A REVIEW PAPER ON CRYPTOGRAPHIC APPROACH FOR LICENSE MANAGEMENT SYSTEM IN CLOUD COMPUTING

Urvashi Goel*
M.TECH Electronics
JAIPUR NATIONAL UNIVERSITY
JAIPUR, 302001, INDIA
urru.cs1988@gmail.com

Prof. RAJESHWAR LAL DUA
HOD of Electronics Department
JAIPUR NATIONAL UNIVERSITY
JAIPUR, 302001, INDIA
rndua@yahoo.com

Abstract
Computational world is become very large and complex. Cloud computing has emerged as a popular computing model to support on demand services. It has inherited the legacy technology and adding new ideas. The goal of cloud computing is to make effective utilization of distributed resources, and put them together in order to achieve higher throughput and be able to perform high scale computation problem. So, cloud computing can be defined as a large-scale distributed computing paradigm that is driven by economies of scale, in which, a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet. In cloud computing, the license not only deals with software services, but also it should be able to provide an agreement for infrastructure and platform services in an effective way. A License Management System is definitely an important component of any commercials cloud system. The major challenge in License Management System is provide secure communication of licensees between different parties in cloud environment. Thus traditional license management pattern is not able to specify all necessary specification of agreement of cloud services. After studying various stages of work carried out, we are providing a generalize model of license pattern, which meet all requirement for licensing a service in cloud computing environment.

Keywords: Cryptographic Approach, License Management, Cloud Computing, Saas, Paas, Haas.

1. Introduction

Modern civilization is based on utility service, as-per-as-use basis. As for example, the utility services like water, gas, electricity etc are chargeable as used basis. Similarly, the agenda of cloud computing is to provide on demand IT resources, computation and services on pay per user basis. Cloud computing can provide many users at any point in the world at the same time having different Quality of services (QoS) requirement. Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources like network servers, storage, application and services that can be rapidly provision and released with minimal management effort or service provider's interaction. It can be defined as a large-scale distributed computing paradigm that is driven by economies of scale, in which, a pool of abstracted, virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet.

The term "License" can be define as an agreement between provider and user to form a legal relationship between them. A set of pattern can be used to indicate a license structure, called license pattern. In cloud computing, end user can get service from provider via internet pay-as-per-use basis. The service may be any of the three types: Software-as-a-Service, platform-as-a-service or infrastructure-as-a-service. As cloud services are on demand, highly scalable, and as per used based on the license pattern must be adjusted according to the requirement of cloud computing. In next section 2, we are describing about different patterns for a license management system in cloud computing.

2. Different Approaches for a LMS in Cloud Computing

In this section we are describing the some major works being used for license patterns in cloud computing. The main key concept of cloud computing is virtualization. It is a technique by which we can run multiple virtual machines on a single physical server. Virtualization provides necessary abstraction, encapsulation of different services and fault tolerance.

2.1 Ensuring Data Storage Security in Cloud computing by Cong Wang

Cong Wang et al. [11] stated that data security is a problem in cloud data storage, which is essentially a distributed storage system. And explained their proposed scheme to ensure the correctness of user's data in cloud data storage, an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append relying on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. Their scheme could achieve the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, Could almost guarantee the simultaneous identification of the misbehaving server(s) through detailed security and performance analysis.

2.2 Cloud computing: An Overview By Srinavasa Rao V1 Nageswara Rao NK2 E Kusuma Kumari3

This paper describes the basic concept of cloud computing, and outlines the general architecture with applications of Cloud computing. Cloud computing provides the facility to access shared resources and common infrastructure, offering services on demand over the network to perform operations that meet changing business needs. The location of physical resources and devices being accessed are typically not known to the end user. It also provides facilities for users to develop, deploy and manage their applications 'on the cloud', which entails virtualization of resources that maintains and manages itself.

2.3 Controlling Data in the Cloud By Richard Chow, Philippe Golle, Markus Jakobsson

In this paper, Mr. Richard et al. [4] characterizes the problems and their impact on adoption. They stated as Cloud computing is clearly one of today's most enticing technology areas due, at least in part, to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding momentum and will eventually compromise the vision of cloud computing as a new IT procurement model.

2.4 License Management for Grid and Cloud Computing Environments By Mathias Dalheimer and Franz-Josef Pfreundt

GenLm gives an idea of license management system on cloud computing. It mainly deals with a system, called GenLM, which manages license in cloud and grid environment. A work done by GenLM, a license management solution is suitable for these environments. It has been built in order to provide a secure and robust solution for ISVs that want to extend their software usage to these systems. It also provides ISVs a tool chain to implement arbitrary software licensing models. Different kind of license pattern design and interpretation is given in, which can be used to standardized license specification. It also provides some software license strategy about different license policy like capacity software license, concurrent software license, etc.

