Abstract

Determining the user's trust is a growing concern for ensuring privacy and security in a cloud computing environment. In a cloud, user's data is stored in one or more remote server(s) which poses more security challenges for the system. Most important concern is to protect user's sensitive information from other users and hackers who may cause data leakage in cloud storage. This paper is to aims towards proposing a new trusted and collaborative agent-based two-tier framework to protect cloud resources. Uniqueness of the proposed security solution is to ensure security and privacy both at the service provider level as well as at the user level in a cloud environment. Existing System is mainly designed under traditional cryptography techniques which will be frequently affected with attacks such as SQL injections, Cross Site Scripting, Domain name service (DNS) attack, Denial of service (DOS) attack and Distributed Denial of service (DDOS) attack. Disadvantages of Existing System is less secured, It is frequently affected with attacks such as SQL injection, Cross Site Scripting, Domain Name Service (DNS) attack, Denial of Service (DOS) attack, Distributed Denial of Service (DDOS) attack, there is frequent data leakage and it has poor performance. Proposed Cloud Security Framework is Two-tier Architecture includes Broker Domain and Cloud Service.
Provider Domain. Another one is Broker Domain includes Cloud Service User (CSU), Proxy Server and Cloud Service User Agent (CSU_A). Another one is Cloud Service Provider Domain includes Cloud Service Provider (CSP) and Cloud Service Provider Agent (CSP_A). Features of Proposed Model are domain-based and set a special trust agent in each domain to manage trust. It distinguishes two different roles in cloud: customer and provider and designs different trust strategies for them. Advantages are Domain remains unaffected (with only decreased amount of trust degree than that of non-trusted users) when a said non-trusted CSU does malicious activities in the system. The trust degree of the domain will decrease accordingly with the malicious activities and updating policies. The CSP_A and CSU_A maintain their own databases, user activities information and updated trust degrees for calculating updated trust degree. It provides more security when compared to earlier models. The performance of the system is high to that of the previous models.

References

- Xiangyi Meng, Guangwei Zhang, Jianchu Kang, Hesong Li, Deyi Li. : A New Subjective Trust Model Based on Cloud Model. ICNCSC 2008, 5th IEEE International Conference on Networking, Sensing and Control Sanya China April 6-8, 2008.
- Rajkumar Buyya, Chee Shin Yeo1 and Srikumar Venugopal "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities".


Index Terms

Computer Science

Security

Keywords
Cloud security  Denial of service (DOS) attack  ensuring privacy and security
Distributed Denial of service (DDOS)

Domain Name Service (DNS)

Cloud Service User (CSU)

Proxy Server and Cloud Service User Agent (CSU_A)

cloud computing environment

VM (Virtual Machine) monitoring system.