Abstract

Cloud Computing has attracted a lot of attention in both academia and industry lately. With its focus on scaling, collaboration, agility, availability and cost reduction, cloud computing offers a compelling alternative to in-house IT solutions. However, by "outsourcing" the computing infrastructure, it introduces a number of security issues. Specifically, since cloud computing is a shared computing platform, it needs to provide strong mechanisms for authenticating its users and ensuring that no confidential information stored on the cloud is compromised. This paper addresses a number of vulnerabilities in existing authentication mechanisms and proposes enhancements to mitigate these vulnerabilities. In addition, the paper studies how these enhancements affect performance. The results show that the existing vulnerabilities can be overcome by the proposed mechanisms. However, this results, in the worst case, in a six-fold increase in execution time. This can be considered relatively small when security is prime important.
Index Terms

Computer Science

Distributed Systems

Keywords