2.5 Market –Oriented Computing And Global Grid By Rajkumar Buyya AND Srikumar Venugopal

In this paper both the authors describe about the grid computing with its service-oriented architecture which provides the hardware and software services and infrastructure for secure and uniform access to heterogeneous resources and enables the formation and management of virtual organizations (VOs). They also stated that grid computing also supports application and services composition, workflow expression, scheduling, and execution management and service-level agreement (SLA)-based allocation of resources. The development of the Grid infrastructure, both hardware and software, has become the focus of a large community of researchers and developers in both academia and industry. The major problems being addressed by Grid developments are the social problems involved in collaborative research:

Improving distributed management while retaining full control over locally managed resources

Improving the availability of data and identifying problems and solutions to data access patterns

Providing researchers with a uniform user-friendly environment that enables access to a wider range of physically distributed facilities improving productivity.

2.6 Above the Clouds: A Berkeley View of Cloud Computing By Anthony D. Joseph, Randy Katz

In this paper we found the answers of the following questions in respect of cloud computing as:

What is Cloud Computing, and how is it different from previous paradigm shifts such as Software as a Service (SaaS)?

Why is Cloud Computing poised to take off now, whereas previous attempts have foundered?

What does it take to become a Cloud Computing provider, and why would a company consider becoming one?
What new opportunities are either enabled by or potential drivers of Cloud Computing?
How might we classify current Cloud Computing offerings across a spectrum, and how do the technical and business challenges differ depending on where in the spectrum a particular offering lies?
What, if any, are the new economic models enabled by Cloud Computing, and how can a service operator decide whether to move to the cloud or stay in a private datacenter?
What are the top 10 obstacles to the success of Cloud Computing—and the corresponding top 10 opportunities available for overcoming the obstacles?
What changes should be made to the design of future applications software, infrastructure software, and hardware to match the needs and opportunities of Cloud Computing?

2.7 Security Analysis of Cloud Management Interfaces By Juraj Somorovsky

This paper states that a security analysis pertaining to the control interfaces of a large Public Cloud (Amazon) and a widely used Private Cloud software (Eucalyptus). Cloud Computing resources are handled through control interfaces. It is through these interfaces that the new machine images can be added, existing ones can be modified, and instances can be started or ceased. Effectively, a successful attack on a Cloud control interface grants the attacker a complete power over the victim's account, with all the stored data included. In this paper, also refer two distinct classes of attacks on the two main authentication mechanisms used in Amazon EC2 and Eucalyptus cloud control interfaces. The first class of attacks complies of the XML Signature Wrapping attacks on the public SOAP interface of the Cloud. The most important in this analysis is that managing and maintaining the security of a cloud control system and interface is one of the most critical challenges for cloud system providers worldwide.

2.8 Different Aspects Of Cloud Security BY Madhu Chauhan

This paper presented a selection of issues of Cloud Computing security and approaches of virtualization. And investigated ongoing issues with application of XML Signature and the Web Services security frameworks (attacking the Cloud Computing system itself), also discussed the importance and capabilities of browser security in the Cloud Computing context (SaaS), raised concerns about Cloud service integrity and binding issues (PaaS), and sketched the threat of flooding attacks on Cloud systems (IaaS). Cloud computing is defined as a pool of virtualized computer resources. Based on this Virtualization the Cloud Computing paradigm allows workloads to be deployed and scaled-out quickly through the rapid provisioning of physical machines. As can be derived from paper observations, a first good starting point for improving Cloud Computing security consists in strengthening the security capabilities of both Web browsers and Web Service frameworks.

2.9 A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment by M.Sudha

M. Sudha et al.[9], stated that Cloud service providers enable users to access and use the necessary resources via the internet. To provide these resources, providers often fall back upon other providers in the cloud, hence this raises security issues in Cloud Environment as Clouds have no borders and the data can be physically located anywhere in the world. So this phenomenon raises serious issues regarding user authentication and data confidentiality. Due to these security issues they implement a simple Data Protection framework which performs authentication, verification and encrypted data transfer, thus maintaining data confidentiality. And Advanced Encryption Standard security algorithm is also implemented for ensuring security framework.

