Cloud Access Security Broker (CASB): A pattern for secure access to cloud services

EDUARDO B. FERNANDEZ, Florida Atlantic University
NOBUKAZU YOSHIOKA, National Institute of Informatics
HIRONORI WASHIZAKI, Waseda University

Companies are using more and more cloud services, especially SaaS. These applications may handle sensitive data and the companies' IT departments need to manage the security of a potentially large number of applications. Although the service provider may have a strong security infrastructure, the consumer is responsible for the security of the data used in these applications (the provider does not understand the data semantics). A new type of system software has recently appeared that can organize this security management; this is the Cloud Access Security Broker (CASB). A CASB controls access to the resources available to application users and also protects the data from malware. We present a pattern for this type of system. CASBs are an important part of the cloud ecosystems.

Categories and Subject Descriptors: D.2.11 **[Software Engineering]** Software Architectures–Patterns; D.5.1 D.4.6 **[Security and Protection]** Authentication

General Terms: Design

Keywords: security patterns, cloud computing, cloud brokers, SaaS

1. INTRODUCTION

Cloud computing has brought a variety of services to potential consumers. Many companies typically access around 600 services, mostly of the SaaS type [Sky14]. Those companies also have internal resources and governing access to external and internal resources can be a complex logistic problem in that access to those services need to be controlled because they may provide access to highly sensitive enterprise data. Although the service provider (SP) may have a strong security infrastructure, it does not understand the semantics of the applications running on it and the consumer must control access to its sensitive information. A new type of system software has recently appeared that can organize the management of these applications; this is the Cloud Access Security Broker (CASB). According to [Mul14], there are already about 14 vendors of this type of product. A CASB becomes a key part of the IT governance structure of the institution. Access to the company resources may come from portable devices such as smartphones, tablets, and laptops, and there is also a need to grant some users temporary access to cloud applications [McV13]; all this variety can be conveniently handled by CASBs. A CASB is also an important part of cloud ecosystems. An ecosystem is the expansion of a software product line architecture to include systems outside the product which interact with the product [Bos09]. The CASB pattern provides network functions for a cloud reference architecture and is an important part of cloud ecosystems. An ecosystem is the expansion of a software product line architecture to include systems outside the product which interact with the product. Figure 1 shows a partial cloud ecosystem. The Cloud Security Reference Architecture (SRA) is the main pattern that defines the ecosystem [Fer15]. This can be derived from a Cloud RA by adding security patterns to control its identified threats. Cloud Web Application Firewalls [Bon13] and Security Group Firewalls [Fer14] provide filtering functions that can be provided as services through NFVs. The Cloud Compliant Reference Architecture applies patterns for regulations to the Cloud RA.

Authors' addresses: Eduardo B. Fernandez (corresponding author), Dept. of Computer and Electrical Eng. and Computer Science,Florida Atlantic University, 777 Glades Rd., Boca Raton, FL33431, USA; email: ed@cse.fau.edu; Nobukazu Yoshioka, GRACE Center, National Institute of Informatics, Tokyo, Japan, email: nobukazu@nii.ac.jp; Horonori Washizaki, Waseda University, Tokyo, Japan, email: washizaki@waseda.jp

We present here a pattern for a CASB. This pattern complements our work on cloud reference architectures by adding a security structure in the consumer side [Fer14]. Our audience includes system architects and system designers involved in cloud applications and architecture design.

