International Journal of Research in Advent Technology, Special Issue, NCRCEST 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Enhancing Features Of Cloud Computing Using Cloud Access Security Brokers - To Avoid Data Breaches

Shabnam Kaur[1], Dr. Rajandra Gupta[2]
Research Scholar[1], Associate Professor[2],Rabindranath Tagore University, Bhopal[1,2]
Email: kmscollegedasuya@gmail.com[1] ,rajendragupta1@yahoo.com[2]

Abstract*:* Data breaches have gained widespread attention as businesses of all sizes become increasingly reliant on digital data, cloud computing, and workforce mobility. Cloud applications reduce costs and improve productivity. But it is equally important to monitor and protect data in a cloud environment. These are the questions that arise how to deal with lost visibility, unmanaged devices, and careless users. This paper explains how cloud access security brokers (CASBs) extend security to cloud applications, awareness for data breaches, providing visibility, threat protection, access control, and compliance. The key characteristics and benefits of cloud access security brokers (CASBs) are visibility, threat protection, access control and compliance are key components of this paper to extend data loss prevention (DLP). There is need to create the architecture of CABs having feature to deal with all types of Data Breaches. The result of the study provided a secure architecture to fulfill the security needs and tracks the complex connections between enterprise infrastructure and its cloud service provider.

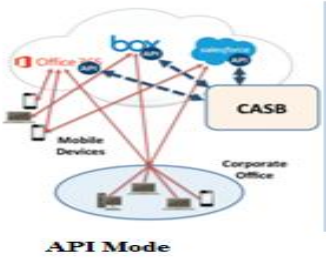
Key Words: Data Breaches, Cloud Access Security Brokers (CASBs), Data Loss Prevention (DLP)

1. INTRODUCTION

Cloud Access Security Broker(CASB) act as a gatekeeper, allowing the organizations to extend the reach of their security policies beyond their own infrastructure. Cloud access security brokers not only monitor access to cloud applications, they also provide a central point for controlling access, preventing sensitive information from being downloaded to insecure devices, and enforcing encryption. In effect, a CASB can extend data loss prevention (DLP), network access control (NAC), and other security technologies to cloud environments. They can also ensure enforcement of data sharing and compliance policies. CASBs differ in how many cloud applications they can access via APIs. However, lesser-known SaaS applications and internally developed applications can be submitted to the CASB vendor for integration with their solution.

1.1 Deployment Mode Options for CASBs

There are two deployment mode options for CASBs to monitor sanctioned applications: API mode and proxy mode (Figure1)



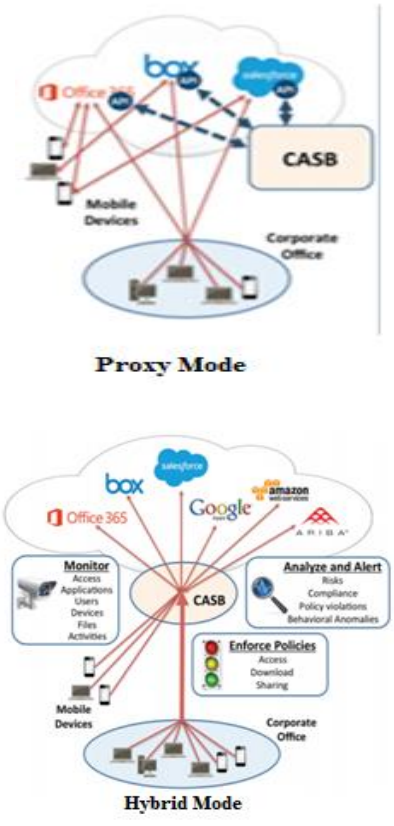


Figure 1 : CASBs can be deployed in API Mode , Proxy Mode and Hybrid Mode

1.1.1 API Mode A CASB deployed in API mode, users communicate directly with cloud applications, and the CASB obtains data from the applications through their APIs. This approach provides very detailed visibility into

data at rest and user activities, including logins and logouts, file uploads and downloads, information sharing, and administrative actions. CASBs deployed in API mode can also perform administrative tasks and enforce governance policies. For example, if a user violates policies by publicly sharing files containing sensitive information, administrators can use the CASB to change the access permissions on the files, or to take file ownership away from the offending user. A major advantage of API mode is speed: a CASB can be implemented literally in minutes because no changes to networks, endpoint devices, or applications are needed.