2.10 Data security in the world of cloud computing by John Harauz

John Harauz et al. [10], described the Security Content automation protocol (SCAP) and benefits it can provide with latest cloud computing paradigm with reference to the latest report released by NIST, giving insight as to what SCAP is trying to do, It states that many tools for system security, such as patch management and vulnerability management software, use proprietary formats nomenclatures, measurements, terminology, and content. Their example states that, when vulnerability scanners do not use standardized names for vulnerabilities, it might not be clear to security staff whether multiple scanners are referencing the same vulnerabilities in their reports.

3. FRAMEWORK FOR LICENSE MANAGEMENT SYSTEM

After analyzing or studying different aspects of license management system in cloud computing we proposed the framework for License Management System on the basis of different conclusions made by different analysis. So, in this section before define a framework one must understand the system architecture.

3.1 SYSTEM ARCHITECTURE

Before discussing our proposed framework for license management system, it is required to discuss architecture of cloud environment used here. Basically it consists of three main users as given below:

3.1.1 Cloud users
These are the general users who want to get service from cloud; they may ask three different kinds of services: software, hardware and platform.
3.1.2 Cloud provider
These are the original service provider, who provides services to cloud environment .In our system may contain a number of Cloud Provider, who can provide different service. We can classify Cloud provider into three categories based on the service they provide like, software provider, hardware provider, and platform provider. In our system, we assume that there are many numbers of Cloud Providers.
3.1.3 Cloud Vendor
These are the entity who manages the interaction between cloud user and cloud provider. The main function of cloud vendor is to provide certificate and manage license. We assume that Cloud vendor is already authenticated to cloud provide. Cloud vendor has the capability of handling multiple cloud providers. When a user send a request for a service, Cloud vendor can search the whole list of Cloud provider and find the Best suited list of Cloud provider who able to provide service to the cloud user in most cost-effected way.
The basic interaction between different users is given in Figure 3.1.

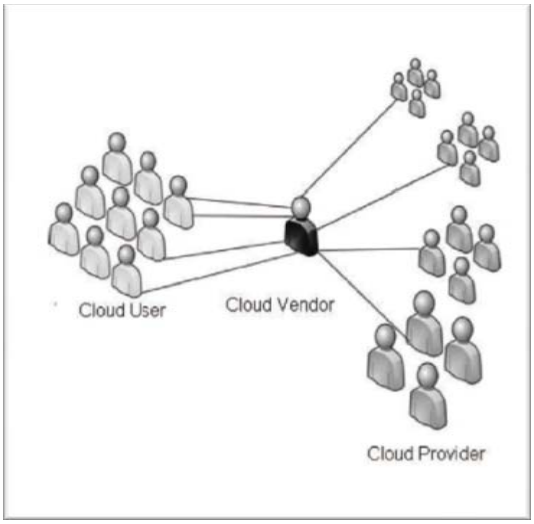

Figure 3.1: BASIC CLOUD MODEL FOR LMS

3.2 System Model
Our license management system consists of 3 main components:

3.2.1 Client License Interface
Client License Interface (CLI) is software installed in the cloud customer side to retrain license which provide services access through cloud. This Client side software allow user to specify requirement of the service. This Client license Interface is responsible to authenticate user, generate license requirement specification and send to cloud provider. It also used to provide license encryption and decryption. The overall functions are discussed in System protocol section.
3.2.2 License manager
This the core part of license management scheme. This component mainly resides in cloud vendor. This is mainly consists of two Modules:

(1) Software module
This software handles the license generation and license verification all computation part of license management. There are two type of software used to deal with license:
(i) License generator
this software module is responsible to generate appropriate temporary license and update License entry table (LED).
(ii) 1st level License verifier
It is responsible to verify the license send by client License interface and perform restricted check on it and also perform some modification on LED, if required.

(2) Database module
An appropriate database is required to store client information and the license information.

This database is called as License Entry Database (LED). LED is updated by both software module of license manager. The Data base stature and function of LED module is discussed details in System design protocol section.

(3) Cloud providers Module

To ensure high security of accessing services, one more license verification module is added in Cloud provider side. This software contains only one module as below:

(i) 2nd Level License verifier

This second level of verification is done by cloud provider, which also perform certain check about the license (may be part of the license and cloud vendor authentication) before schedule to processing unit.

3.3 System Description

After having the brief overview of different component, let's see how these all module interact with each other. The overall Algorithm is given as below:

Step1. Initially cloud customer, who wants to get service from cloud, should request for a temporary license for renting services. He first login Client license Interface, specifying software requirement specification.