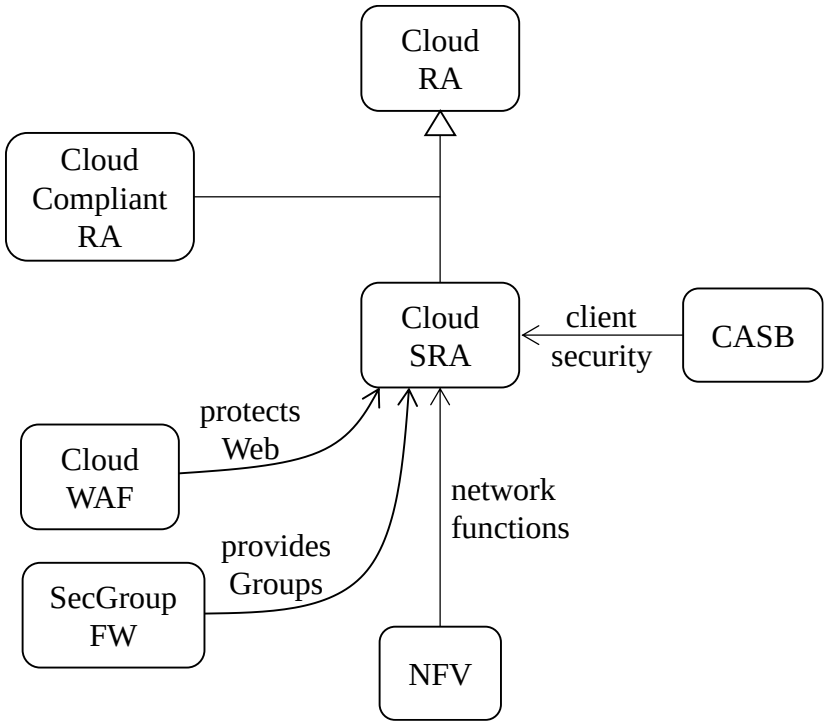

Fig. 1. A cloud ecosystem

2. CLOUD ACCESS SECURITY BROKER (CASB)

Intent

Cloud Access Security Brokers (CASBs) are security enforcement points between consumers and service providers that apply security controls to access cloud services, usually SaaS services. They may also control access to internal company resources. Security controls may include authentication (credentials and passwords), authorization policy enforcement, intrusion prevention, antimalware filters, security logging/auditing, and encryption.

Example

"Find Paradise" is a travel agency that provides a variety of services to its clients, including flight reservations, car rentals, and hotel reservations. They decided to use a travel software available from a cloud system as SaaS, which now handles all the functions previously handled by the company servers. However, lack of controls accessing their travel applications resulted in data leakage, their customers had their credit and other sensitive information exposed and the agency incurred in expenses and loss of reputation.

Context

Many institutions are using cloud services; most likely at the SaaS level, where they access applications provided by the cloud service providers (SPs) but where they store their own data. Consumers (the users of cloud services) within an institution, use services provided by (SPs). Each SP has a set of services or functions available to the consumers to access their applications. The applications may handle sensitive data and each institution may have its own policies

to let its consumers access the cloud services in a controlled way. A company may access services from several SPs. The consumers may use a variety of devices to access cloud services from public networks using unmanaged devices.

Problem

An institution needs to protect its information assets. If an institution decides to use cloud services, in particular SaaS applications, it needs to control access to those applications because they may handle sensitive information. The SP only provides general controls for its services, e.g., prevention of DoS or IDS; specifically, the SaaS provider takes responsibility for the application, the IaaS provider protects the creation and isolation of VMs (Virtual Machines). However, the SPs cannot understand the semantics of the applications; the institutions using the applications must define policies for their appropriate use and comply with regulations. Consumers need to consider new threats, unique to SaaS, in addition to the usual threats to Internet-based systems. New threats include data theft as well as data manipulation; malware may be delivered via data storage systems such as DropBox [Ada15]. *How can the institution perform this security control in a convenient and effective way?*

The solution to this problem is affected by the following forces:

Policy-based services--consumers should be able to define security policies to apply to the services they use in order to restrict the access of their employees and customers to cloud data.

Secure channel—the channel to access cloud services should be protected or messages could be intercepted producing data leakage.

Data encryption—the SP can provide data encryption but using its own key; consumers would like to encrypt their data using their own keys.

Compliance—depending on the type of application, consumers should be able to demonstrate compliance with specific regulations.

Discovery—users at the company should be able to find out what services they have available.

Transparency—security should be transparent to the application consumers.

Transparent security—the security services should be transparent to the consumers.

Malware detection—the cloud application may contain malware and consumers do not want to get it when they access a service. They should be alerted to possible intrusions.