1.1.2Proxy Mode A CASB deployed in proxy mode is "inline"; network traffic between users and cloud applications flows through the CASB proxy. This is achieved in one of two ways:

1. In a forward proxy, traffic is routed to the CASB proxy by network devices (for office users) or by agents on each endpoint (for external users).
2. In a reverse proxy, cloud applications are configured to guide traffic through the CASB proxy.

Proxy Mode also gives the CASB visibility into data in motion and allows it to enforce policies in real time. For example, the CASB can ensure that files being uploaded are encrypted, and can block the download of sensitive files to noncompliant devices. It can also generate alerts in real time, allowing security teams to react immediately to security incidents, policy violations, and anomalous behaviors. However, proxy mode takes longer to implement. To route traffic to the CASB proxy, changes need to be made to network devices and endpoints (for forward proxy), or to applications (for reverse proxy). Also, some implementations of forward proxies require the installation of software agents on endpoint devices, which may be impossible with unmanaged devices. Further, some reverse proxies can break application functionality.

1.1.3 Hybrid Mode

Some CASBs offer a hybrid mode that combines API mode and proxy mode. This allows the CASB to support a wide range of use cases with visibility, policy enforcement, and ways to deal with unmanaged devices.

2. PILLARS OF CASBs

2.1 Visibility

CASBs can give perceivability into client practices and exercises over all cloud applications. Normally, perceivability comes as a total review log with more elevated amount investigation, reports, and alarms on that information. Examination and reports can assist you with observing patterns and bits of knowledge into deviations from typical standards of conduct. Alarms can keep you advised of potential security and consistence issues, for example, wrong information get to, client account bargain, and so on. Since CASBs middle of the road the majority of your cloud applications, they can give perceivability that traverses your whole cloud arrangement.

2.2 Identity

Identify sensitive data in the cloud and enforce DLP policies to meet data residency and compliance requirements. Identity is a key test for some endeavors that have moved to cloud applications. Much of the time, enterprises have made isolated and unmistakable records for new cloud applications as they have included them. This causes colossal issues with secret word the executives, client account refreshes, worker end, and so on. A CASB should assist you with ensuring that all cloud applications influence a solitary personality store, either by confirming clients straightforwardly against your corporate catalog, or through an outsider cloud character supplier. This wipes out repetitive records and enables you to all the more viably implement secret word arrangements. Some CASBs can go about as a cloud character supplier, wiping out the need to purchase a third party solution.

2.3 Access Control

Enforce data-centric security such as encryption, tokenization, access control, and information rights management. Access Control answers the question of who is allowed to access a particular cloud app, and under what conditions and context. A CASB should enable you to define policies by applications, or even by functionality within an application. These policies should be based on:

- **Group or role in the organization:** Typically as defined in Active Directory. For example, Executives and members of the Finance team might have access to this quarter's financial results but nobody else should be able to access that data.
- **Device type or operating system:** Many organizations have policies on what can be accessed on a corporate managed Windows Laptop versus a personally owned mobile device, as an example.
- **Geography:** Physical location of a user may indicate suspicious or rogue behavior for some organizations, so they want to limit access to sensitive data from certain regions or countries

3. DATA PROTECTION

Detect and respond to negligent or malicious insider threats, privileged user threats, and compromised accounts. At access, CASBs are in charge of recognizing and ordering delicate data, and after that enabling the client to make strategies that figure out what ought to be finished with that data. These capacities are like Data Leakage Prevention abilities normally found within a corporate premise arrange or on oversaw endpoint gadgets.

