Abstract

Previously, computer software was not written with security in mind; but because of the increasing frequency and sophistication of malicious attacks against information systems, modern software design methodologies include security as a primary objective. With cloud computing systems seeking to meet multiple objectives, such as cost, performance, reliability, maintainability, and security, trade-offs have to be made. Any cloud server is vulnerable to an attacker with unlimited time and physical access to the server. Additionally, physical problems could cause the server to have down time. This would be a loss of availability, which is one of the key principles of the security triad — confidentiality, integrity, and availability (CIA). Availability addresses the issues that include attempts by malicious entities to control, destroy, or damage computing resources and deny legitimate access to systems. While availability is being preserved, confidentiality and integrity have to be maintained. In this paper, we propose an effective and flexible scheme opposing to its predecessor. By utilizing the homomorphic token and cryptographic encryption method achieves the integration of storage correctness insurance and error localization i.e. the misbehaving of servers. The new scheme further supports to dynamic operations on data blocks like delete, update, insert, append etc.
Secure Approach for Data in Cloud Computing

- I-Hsun Chuang, Syuan-Hao Li, Kuan-Chieh Huang, Yau-Hwang Kuo, "An Effective Privacy Protection Scheme for Cloud Computing", ICACT-2011, Pages 260-265
- Ayad F. Barsoum and M. Anwar Hasan, "On Data Replication and Storage Security over Cloud Computing: Are we getting what we are paying for?", in digital library citeseerx.ist.psu.edu/viewdoc/ pg. 1-36

Index Terms

Computer Science

Security
Keywords
Availability  Cloud Computing  Data Security