Research on data access security agent technology in cloud computing security

Xian Ou
Department of Information and Communication, Officers college of PAP, China
ouxianer@126.com

Abstract. Cloud computing is a new application model, with multi-tenant, flexible, fast and easy to scale features, it can significantly reduce operating costs and improve operational efficiency. Cloud computing has received extensive attention from the business community and academia. With the continuous development of cloud computing technology, security and privacy issues have become the biggest obstacles to cloud computing applications. This paper first introduces the main problems faced by access control in the cloud environment, then researches and analyzes the cloud access security agent technology in terms of functional role and key technologies, and predicts the future challenges of the cloud access security agent technology based on the analysis of existing technologies.

1. Introduction
In the age of no internet, we store data content on computers, and when using that data we must access the computer and cannot directly access the content on another computer from another device or computer. The development of cloud computing shows significant advantages: data stored in the cloud is not afraid to be lost, it does not have to be backed up and can be restored at any point; software stored in the cloud can be automatically upgraded without downloading; Users can perform computing services at any time, anywhere, on any device, with unlimited space, unlimited speed. Previous studies have shown that users' data storage, processing, network transmission, etc. are all related to cloud computing systems, and modern users are outsourcing data processing and storage to cloud service providers, which means that data and its processing are out of the hands of data owners [1]. Preventing cloud service providers from illegally accessing data becomes a problem if critical or private information is lost or stolen, which is undoubtedly fatal to the user, so access control has always been an issue that only needs to be addressed in cloud computing.

2. Key issues for access control in cloud environments
In the traditional computer model, the software and hardware devices in the enterprise information system are deployed within the enterprise. Within the enterprise, devices such as computers and routers are used to create a network that can be controlled by the enterprise information system managers, which is the controlled information domain. [4]. In this model, all resources are under full enterprise control, so it is not difficult for the enterprise to use identity management and access control. An important technology in the creation of the cloud environment access control service platform is virtualization, which leads to the sharing of the same hardware resources between different users. Figure 1 shows the logical structure of the access control model in a cloud environment.
The cloud client side is where the user connects to the cloud interface and then sends the service request to the cloud via the browser, enabling cloud interaction and also enables registration and login.

The management system manages the user's identity, assigns user authentication rights after the user is registered and logged in, and manages cloud resources and services so that user requests can be forwarded within the service resources. The main purpose of the deployment tool is to enable dynamic deployment of resources in the cloud. Server clusters that want to expand the pool of physical server resources can be virtualized and managed with a management system that provides storage and computing power.

However, in a cloud computing environment, cloud users face new challenges such as lack of control over the permissions obtained for resources, lack of trust between users and cloud service providers, and virtualization technology leading to malicious resource grabbing among multiple tenants. Also, when an enterprise puts some or all of its business in the cloud, there is no controlled information domain, and the information system works in a larger domain. This leads to access control in enterprise cloud environments with access authorization issues, authentication issues and data security issues[2].

### 3. Cloud access security agent

The cloud access security agent (CASB), an emerging technology that is a system to help corporate enterprises implement security policies in the cloud, is designed to address security issues when users use cloud computing services and sits between cloud service providers and corporate enterprises that consume cloud services. CASB can be envisioned as a central data authentication and encryption hub for all cloud-based services and on-site systems in the enterprise, and can be accessed by all endpoints, including private smartphones and tablets. CASB does four main things: discover what cloud applications companies are using; protect data; defend against threats; and ensure compliance. It can implement customized security policies for different users' business systems and different cloud computing platforms to detect and prevent unauthorized behavior, thereby monitoring the security risks of cloud services and ensuring users' security when using cloud computing services, thereby promoting the development of cloud computing.

Cloud access security agents are actually complementary technologies to network agents and firewalls. By integrating with these solutions, cloud access security agents can leverage existing network architectures to gain visibility into cloud service usage. At the same time, cloud access security agents realize their own usage value through cloud-aware. We can approach the integration of cloud access security agents with network security solutions in three main ways: log collection, packet capture and agent tandem.

### 4. Key technical studies

Cloud access security agent does not have unified fixed functional requirements, and different enterprises have different security focus, although the form varies, but the main functions include virtual desktop protocol adaptation, visualization, data security, threat protection, etc.
4.1. Visualization
CASB lets business owners know if the cloud services that all employees insist on using in their networks are secure. CASB can be used to find and monitor traffic to and from cloud services in a way that gives users an intuitive view of how cloud computing resources are being used, it can tell security teams which employees are using cloud services and how they are accessing them, and it can document and present threats, vulnerabilities, risks, etc. in the current use of cloud computing services.

4.2. Compliance
As technology evolves, especially as CASB uses API rather than proxies to improve visibility into business on the cloud, they are able to view data transferred from one cloud to another and between on-premise infrastructure and clouds. In addition to giving security teams a better understanding of the organization's cloud infrastructure, this allows them to view the data stored in the cloud as well as being processed.