Access unification—the application should not have to deal with a variety of credential types and protocols.

Heterogeneity—access to the cloud could be made from any type of device, including all types of mobile devices.

Logging/auditing—for security and compliance reasons we need to keep logs that can be later audited.

Identity—we need to precisely and uniquely identify our users to make them accountable for their actions.

Solution

Use an intermediary system, called a CASB, which provides security controls (authentication and authorization), can monitor the use of services by users, and can perform malware detection when users access cloud applications. Additionally, other services such as performance, identity, and search can be provided. Figure 2 shows the idea: The users of a company can only access applications, including internal applications, through the CASB. The CASB enforces

institution policies in any access as well as protecting against malware. In other words, the CASB is an enhanced Reference Monitor [Fer13].

Structure

Figure 3 shows the class diagram of the CASB. Consumers (users) request services through the Broker, which in turn gets them from one of the Service Providers. The Broker includes a set of security mechanisms such as a SecurityLogger/Auditor, an Authorizer, an Authenticator, an Encryptor, and maybe others. Consumers and CASBs can be mutually authenticated. The CASB enforces rights for the consumers when they try to access an application. InternalResources (applications) can also be controlled by the CASB. An Identity Federation provides identifiers across consumers and SPs.

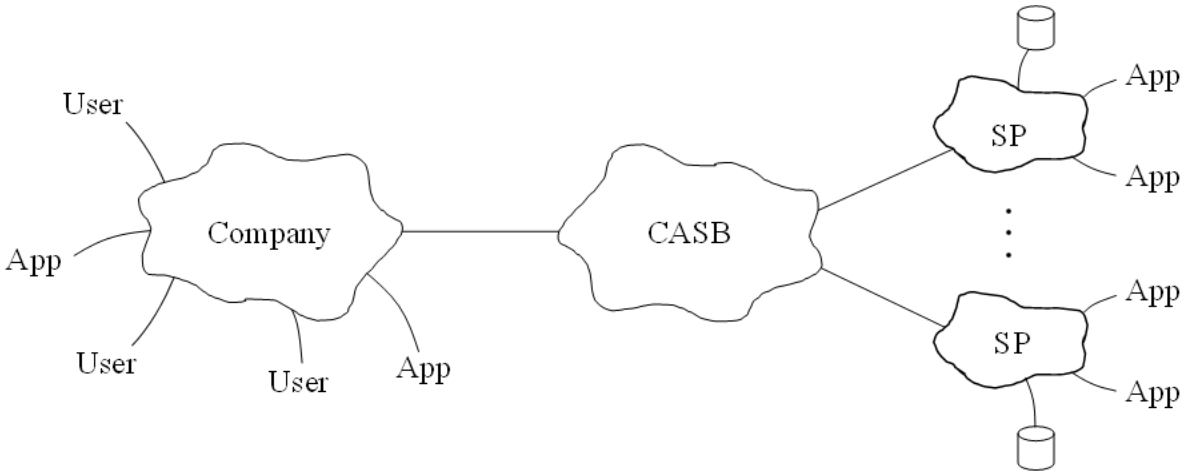

Fig. 2. Idea of the CASB

Dynamics

Use cases include search for an appropriate service, access application service, define security policies, and register a service [Mul14]. Figure 4 shows use case “Access an application service”.

Implementation

- We need to define policies to control what data can be accessed by the consumers from company-owned systems or from their own devices.
- Policies are typically stored in the system directory (Active Directory or LDAP).
- Personally-identifiable information should be separated and protected.
- CASBs are concrete versions of the abstract idea of reference monitor [Fer13]. According to the principle of full mediation [Sal75], every access to a service must be checked by the CASB.
- The location from where accesses are made should be identifiable because it can indicate illegal actions.
- Encrypted data should be propagated to the device where it is downloaded.
- Data in mobile devices should be able to be selectively deleted.
- It is useful to use data fingerprinting.
- The CASB should be configured using a Reverse Proxy architecture.

