Simulation Modelling Practice and Theory 000 (2016) 1–15

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat

Non-deterministic security driven meta scheduler for distributed cloud organizations

Agnieszka Jakóbik[a], Daniel Grzonka[a,*], Francesco Palmieri[b]

[a] Institute of Computer Science Cracow University of Technology, Poland
[b] Universit degli Studi di Salerno Fisciano, Campania, Italy

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Cloud computing
Cloud security
Independent batch scheduling
Genetic algorithms
Multi-agent systems

ABSTRACT

Security is a very complex and challenging problem in Cloud organizations. Ensuring the security of operations within the cloud by also enforcing the users' own security requirements, usually results in a complex tradeoff with the efficiency of the overall system.

In this paper, we developed a novel architectural model enforcing cloud security, based on a multi-agent scheme and a security aware non-deterministic Meta Scheduler driven by genetic heuristics. Such model is explicitly designed to prevent Denial of Service and Timing Attacks over the cloud and has been demonstrated to be integrable within the well-known OpenStack platform. Additionally, we proposed two different models for assuring users security demands. The first is a scoring model that allows scheduling tasks only on the Virtual Machines offering proper security level. The second model takes into account the time spent on the necessary cryptographic operations dedicated to particular task.

The above scheduling system has been simulated in order to assess the effectiveness of the proposed security architecture, resulting in an increased system safety and resiliency against attacks, without sensibly impacting the performance of the whole cloud environment.

1. Introduction

In the recent years Computational Clouds become very essential part of information modern society. New architectural models, management strategies and techniques, supporting these scalable, flexible, virtualized and geographically distributed systems are very intensively developed. Vendors are offering very efficient, sophisticated tools for science, industry and business that are widely used by common users for their day-to-day activities. Computational Cloud (CC) environment can be defined as a model of large-scale distributed physical and virtual network with shared resources. The classic Cloud model consists of many different elements, usually interconnected through an high-performance transport network, that are strictly related each other [1,2]. Data and tasks from Customers are uploaded to be managed, scheduled and processed by Cloud Providers. Users' data are often stored in different sites that may be geographically scattered throughout the world. Very often, the middlemen chain represented by Technical or Business Brokers is incorporated in the processing and resource management infrastructure and handled in an almost fully automated way. Therefore, different aspects of security in such a complex systems become fundamental. Most of the responsibilities to ensure the safety rests with the Cloud Providers that

* Corresponding author.
E-mail address: grzonka.daniel@gmail.com (D. Grzonka).

http://dx.doi.org/10.1016/j.simpat.2016.10.011
1569-190X/

have to provide the proper level of authentication, authorization, and confidentiality as well as the HW/SW infrastructure i.e. reliable and resistant to attacks and security menaces.

The basic security objectives that have to be achieved in modern Clouds are:

- the preservation of **confidentiality** - information/data/services should be accessible only from users/entities who are explicitly authorized for this;
- **integrity** - consists in ensuring the consistency, accuracy, and trustworthiness of all provided service and stored data over their entire life cycle.
- **availability** - involves always guaranteeing access to informations and services as well as their correct behaviour, also in presence of hardware or software failures or security attacks. The inherent redundancy and the distribution of resources in multi-site or federated clouds provide an ideal safeguard against data losses or service interruptions.

In this scenario, **Cloud security** concerns the security of the Cloud infrastructure itself, whereas **Cloud computing security** aims at ensuring trust on the computing services provided by the cloud and finally, **Cloud for security** involves the usage of Cloud technologies to develop and deliver security solutions for massive scale recipients [3]. The presented paper considers the first two problems. Information security methods are used for the cryptography service designed and implemented as the working example for the theoretical model.

By considering the above security objectives, a Cloud architecture can be divided into multiple components that have to be properly secured in order to ensure the security of the whole Cloud system [4]:

- Cloud consumers, providing security when accessing services (e.g. keeping private keys secret),
- Cloud providers: providing secure service orchestration, secure service deployment, secure resource abstraction, and management, as well as physical layer security.
- Cloud brokers: providing secure services aggregation, secure wrapping services, etc.

Cloud infrastructure is exposed to many new security threats. The examples of such are: stealing data and computational time or Distributed Denial-of-Service attacks. Moreover, a large number of threats come from the fact that such systems may have millions of users that have different roles with distinct privileges as far as access to different resources. Service providers must also take into account local security policies, governance and geographical regulations. Consequently, users' side security requirements specified in Service Level Agreement (SLA) have to be taken into consideration during tasks scheduling and resources provisioning.

Eighteen security control points are introduced by NIST in [5]. The model proposed in the paper may be located in the following: Access Control, Protection, Audit and Accountability Planning, Security Assessment and Authorization, Risk Assessment, Identification and Authentication, System and Communications Protection, Incident Response and System and Information Integrity.

Security in clouds is standardized by international independent institutions. The model presented in the paper meets the criteria of NIST Cloud Computing Security Reference Architecture standard [4]:

- Rapid provisioning: automatic service deployment considering the requested service and resources and capabilities.
- Resource providing and changing: mapping authenticated and authorized data and tasks into VMs, assuring proper quality of service as far as computational time usage and security requirements.
- Monitoring and reporting: generating security reports and monitoring the state of the environment.
- Metering: providing a metering for storage, processing, bandwidth, active user accounts. Securely managing metering includes tools for internal control to ensure encrypted storage, secure processing, detection of any abnormal usage, and ensuring compliance security policies.
- Service Level Agreement management: ensuring agree between customer and service providers in the context of scope, quality, responsibility and security.

Guaranteeing the security of both data storage and processing operations together with the integrity of the operating environment itself, according to the more and more challenging customer requirements, usually results in a tradeoff with the efficiency of the overall system. Starting from these considerations, in this work, we developed a novel cloud security architectural model, based on an Agent-Supported Security Aware Non-Deterministic Meta Scheduler. The proposed model may be seen as a part of a secure resource management system. It supports secure task distribution inside the cloud infrastructure according to the security demands coming from cloud consumers. To meet the security requirements, an Independent Batch Scheduler, leveraging a genetic heuristic approach is used. The scheduling process is supported by a multi-agent system that monitors the task flow characterizing the cloud processing activity. Such model is explicitly designed to prevent two types of threats on the Cloud: Denial of Service and Timing Attacks. All the scheduling, monitoring and reporting activities are accomplished in non-deterministic time intervals, which prevents timing attacks.

In addition, two different models for supporting users' security demands are proposed. The first one is a scoring model, that allows scheduling tasks only on the Virtual Machines that are characterized by a security level (and hence a score) higher or equal than the demanded one. In this model the additional processing time associated to security operations is averaged and added to the fee for the total runtime used by each customer. The second model takes into account the time needed by the cryptographic operations associated to each specific task. These operations are modelled by enlarging the time required for processing the task and are considered during the scheduling process.

Please cite this article as: A. Jakóbik et al., Non-deterministic security driven meta scheduler for distributed cloud organizations, Simulation Modelling Practice and Theory (2016), http://dx.doi.org/10.1016/j.simpat.2016.10.011