Cloud Surveillance Using SLAs

Soundaryaa.A*1, Sibiya.M *2,Vishnu siddarth.R*3, Vidya.S*4

Department of Computer Science and Engineering,
Anna University,
SNS college of Technology(Autonomous),
Sathy main road,Coimbatore-35,
Tamil Nadu,India.
1soundaryaasou184@gmail.com,
2sibimathi96@gmail.com,
3vishnusidd03@gmail.com
4vidya.sns34@gmail.com

***Abstract*— Cloud computing which provides distributed resources to the users globally. Cloud computing contain scalable architecture which provides multiple challenges exists in the cloud service. This paper describes the different SLA models proposed in cloud computing, to overcome the challenges exists in SLA. Challenges which is related to security and memory allocation. The main related issues involve:(i) representing the security features so that it is understandable by both customer and provider,(ii) The provisioning of security mechanisms able to grant beside security features ,and (iii)continuously monitoring the services in order to verified the fulfillment of specified security.**

***Key Words*— cloud security , security level agreement , optimal resources allocation**

INTRODUCTION

Cloud computing is a source for providing an elastic resources. It is an on-demand cloud computing which gives shared resources or applications to the consumer of the cloud .cloud is an elastic sources of applications or resources. The wide adoption of cloud computing in many application domains has urged the need for the introduction of Service Level Agreements (SLAs) and above all , security related SLAs in order to meet the continuous demand from cloud customers to fulfill diverse business requirements , including security.

Indeed, the wide adoption of SLAs and security of SLAs in the cloud is recent. The adoption of security SLAs, instead, requires automating the process of setting up and configuring security features for a target services on the basis of customer requirements .The well defined representation of security requirement that is understandable for both customer and provider .The capability of effectively monitoring that such requirements are met. Security Service Level Objectives (SLOs) can be offered and granted to the cloud customer .Such security capabilities and metrics can be enforced and monitored through the activation of proper security mechanisms that related monitoring system automatically chosen on the basis of a standard security framework .

LITERATURE SURVEY

Several researchers investigated various resource allocation problems in irrigation system

[1]“Automatically Enforcing Security SLAs in the cloud” by Valentina casola, Alessandra De Benedicts Madalina Erasu, Jolanda Modic and Massimiliano Rak Security SLA should enable the cloud customer to specify its own requirements via SLA and verify the evidence of the grants through measurable Service Level Objectives.SLA Life cycle model for Negotiation, Implementation, Monitoring, Remediation phases.SLA allocates resources with minimum set of cloud resources.

[2]“Service level Aggrement in cloud computing: A Survey” by Usman Wazir, Fiaz Gul Khan, Sajid ShahThe SLA in Cloud computing such as Software as a service (SaaS),platform as a Service (Paas) and Infrastructure as a service(IaaS).Every Service which contains of the five parameters Performance (response time), Customer Level Satisfaction, pricing, Security and SLA violation. This can facilitate Price and Time-slot Negotiation.

[3] “Service Level Agreement in the Cloud Computing” paper by Pankesh Patel, Ajith Ranabahu, Amit ShethThe WSLA framework has the parties(cloud provider,cloud customer and third party), SLA parameters and also Service Level Objective(SLO) to capture service level agreement in a formal way.WSLA contains supporting parties, signatory parties and service definitions.

[4]“Dynamically changing Service Level Agreement (SLAs) Management in cloud computing” by Waleed Halboob,Haider Abbas,Kamel Haouam,Asif YaseenThe changes in the SLA needs updation of the Service level agreement process resolves to the remapping and reformation. Dynamically manage cloud computing SLAs is based on the Real Options Analysis (ROA) concept. This technique incorporates any new change dynamically; by mapping it to alimited number of SLAs based on various options presented by ROA.