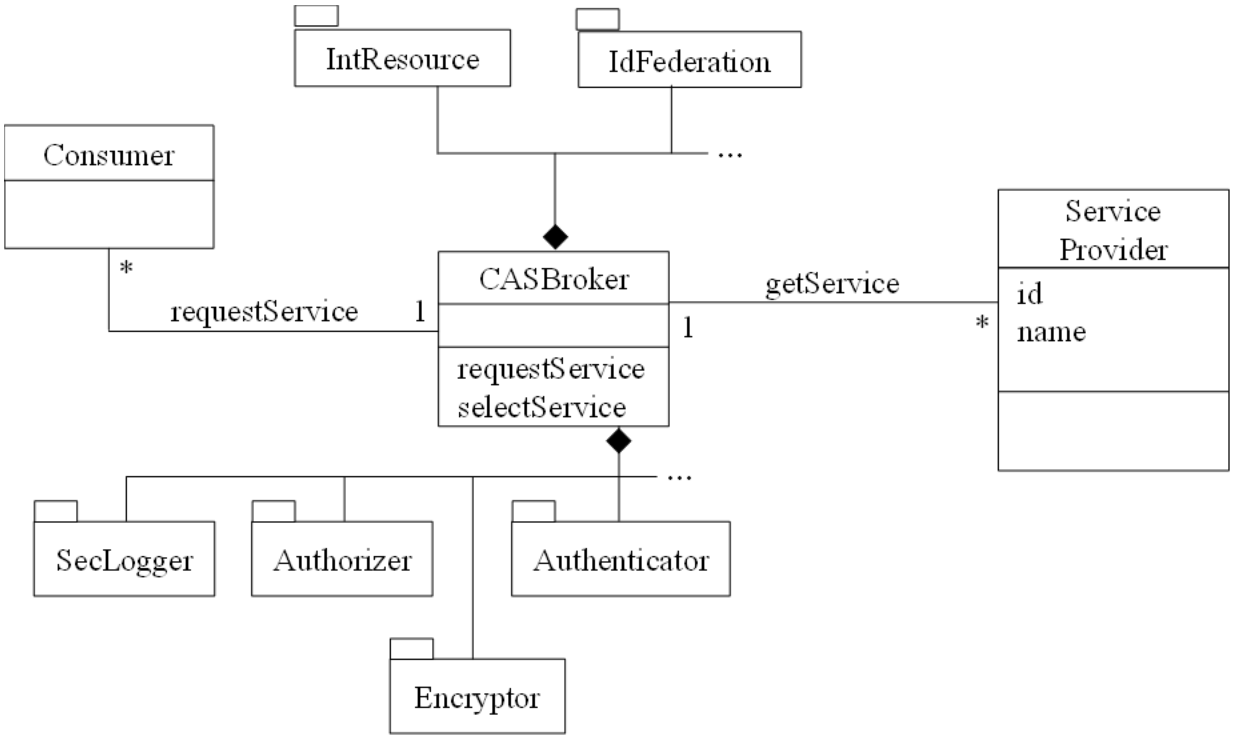

Fig. 3 Class diagram of the CASB pattern

Known uses

- Adallom [Ada15]—integrates with the authentication services in SaaS to let institutions monitor the activities of users in any location and any device. This product includes a behavior analysis component to assess the possible risk of specific transactions.
- Bitglass [Bit]—provides RBAC, encryption, session control, identity, and DRM.
- Cipher Cloud [Cip]-- protection controls include encryption, tokenization, monitoring, data loss prevention, and malware detection.
- Elastica Cloudsoc [Ela15]—Provides authentication, authorization, monitoring, and other services. It can interact with third-party APIs.
- Skyhigh Networks [Sky]—includes encryption, logging/auditing, access control, and anomaly detection (IDS). It also provides risk ratings of cloud services. Integrates authentication with standards such as SAML.

