**云计算中的身份认证技术研究**

余幸杰,高能,江伟玉

**一、论文相关信息（Related Information）**

Date：2012

Journal Information：



Author Unit：中国科学院信息工程研究所信息安全国家重点实验室、中国科学院研究生院

Key Words：身份认证；安全凭证；单点登录；OpenID；SAML

Citation Times：103

**二、摘要（Abstract）**

We analyze the security-credentials-based authentication and the single sign-on-based federated authentication, and make a comparison among the popular schemes. In addition, we present some methods and suggestions to improve the authentication mechanisms in cloud computing.

**三、引言（Introduction）**

The degree of user control over computing resources is greatly reduced. Therefore, the development of cloud computing has brought massive access authentication requests and complex user authority management, which has promoted the continuous development of identity authentication technology. Identity authentication technologies based on multiple security credentials have emerged in cloud computing. With the popularization of cloud computing, a large amount of user sensitive data is stored in the cloud. Once the user's identity is counterfeited, it is easy to cause the leakage of privacy and sensitive data. Traditional identity authentication technology based on a single credential can no longer meet the security needs of users. Many cloud service providers have adopted identity authentication technologies based on multiple security credentials, but there is currently a lack of summary and comparison of these technologies. Therefore, this article summarizes the multiple credential-based identity authentication technologies that are currently widely used in cloud computing. There are complex identity authentication scenarios in cloud computing, and API call source authentication is a typical authentication scenario. According to the different types of APIs, the security credentials used for authentication of API call sources are also different. This article focuses on the A PI call source authentication mechanism based on different security credentials. The development of cloud computing has promoted the development of federated identity authentication technology based on single sign-on. The development of federated identity authentication technology allows users to log in to multiple cloud services through a single account, which greatly simplifies user operations. Based on the single sign-on scheme, a federated identity authentication mechanism can be well implemented. This article introduces in detail the most widely used single sign-on scheme-O penID protocol and SA M L-based single sign-on scheme, and analyzes and compares them, and puts forward some suggestions for improvement.

**四、各部分总结（Headings of all sections and conclusion）**

**1. Identity authentication based on security credentials**

Traditional identity authentication is often based on user names and passwords. Faced with the complex application environment and role definition in cloud computing, the user name and password are used as a single security credential

The method can no longer meet the security requirements of multiple authentication scenarios in cloud computing. Therefore, a variety of security credentials have appeared in cloud computing. This section analyzes Google, Amazon, A variety of security credential-based identity authentication technologies used in cloud computing environments such as Microsoft have been compared.

**2. Federated identity authentication based on single sign-on**

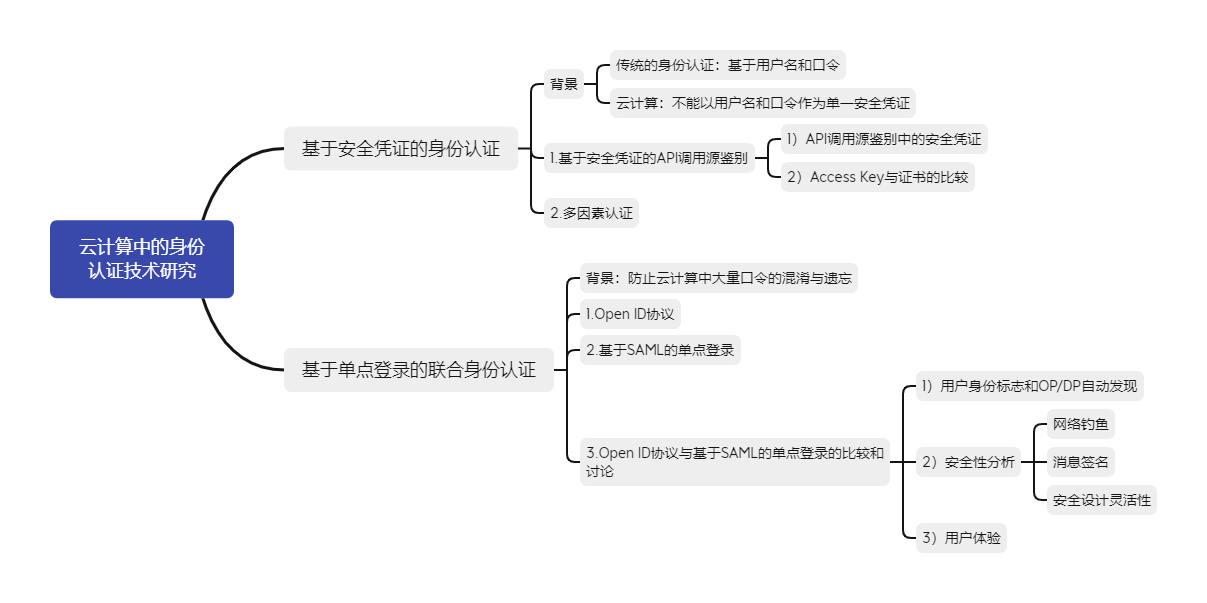
In addition to the identity authentication technology based on multiple security credentials introduced in the second section Technology, another rapidly developing identity authentication technology in cloud computing is based on single sign-on Record (SSO, Single Sign-On) federated identity authentication technology. With cloud computing With the development and popularization, users often use the cloud of many different cloud service providers.

The service has a large number of different passwords, which can easily cause confusion and forgotten passwords. The federated identity authentication technology is to solve this problem, users only need to Log in once when using a cloud service, you can access all mutually trusted cloud platforms Station without the need to repeatedly register and log in to multiple accounts. Single sign-on scheme is real Now an effective means of federated identity authentication, currently many cloud service providers support Joint authentication based on single sign-on. This section introduces two typical single sign-on Implementation scheme: O penID protocol and single sign-on based on SA M L, and two kinds of The plans were compared and discussed.

**3.Conclusion**

In this paper, the mainstream identity authentication and authorization technology in cloud computing is based on security Credential authentication and federated identity authentication based on single sign-on It is summarized and introduced. At the same time, we have also carried out the existing technology from multiple angles Compare and analyze, and put forward some improvement measures. This article is for most cloud services The mainstream identity authentication technology adopted by the provider has conducted a more comprehensive analysis and research However, it has not been adopted by some cloud service providers and has not been widely used. To discuss the identity authentication technology. In the next step, we will Based on the identity authentication with its own characteristics used in some cloud services Technology to carry out further analysis and research.

**五、评价分析（Evaluation and Analysis）**



This article on the current cloud. The widely used identity authentication technology based on multiple credential in computing is summarized. There are complex identity authentication scenarios in cloud computing, and A PI call source authentication is a typical authentication scenario. According to the different types of APIs, the security credentials used for authentication of API call sources are also different. This article focuses on the A PI call source authentication mechanism based on different security credentials. The development of cloud computing has promoted the development of federated identity authentication technology based on single sign-on. The development of federated identity authentication technology allows users to log in to multiple cloud services through a single account, which greatly simplifies user operations. Based on the single sign-on scheme, a federated identity authentication mechanism can be well implemented. This article introduces in detail the most widely used single sign-on scheme-OpenID protocol and SAML-based single sign-on scheme, and analyzes and compares them, and puts forward some suggestions for improvement.