The first step is to identify corporate data. All CASBs should include an ability to define templates or policies that classify corporate data into different risk or sensitivity levels. For example, an organization that handles personally identifiable information (PII) for its customers must be able to identify all files that contain PII, and then take action to protect it from leaking outside of the organization. Policy actions range from lightweight visibility mechanisms to outright blocking. A lightweight

CASB action might be to allow data to be downloaded, but either encrypt or track . More aggressive actions would include redacting sensitive data from a particular transaction, or blocking a file from download altogether. Every organization must make judgments and create policies around what type of actions to take based on applications, users/groups, and data.

4. RECOMMENDATIONS FOR SELECTING THE RIGHT CLOUD ACCESS SECURITY BROKER

When organizations migrate to the cloud, protecting data becomes more essential than ever. Adopting the right cloud access security broker is an absolute must for any organization that wants to ensure complete cyber security in this new environment. Cloud access security brokers are a relatively new technology and products of different vendors differ widely in capabilities.

4.1 Size of the Applications

Every cloud application is different, so some work is required to fully integrate a CASB with each new one. Choosing a CASB that covers both an API method of deployment and multiple proxy methods of deployment is best for cloud. In particular RESTful (Representational State Transfer) APIs allow client/server based architecture to be used to interact with infrastructure in a programmatic way. The six guiding principles to RESTful programming are Client/server based, Stateless, Cacheable, Uniform interface, Layered system and Code on demand.

4.2 Required Security Level

A CASB leverages proxies and APIs to protect data in the cloud and at access. Proxies enable real-time, inline security while API integration provides control over backend functions like external sharing. Most organizations require a hybrid CASB that provides both proxy-based and API-based protections for comprehensive cloud data protection. This Allows organizations to protect against leaking sensitive data such as credit card numbers and other sensitive data.

4.3 Heuristics for Threat Protection

One of the highest priorities for security teams today is identifying advanced targeted threats or breaches before they can damage the enterprise. CASBs contribute to this effort by detecting anomalous behaviors and clues about cybercriminals probing and manipulating cloud applications. CASB applied have heuristics engine and alerting capabilities.

5. CLOUD ARCITECTURE VERSUS CLOUD INFRASTRUCTURE WITH CASB

Security issues	Traditional Cloud Architecture	Infrastructure having CABs	Reviews
Challenges in Confidentiality, Integrity & Availability	✓	×	P.Ravi Kumar(2018),P.Herbet Raj (2018) P.Jeliciana(2018)
Network Infrastructure Complications	×	✓	Dan Gonzales(2017), Dulani Woods (2017)
Privacy Leakage	✓	×	Nabeel Khan (2016), Adil Al-Yasiri (2016)
Data Loss	✓	×	Naresh Vurukonda(2016), B.Thirumala Rao(2016)
Infrastructure benefit lost	×	✓	Tulin Atmaca (2016),Thomas Begin ; Alexandre Brandwajn(2016)

5.1 Directories and SSO solutions

Most CASBs integrate with enterprise directories, single sign on (SSO) products, and other identity and access management (IAM) solutions. These integrations give the CASB access to additional information about users, such as their roles, departments, and business units.

SSO offers maximum security when moving to the cloud, the highest convenience to all parties, the highest reliability as browser and web applications go through revisions and generally have the lowest total cost of ownership. One more aspect of SSO is that authentication is driven by standards-based token exchange while the user directories remain in place within the centrally administered domain as opposed to synchronized externally. Standards such as SAML (Security Assertion Markup Language), OpenID Connect and OAuth have allowed for this new class of SSO to emerge for the cloud generation. Standards are important because they provide a framework that promotes consistent authentication of identity by government agencies to ensure security.

5.2 Data Loss Prevention

Cloud DLP features allow a CASB to detect sensitive information in files and prevent those files from being downloaded to unmanaged devices, or from being downloaded at all. Some CASBs integrate with DLP products to leverage existing DLP policies and file classifications, allowing a single set of DLP policies to be enforced across cloud and on-premises datacenters.

5.3 Cloud NAC

A CASB can work with third-party cloud network access control (NAC) solutions. Endpoints that are unmanaged or non-compliant with corporate standards can be blocked from accessing cloud applications, or can be given restricted access and limited ability to download or share files.