Many aspects of compliance depend on understanding where and how data is stored. In addition to external regulations, many organizations have internal rules for how certain types of data are stored and handled. CASB gives security teams a clear picture of the status of cloud-bound data so they can detect and correct employees who are storing or migrating data to avoid violating external regulations.

4.3. Threat protection
Traditionally, enterprise applications are deployed locally and information security is the responsibility of the enterprise itself. When an organization moves applications to the cloud, it places a certain amount of security responsibility on the cloud computing platform. However, cloud computing platforms tend to focus on information security through relevant compliance certifications and are not concerned with specific security threats to user-specific business data. With a large number of users and different business systems, it is also difficult for cloud computing platforms to help users solve individualized security issues[3].

One of the goals of the Cloud Access Security Agent is to address security threats that the cloud computing platform cannot help users address. Cloud Access Security Agent The vendor continuously updates threat intelligence and provides it to the cloud access security agent deployed by the user by creating a threat intelligence library. The Cloud Access Security Agent examines data coming in and out of the cloud computing platform, conducts surveillance reviews of access behaviors, and, through comparison with the threat intelligence base, detects threats in a timely manner and takes appropriate defensive measures.

4.4. Virtual desktop protocol adaptation
Desktop virtualization is one of the important ways to achieve cloud computing. Desktop virtualization virtualizes the end systems of computers to achieve security and flexibility for desktop use. End-users access their personal desktop systems via the Internet. Desktop virtualization relies on desktop virtualization protocols. At present, mainstream desktop virtualization vendors have their own desktop virtualization protocols, such as Huawei's HDP protocol, Microsoft's RDP protocol, Citrix's ICA protocol, VMware's PCoIP protocol. There are major differences in the desktop virtualization protocols of various vendors, protocol functions and implementation principles are also different, using desktop virtualization technology, the core data is stored in the cloud business database, computation and processing by the server, while the push to the user terminal is only virtual desktop, that is, picture information. Therefore, in order to prevent the leakage of important data through virtual desktops, a cloud access security agent must be able to parse the information contained in the image and determine whether the current user has the appropriate data access rights and whether important information has been illegally leaked[3].

Cloud Access Security Agent Deployment Location Issues. If the data is reviewed before it is protocol-transformed, there is no parsing of the virtual desktop protocol-transformed data but it is difficult to deploy inside the user's business system; if the cloud access security agent is deployed at
the external boundary of the business system, the virtual desktop protocol-transformed data needs to be parsed and reviewed. For the current mainstream desktop virtualization protocols, the Cloud Access Security Agent should support multiple virtual desktop protocols and adapt to different cloud computing service environments in order to have more leeway.

5. Future Challenges of CASB

Through our study of CASB technology, we have found that cloud access security agents offer many benefits. First, they build barriers to reduce risk and security threats by tracking the behavior of authorized users, insider threats and potential hackers. The system is also flexible; in addition to identifying potential threats, it also provides varying degrees of policy implementation.

Despite these benefits, cloud access security agents also present some challenges.

(1) To optimize their cloud security strategy, enterprises should integrate cloud access security agents with their existing security products. However, the integration process can be time consuming and difficult.

(2) Affecting application performance and user experience, users of cloud access security proxies handle traffic from private users, meaning employees may resist using applications that may expose personal traffic. The cloud access security agent must have policies and processes that apply to standards acceptable to the company and that are agreed upon by all employees.

(3) Cloud access security agents have to consider accommodating a variety of different end devices, as users want to log into cloud applications from an ever-growing number of open-ended products. This type of endpoint flexibility is particularly important in cloud access; in addition, cloud access security proxy tools should not inhibit flexibility. Otherwise, users will be denied the use of cloud applications to support other cloud access security agents.

6. Conclusion

Cloud access security agents protect cloud environments from threats and are tools used to listen and manage traffic between cloud applications and users. While it can help protect cloud environments, the tool can also impact users in a way that is not expected, potentially reducing productivity and leading to shadow IT. When evaluating cloud access security agents, businesses and IT leaders need to consider the impact on user privacy, on application availability, and on endpoint mobility. Therefore, it is not enough to explore the solution to the cloud computing security problem from the technical point of view, it requires the joint efforts of the information security academia, industry and relevant government departments.

Acknowledgments

First of all, I am thankful for my university, which has given me a comfortable atmosphere to study and research. Secondly, I would like to thank my colleagues who have given me some advice on academic research. Finally, I would like to express my gratitude to my parents who have helped me out and supported me without complaint.

References

[1] Feng Chaosheng, Qin Zhiguang, et al. Key technologies for access control in cloud computing environments[J]. Electronic Journal, 2015, 43(2):312-319(in Chinese).
[2] Zuo Danxia. Cloud security technology and implementation exploration[J]. Network and Information Engineering, 2016:117-118(in Chinese).
[3] Zhang Zhi, Jin Dapeng. Cloud access security agent technology research[J]. Communications Technology, 2017, 50(5):1016-1019(in Chinese).
[4] Gan Rong. Issues facing access control in cloud environments and cloud access control technologies[J]. Electronic Design Engineering, 2019,27 (2):85-88(in Chinese).