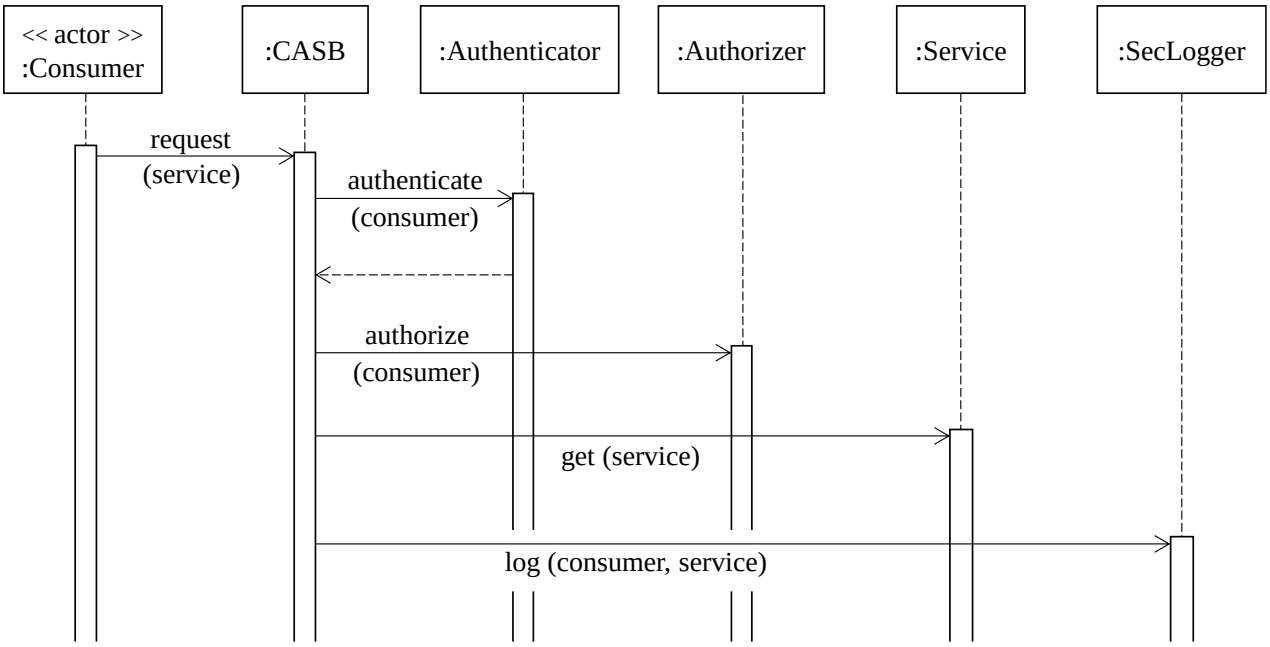

Figure 4. Use case "Access an application service"

Consequences

Advantages include:

Policy-based services--consumers can define security policies, e.g., RBAC, to apply to the services they use in order to restrict the access of their employees and customers to cloud data.

Secure channel—the channel to access cloud services can be encrypted.

Data encryption—CASBs can let consumers encrypt their data using their own keys.

Compliance—consumers can demonstrate compliance with specific regulations because CASBs normally include security loggers/auditors.

Discovery—users at the company are able to find out what services they have available through the CASB.

Transparency—security is transparent to the application consumers when they use the CASB, they would only know about the CASB if an attempted access is rejected.

Access unification—Consumers do not need to deal with a variety of credential types and protocols.

Heterogeneity—access to the cloud can be made from any type of device.

Malware detection—access to the cloud application through a CASB can guarantee that no malware will be found in the accessed service.

Logging/auditing—the CASB keeps logs for security and compliance reasons; these can be later audited.

Identity—the CASB can provide identification services.

Liabilities include:

Complexity due to using different types of credentials. It can be fixed by using some standard such as SAML for all the credentials.

If the consumers encrypt their data with their own keys, the SP cannot search that data and cannot apply its procedures to it.

The CASB may incur in possible privacy violations, but careful use of its security controls can improve users' privacy.

