each CSP, a similar matrix to the difference matrix above is computed. The values of the two matrixes are scaled independently by column and added together.

•The max. value in each column determines the destination for an entity to migrate if it's values of cost and security difference were both positive.

FUTURE WORK

•Develop a generalized equation for the Cost benefit tradeoff Analysis so that it can be automated

•Develop additional categories and expand the SLA Grading Framework

•Test the equation for local area for the effect of changing the log base

•Implement the three frameworks and integrate it with current off-line risk assessment tool

REFERENCES

[1] S Madria and A Sen "Offline Risk Assessment of Cloud Service Providers." *Cloud Computing, IEEE* 2.3 (2015): 50-57.
[2] Alhamad, Mohammed, Tharam Dillon, and Elizabeth Chang. "Conceptual SLA framework for cloud computing." *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on*. IEEE, 2010.
[3] D Dhillon"Developer-driven threat modeling: Lessons learned in the trenches." *IEEE Security & Privacy* 4 (2011): 41-47
[4] Ajeh, D Edache, J Ellman, and S Keogh. "A Cost Modelling System for Cloud Computing." *Computational Science and Its Applications (ICCSA), 2014 14th International Conference on*. IEEE, 2014.