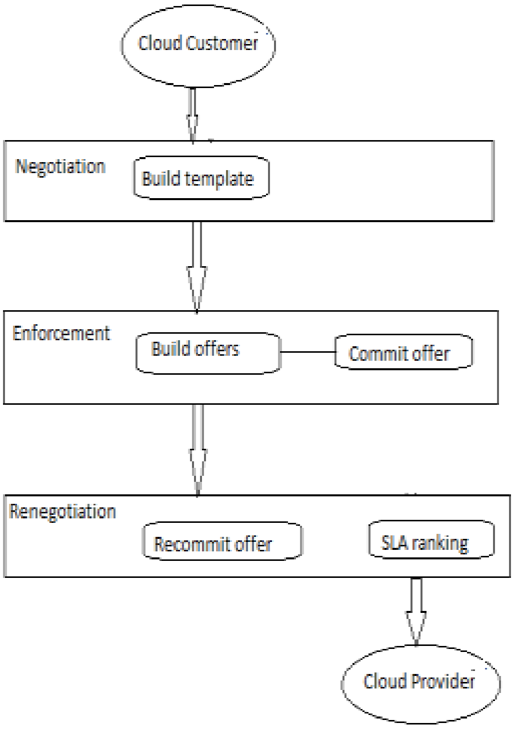
MODULE DESCRIPTION

[1]Negotiation module: The SLA template will be build from the requirements of the customer.The ranking of SLA offers can also be implemented in this module.

[2]Enforcement module: The planning component in this module consists of solver which can compose the SLA offers. The customer has given the opportunity to select one of the

offers and then they commit with it. The customer after committing with SLA offer they will sign in the agreement.

[3]Renegotiation module: After committing with SLA offers customer can renegotiate with cloud provider and can change into new offers without any violation. The customer can resign with new offer.



THE SLA LIFE CYCLE

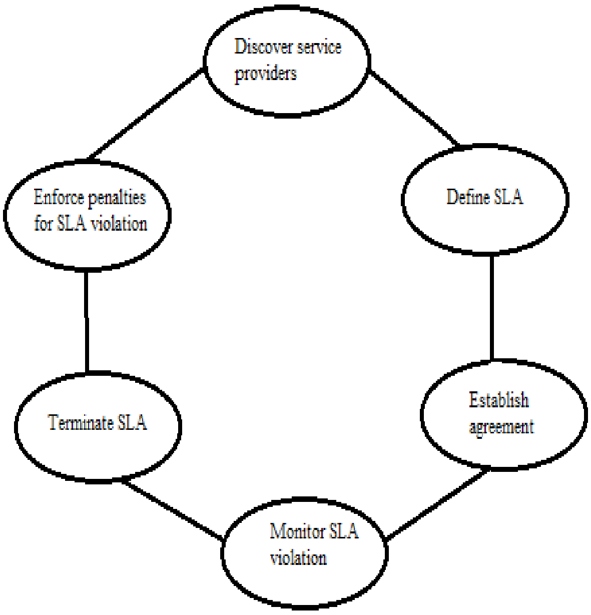
The SLA lifecycle has mainly 4 phases.

[1] Negotiation phase: The cloud customer can provide their security and business requirements with that provider has to generate new SLA offers. An agreement initiator will plays the role of the service provider. SLA template will be prepared with that SLA offers may be build.

[2] Implementation phase: It provides the monitoring and management tool to the customer.

[3] Monitoring phase:The customer and provider has to verify the terms (SLO).

[4] Remediation phase: The SLA violation has been covered and measures has been taken to recover it.



EXISTING SYSTEM

The automatic enforcement of security controls are provided by the cloud services based on a Security SLAs. Automatically allocate the resources in the cloud and also provide security guarantees to the customers. When a customer wishes to use a cloud service, then he will negotiate with the cloud provider and a specific SLA will commit, and the service will be provisioned. If there is a violation of some SLA guarantee term then they cannot commit to the other negotiated SLA. It gives solution for the problem of automatically planning the allocation, on a minimum set of cloud resources, of the software components needed to implement security features requested by a cloud customer. The focus of this paper is on solving the planning problem , that is, on finding the best allocation of software components necessary for enabling security mechanisms on a (minimum) set of virtual machines.WS-Agreement is a context of the GRID computing. It is used to support both the SLA representation and protocol for its automation. The WS-Agreement has two terms guarantee terms and service terms. Guarantee terms consists of the parties will agree and then Service terms consists of description and property terms which has the service name and the functionality in it. The SLA lifecycle will depend on the SPECS framework. The SPECS framework mainly runs on the Negotiation phase. The SPECS framework which is made of three main modules namely Negotiation module which manages Negotiation and Renegotiation phase, the Enforcement module which manages remediation and implementation, the Monitoring module which maintains the customer level satisfaction. There is no possibility to one of the two customer to change the agreement terms before the SLA termination.