Related patterns

- Single access point [Sch06]—all the information must be checked by the CASB or security cannot be guaranteed.
- Authenticator [Fer13]—mutually authenticates consumers to CASBs and CASBs to SPs
- Authorizer [Fer13]—corresponds to the part of the CASB that applies access policies to the services
- Reference Monitor [Fer13]—corresponds to the part of the CASB that Intercepts service requests to check if they are authorized.
- Encryptor [Fer13]—used to protect the communication channels between participating units
- Multicloud Federation [Enc14]—in some cases the SPs form a federation and they need a CASB to let consumers find services [Enc14].
- Security Reference Architecture [Fer14]—defines the context for the CASB.
- Protection Reverse Proxy [Sch06]--protects web servers in conjunction with firewalls.
- Security Logger/Auditor [Fer13]—it can log the use of services by consumers. They are usually components of CSABs.
- Identity Federation [Fer13]--needed to apply authentication in any system.

CONCLUSIONS

This pattern describes how to secure a fundamental unit of a cloud ecosystem by letting consumers control access to the cloud services they use. Like all patterns, its validation will happen when designers use it in their systems.

ACKNOWLEDGEMENTS

We thank our shepherd Eduardo Guerra for his careful comments and suggestions that have improved this paper. The National Institute of Informatics of Japan paid the expenses for the first author to attend AsianPLoP.

REFERENCES

[Ada15] Adallom, "The case for a cloud access security broker", https://www.adallom.com/wp-content/uploads/2014/12/TheCaseForACASB.pdf

[Bit] Bitglass, "The definitive guide to cloud access security brokers", http://pages.bitglass.com/Cloud-Access-Security-Brokers_PDF.html?aliId=3891489

[Bon13] Isaura N. Bonilla, E. B. Fernandez, Maria M. Larrondo-Petrie, and Keiko Hashizume," A pattern for Whitelisting Firewalls", 20th Conf. on Pattern Languages of Programs (PLoP 2013)

[Bos09] J. Bosch, "From software product lines to software ecosystems", Procs. of the 13th Int. Software Product Line Conference (SPLC'09), 111-119.

[Cip] http://www.ciphercloud.com/2014/09/30/public-cloud-security-demands-cloud-access-security-broker-casb/

[Ela15] Elastica, http://cdn2.hubspot.net/hub/349272/file-1350266572-pdf/2014-07-eBook_Promo/Elastica-Whitepaper-RethinkingSecurityForSaaSCloudapps.pdf

[Enc14] Oscar Encina, E.B. Fernandez, and Raúl Monge, “Towards Secure Inter-Cloud Architectures”. Proceedings of Nordic pattern conference on Pattern Languages of Programs, Sagadi Manor, Estonia, April 2014.

[Fer13] E.B.Fernandez, “Security patterns in practice: Building secure architectures using software patterns”, Wiley Series on Software Design Patterns, 2013.

[Fer14] E. B. Fernandez, Nobukazu Yoshioka, and Hironori Washizaki, “Patterns for cloud firewalls”, Procs. of AsianPLoP (AsianPattern Languages of Programs) 2014, Tokyo, Japan, March 2014.

[Fer15] E.B.Fernandez, Raul Monge, and Keiko Hashizume, “Building a security reference architecture for cloud systems”, Requirements Engineering, 2015. DOI: 10.1007/s00766-014-0218-7

[McV13] Lori McVittie, “The mounting case for cloud access brokers”, Virtualization Journal, Feb. 8, 2013.

[Mul14] R. Mullins, “Cloud security brokers play a key role”, 07/11/2014 http://www.saasintheenterprise.com/author.asp?section_id=3154

[Sal75] J. Saltzer and M. Schroeder, The Protection of Information in Computer Systems.
Proceedings of the IEEE 63, 9 (September 1975), 1278-1308.

[Sch06] M. Schumacher, E.B.Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, Security Patterns: Integrating security and *systems engineering",* Wiley 2006. Wiley Series on Software Design Patterns.

[Sky14] Skyhigh Networks, “What is a cloud access security broker?”,2014
http://www.skyhighnetworks.com/cloud-university/what-is-cloud-access-security-broker/