Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 92 (2016) 506 – 512

Procedia Computer Science

2nd International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2016)

Srikanta Patnaik, Editor in Chief

Conference Organized by Interscience Institute of Management and Technology

Bhubaneswar, Odisha, India

Trusted and Reputed Services using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud

Sarojini G[a*],Vijayakumar.A[a], Selvamani.K[b]

[a,]Final ME Student, Department of Information Technology,Jerusalem College of Engineering,Chennai, 600100, India
[b]Assistant Professor, Department of Computer Science and Engineering,Anna University,Chennai 600025, India

Abstract

In cloud computing, trust management is more important when providing users with virtualized and scalable web services. Many existing systems sharply divide trust value into right or wrong. Trust means an act of faith; confidence and reliability in something that is expected to behave or deliver as promised. Trust is required to solve the problem created due to uncertainty and vulnerability caused by open conditions of cloud computing. This paper presents a mutual trust for both cloud users and cloud service providers to avoid security related issues in cloud computing. This is to be done by providing trusted services to the cloud users using enhanced mutual trust to be known as Enhanced Mutual Trusted Access Control Algorithm (EMTACA). This paper proposes the model which considers both the cloud user's behavior trust and cloud service provider's credibility. Trust calculations are based on the behavior which includes history of direct communication between both the user and service provider; based on friends and third party recommendations. The hierarchy based reputation systems has suggested how to safeguard the data objects in the level of file access which ensures the cloud security. The different security measures are used to protect the different cloud services. This proposed system which includes the EMTACA algorithm can assure enhanced, guaranteed and trusted and reputation based cloud services among the users in a cloud environment.

Peer-review under responsibility of the Organizing Committee of ICCC 2016

Keywords: *Cloud Computing; Behavioral Trust; Mutual Trusted Access Control; Reputation System; Cloud Security; EMTACA.*

*Sarojini G., *VijayakumarA Tel.: +917299977815..
*E-mail address:*sarojinigs@gmail.com, kaniporiyalan@yahoo.co.in.

Peer-review under responsibility of the Organizing Committee of ICCC 2016
doi:10.1016/j.procs.2016.07.375

1. Introduction

2. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal service provider interaction. The main idea behind the cloud is that you can access all your information over the internet without having any detailed knowledge of the infrastructure used to enable it. The different cloud types are Public clouds; Private clouds; Hybrid clouds; Virtual Private clouds. Trust in cloud plays a major role in providing services and can be considered as cloud security feature as well. Trust in general is a belief that someone or something is reliable, good, honest and effective. Trust in cloud is required because resources have to be provided efficiently since the resources are limited. Trusted cloud users can only access the cloud and simultaneously users are allowed to select the most credible cloud service providers. This helps in avoiding attacks from illegal and malicious users as well as service providers. Reputation is another factor which has a major effect while providing cloud services. Reputation in general is the assessment of the society about performing a task or service. Cloud users require a reputed system to guarantee the safety of their data, investment and service. Reputation is gained through trust which might be through self experience or through existing users recommendation. Trust and Reputation are mutual for both the cloud users and cloud service providers since their status are equal.

3. Literature Survey

In 1994, Marsh[4] introduced the concept of trust for the first time, and then Baize introduced trust management into network related security applications. Hassan[5] proposed a novel trust evaluation method suitable for the pervasive environment and it considered the dynamic nature of trust and incorporated uncertainty of trust modeling. So, it was well suited for the pervasive environment and could resist malicious behavior. George[6] defined trust relationship as a directed graph path problem. This trust computing method accurately reflected the global trust conditions as well had a good adaptability and malicious detection capability. Wang Wej[7] proposed a trusted resource scheduling algorithm based on Bayesian Theory which is able to obtain an accurate assessment of trust with a much smaller time complexity. Besides, some other dynamic trust models based on fuzzy logic, machine learning, which can better meet the demands of dynamic network were also proposed. Although these dynamic trust models introduced above has many advantages, but there are problems due to the subjective characteristic of trust. Many trust models did not specify the specific implementation issues and the evaluation of performance of trust model is hard. Shouxin Wagng [9] proposed a subjective trust evaluation approach. A cloud model has been introduced to overcome the limitations of fuzzy set theory with the help of an accurate and sole membership degree which has shown effectiveness. Audun Josang [10] presented a survey of trust and reputation systems for online service provision with the basic idea of trust and reputation. Examples would be in building initial trust bootstrapping coalition operations without predefined trust, and authentication of certificates generated by another party when links are down or ensuring safety before entering a new zone. In addition, trust management has diverse applicability in many decision making situations including intrusion detection, authentication, access control, key management, isolating misbehaving nodes for effective routing, and other purposes. Trust management, including trust establishment, trust update, and trust revocation, in cloud environment is also much more challenging than in traditional centralized environments. The trust in the mobile adhoc network is given as a proposed work in the papers. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to changes in topology induced by node mobility or node failure. Further, resource constraints often confine the trust evaluation process only to local information. The dynamic nature and characteristics of cloud services and result in uncertainty and incompleteness of the trust evidence, which is continuously changing over time. Despite a couple of surveys of trust management, a comprehensive survey of trust management in cloud does not exist and is the main aim of this paper. It is to let parties provide