Abstract

In IT industry now a days there is a need for several new resources and storage requirement for terabyte of data generated every day. Cloud Computing is a solution for this in a cost effective manner. Cloud Computing provides on demand resources as services to client. Cloud is highly scalable, flexible and platform in dependable. Although it is benefiting the clients in several ways but as data is stored remotely it has many security loopholes like attacks, data loss, other authentication and security issues. In this paper an authentication model is proposed for cloud computing based on Kerberos protocol using threshold cryptography to provide more security and to increase the availability of key. This model can also benefit by filtering the unauthorized access and to reduce the burden of computation and memory usage of cloud provider against authentication checks for each client. It acts as a third party between cloud server and clients to allow authorized and secure access to cloud services. In this paper we will take a review of related work for cloud security issues and attacks. In next section we will discuss the proposed architecture and its working. Next we will see how it can provide better security and availability to key used for authentication.
A Secure Key for Cloud using Threshold Cryptography in Kerberos

References

- Jeffrey Lok Tin Woo, and Mahesh V., "Tripunitara Composing Kerberos and Multimedia Internet Keying (MIKEY) for Authenticated Transport of Group Keys", IEEE, Transactions on Parallel and Distributed Systems, 2013, pp 1-11.
- C. C. Tan, Q. Liu, and J. Wu, "Secure Locking For Untrusted Clouds", 4th
- www.wikipedia.com

Index Terms
- Computer Science
- Security

Keywords
- Cloud Computing
- Kerberos
- Threshold Cryptography
- Security
- Authentication.