Step 2. After successfully loin to the system, CLI generate license request and sent to the license generator/Allocator in cloud vendor.

Step 3. License generator get the license request from client and perform an initial checking, verifying user and also verifying software rent specifications.

Step 4. After satisfying this it will generate a Software license specification vector which contain all necessary information about the license (basically a temporary license token) and send back to the user.

Step 5. It also insert an entry into LED to keep track the license of the user.

Step 6. When user wants to access the software he can send data item along with previously allotted license.

Step 7. License verifier checks the validity and authentication of license and perhaps modify the LED (license entry database) according to current database and redirect request to cloud provider.

Step 8. 1st level License verifier generate a token to authenticate cloud provider and send the token along with job to cloud provider.

Step 9. After getting the token and input dataset from cloud vendor, it performs some security check (2nd level of verification to authenticate the cloud vendor) and then schedule that job on suitable processing unit.

Step 10. Cloud provider generate results and reply back directly to sender or send to user via cloud vendor.

All the interaction between the components is shown in figure 3.2:

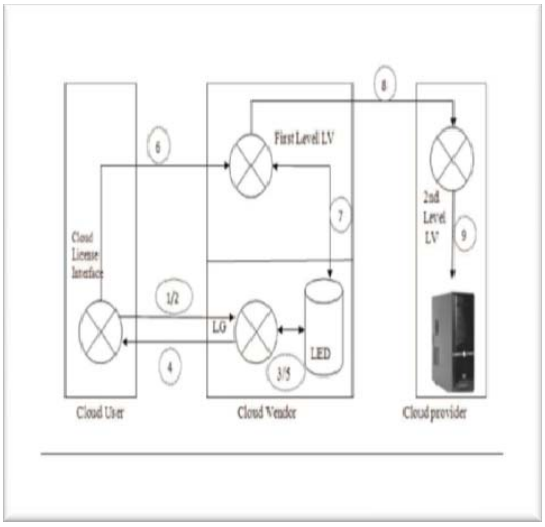

FIGURE3.2: License Management System

CONCLUSION

On the basis of some analysis, we discuss about the framework of LMS in which it can handle the major problem of representation of license. This significantly improves the complexity of license generation and license verification. In this paper we also discuss Our secure license exchange algorithm provide secure communication between cloud user, cloud provider and cloud vendor. Thus, it removes the problem of trapping license or modify license by user or other attackers. As results, we found that our model worked well according to our claims. In the future One major work may be to extend the proposed framework by including the temporary license number assignment and reuse the license number when it expires. It must provide a collision resolution for license number, which is at the same time there should not be two licenses having the same

number. This will remove the problem of assigning license number when a huge number of licenses are generated. In this paper ahead of this we have a future plan for implementing this proposed framework by which We can also improve the system by optimizing of license allocation and reallocation.

References

[1] Boss,G.; Malladi,P.;Quan,D.; Legregni,L.;Hall,H. "Cloud Computing".
[2] BUYYA, R.;VENUGOPAL, S.(2010) –"MARKET-ORIENTED COMPUTING AND GLOBAL GRID" John Wiley & Sons, Inc. .
[3] Chauhan, M ; Malhotra, R; Pathak, M. (2012)- "DIFFERENT ASPECTS OF CLOUD SECURITY"- Vol. 2, Issue 2, Mar-Apr, pp.864-869.
[4] Chow, R; Golle, P; Jakobsson, M. –"Controlling Data in the Cloud"
[5] Dalheimer, M. - "License Management for Grid and Cloud Computing Environments".
[6] Frankova,G. (2007) Service Level Agreements: "Web Services and Security", ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg,vol. 4607.
[7] Joseph, D; Katz, R.(2009-28) "Above the Clouds: A Berkeley View of Cloud Computing" Technical Report No.UCB/EECS-http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009- 28.html February 10.
[8] RAO, S; RAO, N; KUMARI, K. (2005-2009)–"CLOUD COMPUTING: AN OVERVIEW" Journal of Theoretical and Applied Information Technology ,JATIT.
[9] Somorovsky, J; Heiderich, M; Jensen, M; Schwenk, J. - "Security Analysis of Cloud Management Interfaces"- CCSW' 11,October 21, 2011, Chicago, Illinois, USA.
[10] Sudha, M; Monica, M; (2010)- "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment"- Volume 12– No.8 December.
[11] Wang,C; Wang,Q; Ren, K.(2009)—"Ensuring Data Storage Security in Cloud computing" 978-1-4244-3876-1/2/ IEEE.