An Automated Negotiation Model for SLA Based Decision Support System in Cloud Environment

[1] P.Sujan kumar reddy, [2]Ameneni Thanuja , [3]Mrs.S.krishnaveni
[1]Student ,[2]Student, [3]Assistant Professor
Department of Software Engineering, SRM University, Kattankulathur.

***Abstract* – A cloud customer doesn't directly approach a cloud service provider to receive services. The customer first approaches an intelligent third party for going through negotiation phase. Negotiation is a phase where the cloud customer is binded to a cloud service provided based on the customer requirements .In our project, the negotiation phase is an automated process. Various cloud service providers list their security services (in this project, security services are alone dealt with) to the trusted third party. The third party gives a questionnaire to the authorized customers to capture the customer environment details. Thus, the third party recommends security services to the cloud customer. A matching algorithm is designed to match the security requirements with various cloud service providers' security offerings. Matching is followed by a Decision support model where the best suitable cloud service provider for the customer is chosen. A SLA is generated which binds the cloud customer to the cloud service provider. Monitoring of SLA is also handled by the intelligent third party.**

Index Terms : SLA – (Service Level Agreement) , CSP – (Cloud Service Provider), ITP – (Intelligent Third Party), DSS – (Decision Support System) ,CC – (Cloud Customer), ACSP –(Access Control and Security Properties). (keywords)

I. INTRODUCTION

The project focuses on the negotiation phase between the client and the cloud service provider (CSP). The process of negotiation phase includes-Getting the client security requirements, Listing of several CSP security offerings, Matching the security properties with the available CSP security offers, Finding a suitable CSP based on the matching output and Decision support model, Generating an automated SLA with the chosen CSP .The scope of the project lies within the negotiation phase of security requirements where client finds the best suitable CSP. The guarantee, enforcement and monitoring of the security requirements is outside the scope of this project.

II. RELATED WORK

Although the technology and its application are not new, the rising awareness and implementations of cloud services and its underlying technologies cause the need for security requirements being up to date. Cloud computing security requirements have been addressed in publications earlier, but it is still difficult to estimate what kinds of requirements have been researched most, and which are still under-researched. This paper [1] carries out a systematic literature review by identifying cloud computing security requirements from publications between January 2011 and March 2013. It will categorize these requirements in a framework and assess their frequency of research. The paper will then identify changes in the assessment of requirements and proposed solutions.

Representing the security requirements is a difficult task when it comes to Access Control as they are complex involving lot of access rights. In this paper [2], a language is defined for proper representation of Access Control and security properties known as Requirements Specification Language (RSL).The customers express their AC requirements in RSL using the following request: req (roles, objects, actions, cloud Levels, target Roles, target Actions, contexts, permissions). The customer requires that the user endorsing one of the given 'roles' must be 'allowed' to perform given 'actions' on given 'objects' when a given 'context' is true, at a given service level. The other attributes are used when requesting a management action, for example: users having 'roles' request to 'share' 'objects' with the users having 'targetRoles' with 'targetActions' and 'permissions'. When an attribute is not applicable symbol '-' is used. To express choice between several possible arguments. '\' is used. '*' stands for all possible values.AC rules only describe direct access but SP describe also indirect accesses. Properties are such as: Confidentiality, Integrity of Information, Race conditions, Privilege separation, Domain Integrity.

Before negotiating services, conflicts between customer requirements are detected automatically by the broker and some corrections are attributed and communicated to the customer who validates these corrections or modifies its requirements. After all requirements have been corrected and validated, the third party starts negotiating service. Negotiating service will match the ACSP and CSA requirements with cloud providers security offers and SLA life cycle starts with a suitable CSP.A Multi Criteria Decision making Process is needed to choose best CSP. The decision making process is explained in this process [3] through a Decision support Model called Analytic Hierarchy Process. This paper explains the AHP with an example of selecting Cell Phone Services.

Finding the lowest cost plan is relatively straight forward using a computer-based system; each calling pattern can be compared overall plan cost structures. To incorporate non-cost factors, a survey was conducted among small businesses to

determine which they considered to be most important. These factors were then integrated into the MCDSS using the Analytic Hierarchy Process (AHP). The system allows decision makers to have different preferences for the importance of non-cost factors, different rankings for how each service provider performs on these factors, and different weightings between cost and non-cost factors overall.

