Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 48 (2015) 198 – 203

Procedia Computer Science

International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,

Bhubaneswar, Odisha, India

Enhancing security in Cloud using Trusted Monitoring Framework

M.Arun Fera[a], C.manikandaprabhu[b], Ilakiya Natarajan[c], K.Brinda[d], R.Darathiprincy[e] *

[a]*Assistant Professor Dept of IT, Thiagarajar College of engineering, Madurai, 625015, India*
[b,c,d,e]*Final year Dept of IT, Thiagarajar College of engineering, Madurai, 625015, India*

Abstract

Cloud computing is a technology that provides network based services on demand. Cloud computing technology provides advantages to end users and business organizations. Few notable advantages are cost efficiency, increased storage capacity, backup and recovery, continuous resource availability and location independence. Data owners host their private data in the cloud and worry about unauthorized access of their data. They feel uncomfortable about any user misusing their private data. This insecure feeling of data owners holds them back from using cloud services. Any unauthorized users accessing the owner's private data leads to accountability issues. We design a trusted monitoring framework, which provides a chain of trust that excludes the untrusted privileged domain, as well as utilizing the trusted computing technology to ensure the integrity of the monitoring environment. To solve the accountability issue, a mechanism to monitor the actual data usage is proposed. This approach grants access rights to users based on their role and also monitors every access to the owner's data, verifying that the service level agreements have been violated or not.

Keywords: Cloud computing, trusted monitoring framework, Security, Chain of trust, Data auditability.

* Corresponding author. Tel.: +919600302361;
*E-mail address:*cmanikandaprabhuc@gmail.com

doi:10.1016/j.procs.2015.04.170

1. Introduction

Cloud Computing technology provides advantages to end users and business organizations. Few notable advantages are cost efficiency, increased storage capacity, backup and recovery, continuous resource availability and location independence. In spite of these advantages, the biggest issue with the cloud is the "Security‟. Though there are several advantages with cloud, it also imposes several security threats related to outsourced user's data. Since private data is hosted in the cloud and they are being processed at remote machines and are administered by the cloud service providers (CSP), the users are worried about loss of data control in the cloud. There are various reasons for the CSP to involve in unfaithful disclosure or leakage of user's data to any external entity that may turn out to be a serious privacy and security concern for any user towards his/her data. Cloud Users do not know the machines where their data are processed, so they start bothering about losing control over their data. There are no specific mechanisms to check if the service level agreements made between the data owner and the end users have been preserved or not. Data is often being outsourced in cloud, leading to accountability issues and manipulation of personally identifiable information. The monitoring mechanism involves third party services. The third party is an external entity who can behave unfaithfully while the data is disclosed during the auditing process [1]. Moreover, simply relying on a third party auditor without applying any cryptographic technique on the user's data may turn the situation even more badly. So, downloading the user's data alone for auditing will not help for verifying the integrity of user's data since downloading the entire data is expensive because of I/O and transmission cost through the network. To solve these security problems with the cloud, users are assigned access rights based on their role and if any user tries to violate the assigned access rights the data owner is notified with a log report stating about the service level agreement violation. Section 2 tells the related work done in this domain, section 3 explains the work that is done for solving the security issues, section 4 describes the results and the discussion among the results and section 5 concludes the paper.

2. Related work

Cloud Computing is a technology that provides network based services on-demand. Data owners host their private data in the cloud and worry about unauthorized access of their data [2]. They feel uncomfortable about any user misusing their private data. This insecure feeling of data owners holds them back from using cloud services. Any unauthorized users accessing the owner's private data leads to accountability issues. To solve the accountability issue, a mechanism to monitor the actual data usage is proposed. This approach grants access rights to users based on their role and also monitors every access to the owner's data, verifying that the service level agreements have been violated or not.

Though there are several advantages with cloud, it also imposes several security threats related to outsourced user's data. Since private data is hosted in the cloud and they are being processed at remote machines and are administered by the cloud service providers (CSP), the users are worried about loss of data control in the cloud. There are various reasons for the CSP to involve in unfaithful disclosure or leakage of user's data to any external entity that may turn out to be a serious privacy and security concern for any user towards his/her data [3].

Virtualization is a pillar technology in cloud computing for multiplexing computing resources on a single cloud platform for multiple cloud tenants. Monitoring the behaviour of virtual machines (VMs) on a cloud platform is a critical requirement for cloud tenants. Existing monitoring mechanisms on virtualized platforms either takes a complete VM as the monitoring granularity, such that they cannot capture the malicious behaviours within individual VMs, or they focus on specific monitoring functions that cannot be used for heterogeneous VMs concurrently running on a single cloud node. Furthermore, the existing monitoring mechanisms have made an assumption that the privileged domain is trusted to act as expected, which causes the cloud tenants' concern about security because the privileged domain in fact could not act as the tenants' expectation. We design a trusted monitoring framework, which provides a chain of trust that excludes the untrusted privileged domain, by deploying an independent guest domain for the monitoring purpose, as well as utilizing the trusted computing technology to ensure the integrity of the monitoring environment.

The user is more concerned with the privacy and security issues in the cloud environment. Ina cloud platform, the