PROPOSED SYSTEM

SLA may provide security's based on customer expectation with the guarantee services.The purpose of automatically providing Security a machine readable format based on WSAGs scheme has been introduced. The customer can change their service if they meet any violation in the guarantee term. The proposed approach has (i) matching customers' security requirements reported in a security SLA with a set of security mechanisms offered as a service (security –as –a-service) and on (ii) Automatically SLA will generate and implement an allocation plan for actually deploy the software components providing the desired security mechanisms. Our goal is to find the minimum number of resources to acquire to implement an SLA, the best suited approach to solving the planning problem (from the constraints, optimization function, and also read complexity and flexibility point of view) is to use Integer Linear Programming(ILP). If some violation may occur then it will be automatically notify them to the customer. SLA should be monitor able and it is also enforceable. The customer has been acquired with the security services which has capabilities such as resilience during attacks and protection from the unauthorized users. Resources provider may provide the guarantee terms. The guarantee terms consists of the conditions that is used to verify the agreement. The aim of the planning problem is to optimally deploy implementation of the security requirements. The planning activity has two main objectives the first is to verify that the solution to the customer is feasible and second one is to automatically deploy security mechanism and run it as agreed SLA.

CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we addressed the automatic enforcement of security controls On top of cloud services based on a security SLA. In particular, we focused Our attention on the problem of automatically planning the allocation, on a minimum set of cloud resources, the software components needed to implement security features requested by a cloud customer during negotiation SLAs support end-to-end security and compliance with data protection. The main benefit introduced by our model is its flexibility, as it allows the mechanism developer to add, at development time, mechanism specific constraints that will be automatically customized and included in the model at run-time, based on the terms included in a Security SLA. We built a planning model able to find the optimum allocation of components while taking into account several constraints and configuration parameters provided at runtime and partly dependent on input security requirements. In this the security related representation and the automatic monitoring of the SLA security has been carried out. The future work will be in SLA the power consumption will carried out with the help of SLO. The SPECS framework and GRID Computing provides the Service Level Objectives. The planning problem will be handling with the multiple request from the clients for the better feature in SLA.

REFERENCES

[1]. E.Badidi, "A Cloud Service Broker for SLA-based SaaS Provisioning" in Proc. Of the International Conference on Information Society , Toronto, Canada, June 24-26, 2013, pp. 61–66

[2]. M. A. Rodriguez and R. Buyya, "Deadline Based Resource Provisioning and Scheduling Algorithm for Scientific Workflows on Clouds," IEEE Transaction on Cloud Computing, vol. 2, no. 2, 2014

[3]. B. Jennings and R. Stadler, "Resource management in clouds: Survey and research challenges," *Journal of Network System Management*, vol. 23, no. 3, pp. 567–619, 2015

[4]. "A. Taha, R. Trapero, J. Luna, and N. Suri, "AHP-Based Quantitative Approach for Assessing and Comparing Cloud Security," in Proc. of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Beijing, China, September 24-26, 2014, pp. 391–399

[5]. " QOS-prediction Methods to avoid SLA violation in Post-Interaction Time Phase" by Walayat Hussain,Farookh Hussain.

[6]. "Hierarchical SLA Driven Resource Management for Peak Power-Aware and Energy –Efficient operation of a Cloud Datacenter" by Hadi Goudarzi and Massoud Pedram, Fellow IEEE Transaction on cloud computing,volume 4,No.2 ,April 2016.

[7]. "SLA-based Secure Cloud Application Development : the SPECS framework" by 17th international symposium on Symbolic and Numeric Algorithms for scienitific computing.