Abstract

Cloud computing is introducing many huge changes to people's lifestyle and working pattern recently for its multitudinous benefits. However, the security of cloud computing is always the focus of numerous potential cloud customers, and a big barrier for its widespread applications. Companies have increasingly turned to application service providers (ASPs) or Software as a Service (SaaS) vendors to offer specialized web-based services that will cut costs and provide specific and focused applications to users. The complexity of designing, installing, configuring, deploying, and supporting the system with internal resources can be eliminated with this type of methodology, providing great benefit to organizations. However, these models can present an authentication problem for corporations with a large number of external service providers. This paper describes the implementation of Security Assertion Markup Language (SAML) and its capabilities to provide secure single sign-on (SSO) solutions for externally hosted applications, including security measures for federated identity management systems using multifactor authentication, which also includes Biometric identification.
Secure Credential Federation for Hybrid Cloud Environment with SAML Enabled Multifactor Authentication using Biometrics


Index Terms

Computer Science Security

Keywords

SAML SSO Multifactor Cloud security Biometrics Federated identity management