III. PROPOSED SYSTEM

In our proposed system, the negotiation phase is explained and is developed.
We develop a web user interface for cloud customers owned by an Intelligent Third Party. The system allows only admin or authenticated customers to login. Admin can add, modify or delete security mechanisms. The user organizational details are received based on which a set of security services are recommended to the user. To recommend security services to the customers, fuzzy rules are used. The user security requirements are matched with the cloud service provider security offerings and the matching output, a decision support model is used to make a decision considering several cost and non-cost factors. The Decision Support model used in our system is Analytic Hierarchy Process. Thus, the best suitable cloud service provider is chosen. An SLA is generated which binds the user with the respective cloud service provider.

Architecture*:* The architecture was then revised and the final architecture with detailing was developed.

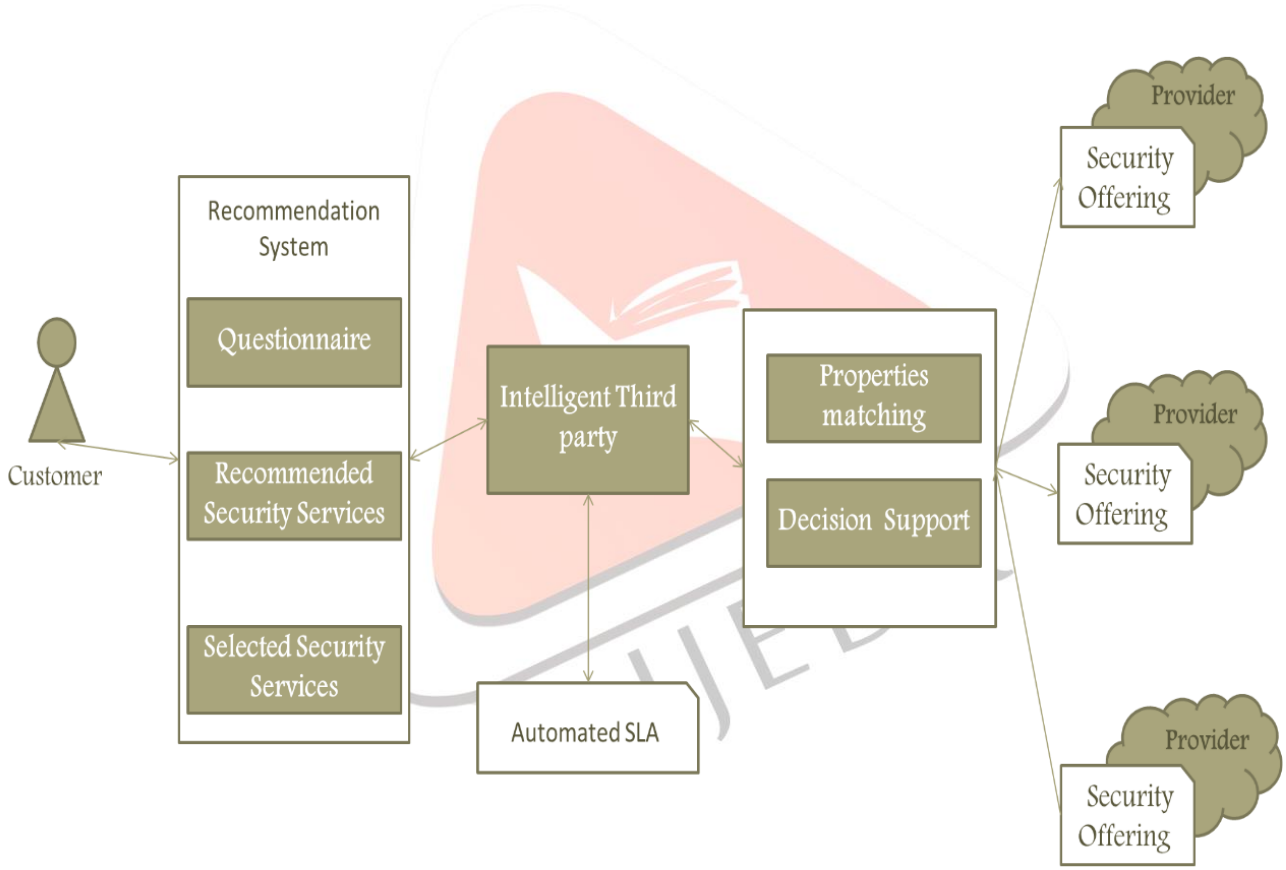

Fig.1: Proposed Architecture Diagram

Introduction to Techniques

Fuzzy rules: A fuzzy rule is defined as a conditional statement in the form:
IF x is A THEN y is B, where x and y are linguistic variables; A and B are linguistic values determined by fuzzy sets on the universe of discourse X and Y, respectively.27 conditions are framed in our project based on fuzzy rules.

