Topic: Ensuring Virtualization security in Cloud Computing Environment

Abstract

The growth of internet era leads to a major transformation in a storage of data and accessing the applications. One such new trend that promises the endurance is the Cloud computing. The key element that comprises the cloud computing is the "cloud" a collective network of servers or a massive scale of individual computers connected to a grid. Cloud Computing, works on a basis in which the programs are not run from the single personal computer, but rather they are stored on the servers and accessed via the Cloud.

Cloud storage security may take as some advantages and too. Many companies and private sectors are providing cloud storage with low cost and allocate space according to their requirements. Meanwhile security lack still remains afraid for some users. In fact, everyday users overcome lot of security issues behind cloud data sharing. So they produce advert of high secure and sharing data. But still doubt remains for many clients. For the security purpose, developers implemented cryptography concepts between the client and server.This research work focuses on designing solutions for data security algorithms in cloud computing system

Cloud computing adoption and diffusion are threatened unresolved security issues that affect both users and provider. In this research work, create how virtualization can increase the security of cloud computing, by protecting both the integrity of guest virtual machines and cloud infrastructure components. In particular, I propose a novel architecture, Advanced Cloud Protection System (ACPS), aimed at guaranteeing increased security to cloud resources. ACPS can be solved on several cloud solutions and can effectively monitor the integrity of guest and infrastructure components while remaining fully transparent to virtual machines and to cloud users. ACPS can locally react to security breaches as well as notify a further security management layer of such events. A prototype of our ACPS proposal is fully implemented on two open source solutions: Eucalyptus and open ECP. The prototype is tested against effectiveness and performance. In particular a) effectiveness is shown testing our prototype against attacks known in the literature b) performance evaluation of the ACPS prototype is carried out under different types of workload. Results show that our proposal is resilient against attacks and that the introduced overhead is small when compared to the provided features.