Fuzzy rules (Table 1)

Application Security	Platform Security	Infrastructure Security

Low	Low	Medium
Low	Low	High
Low	Medium	Low
Low	Medium	Medium
Low	Medium	High
Low	High	Low
Low	High	Medium
Low	High	High
Medium	Low	Low
Medium	Low	Medium
Medium	Low	High
Medium	Medium	Low
Medium	Medium	Medium
Medium	Medium	High
Medium	High	Low
Medium	High	Medium
Medium	High	High
High	Low	Low
High	Low	Medium
High	Low	High
High	Medium	Low
High	Medium	Medium
High	Medium	High
High	High	Low
High	High	Medium
High	High	High

Analytic Hierarchy Process (AHP)

The AHP is designed to solve complex problems involving multiple criteria. The purpose of the AHP is to facilitate making choices among a number of alternatives and criteria by formulating priorities. The process requires that the DM provides judgments about the relative importance of each criterion and then specifies a preference for each decision alternative on each criterion. The output of AHP is a prioritized ranking, indicating the overall preference for each of the decision alternatives. Following are the three elements in AHP.

Goal:

- What will AHP measure, e.g., prioritize organisms for survey activities
- Goal in our project is: To find a weight value for each CSP.

Criteria: Elements integral to attaining the goal.7 Criteria are taken which involve both cost and non-cost factors.
They are: Cost, Availability, Confidentiality, Flexibility, Integrity, Storage, Contingency planning

Alternatives:

- The organisms of concern.
- Each CSP is an alternative in our case.

Analytic Hierarchy Process

- Do pairwise comparisons for criteria, obtain the relative priority for each criteria against other criteria.
- Same way, do pairwise comparisons for alternatives against each criteria.
- Obtain the relative priorities for each alternative against each criteria.

Ranking Criteria (Table 2)

Preference	Ranking
Not preferred	1
Lightly preferred	2
Moderately preferred	3
Strongly preferred	4
Extremely preferred	5

AHP Matrix (Table 3)

Criterion	Alternative 1	Alternative 2	…	Alternative n
Alternative 1	A1/A1	A1/A2	…	A1/An
Alternative 2	A2/A1	A2/A2	…	A2/An
…	…	…	…	…
Alternative n	An/A1	An/A2	…	An/An

Calculating the total priority (weight value) for each alternative:

- Let rc1, rc2,…. rcN are the relative priorities for each criteria and ra1, ra2,…raN are the relative priorities for each alternative,

$$P = \sum_{i=1}^{n} rci * rai$$

- The total priority is:
- ie., P = (rc1 * ra1) + (rc2 * ra2) +…… + (rcN * raN)

Advantages:

1. The customer need not have knowledge on what security services are required. Based on customer's organization environment, system will recommend the customer with several security services available in various Clouds.
2. Latest security mechanisms are updated and are made available to the user.
3. Multi criteria Decision Making process is achieved.
4. Easy user interface.

IV. FUTURE ENHANCEMENT

The project can be extended as follows:

1. As far, only three administrative controls are provided to the Administrator. All other controls such as deciding match percentage, choosing security services based on fuzzy rules, etc., occur at backend process. Administrator or the ITP can completely be made as front end completely by providing all the administrative controls.
2. The negotiation phase is completely developed. But once an SLA is generated, it has to me monitored again by the ITP itself. This phase is called monitoring of SLA phase which is out of scope for this project and most likely be an extension for this project in the future.

V. CONCLUSION

We have taken an existing system where cloud customers can specify their security requirements efficiently. In our proposed system, we show a way to use these requirements and negotiate. The negotiation process is carried by an ITP which contains a store of CSP security offerings. Security requirements are matched with CSPs' security offerings. Among the matched CSPs' to find the best suitable CSP, AHP model of Decision Support System is used. Finally an SLA is generated based on customer interest.

REFERENCES

[1] Patrick Höner, sCloud Computing Security Requirements and Solutions: a Systematic Literature Review, 2011.

[2] Asma Guesmi, Patrice Clemente, Access Control and security properties Requirements Specification for Clouds' SecLAs, 2013.

[3] André Yang, Sajjad Zahir, A Multi-Criteria Decision Support System for Selecting Cell Phone Services, 2006.

[4] Linlin Wu, Saurabh Kumar Garg and Rajkumar Buyya, A Multi-Criteria Decision Support System for Selecting Cell Phone Services.

[5] Judith M Myerson, Best practices to develop SLAs for cloud computing, 2013

[6] Amazon security whitepaper

a. http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

b. IBM cloud security offerings, http://www.ibm.com/cloud-computing/us/en/security.html