5.4 Sandboxing

A CASB can work with a sandboxing product to test files in motion and files residing in cloud applications for malware.

5.5 Encryption and IRM

Integrating a CASB with encryption and information rights management (IRM) solutions can ensure that:

- Files uploaded to cloud applications are encrypted
- Files downloaded to unmanaged and other untrusted endpoints are encrypted
- Sensitive content cannot be printed, exported, copied, or retained for long on endpoints
- Experts debate the relative merits of encrypting all data, or encrypting data at the field level or file level. For CASBs, file level encryption tends to be the best option. Encrypting and decrypting all data creates excessive processing overhead. Encrypting data at the field level often breaks application functionality. For example, using a third-party solution to encrypt Salesforce fields can interfere with searching, as well as disrupting integration with other applications such as Marketo.

5.6 SIEM

All alerts generated by a CASB, together with related information (the context for the alert), can be pushed to security information and event management (SIEM) solutions. That allows the security operations center (SOC) and incident response (IR) teams to see CASB-created alerts immediately, correlate them with on-premises activities, prioritize them alongside other alerts, and respond to them using established workflows. It also gives them instant access to the contextual information collected by the CASB.

6. ENHANCING SECURITY WITH CASBs

A simulation tool is implemented for enhancing security in cloud architecture with CASBs. We have to store and retrieve files from the cloud. Steps performed are :

1. Firstly, text message or a file is sent to the cloud server by the user. Text file is divided into several shares.
2. An image is also selected or given by the user to generate a key for encryption of different shares. So, RSA Key is generated from the image for encryption of the shares.
3. All parts(shares) of the file are then encrypted using the key. Cloud Access Broker(CAB) has information regarding servers in the cloud, their load balancing etc. Cloud Access Broker is like a cloud monitor, gatekeeper or a bridge between cloud and users.
4. Encrypted shares are then stored on servers whose details are stored to the Cloud Access Brokers. CABs access its database and give the information regarding the servers available in the Cloud. It contains IP Addresses of the servers. CloudSim library is used to create Virtual Cloud. After getting the IP Addresses of the servers, file is divided into equal shares. Information related to the encrypted share, their storage system IP address, key used in storage of shares are also stored in the Cloud Monitor.
5. Shares are decrypted using the key generated from the same image that was used to store the file to the cloud server. After decryption, shares are combined to get the input file. If the image used for encryption matches with the image used for decryption then only the data can be retrieved. All the details are maintained by CABs

For the simulation of experiment in CloudSim, certain parameters of Cloud have been set. These parameters are:

1) One user – There is only one user in this experiment who sends one file to the Cloud for data storage in its servers.

2) One Datacenter Broker – In this experiment, only one datacenter broker is included.

3) One Datacenter – Generally, there are many datacenters available with Cloud service provider and datacenter broker chooses one of these datacenters depending on the QOS requirements of the user. However, in this experiment, only one datacenter is included and it is assumed that this datacenter meets the QOS requirements of client's application.

The shares are saved on the servers of the cloud. The Cloud Access Broker manage the IP addresses of the servers

Table:1 Server details stored by CASBs

Servers Information	Description
Server_ID	Unique Server ID
Server_IP	Server IP Address

Information related to the storage details of the data are stored in Storage table in Cloud monitor.

Table:2 Storage Table in Cloud Access Broker

Information Stored	Description
Share_Name	Share_Name
Server_IP	Server IP Address
Key_value	Key used for encyption
Filename	Filename
FileNo	Sequence of share

Data is stored in the form of decrypted files in the server

7 TEST RESULTS

Table: 3 CASB Functionality Areas

Functionality	Features
Visibility	Provide audit level logging, alerts and reports, information regarding stolen credentials converts "Visibility" to "Trustability"
Compliance	Filling the gaps made by SaaS Vendors Encryption of data, identifying the cloud usage and risks in data storage
Data Security	Provide Data-Centric Security Policies
Data Breaches Protection	Provide protection from Data breaches, Prevent unwanted users from accessing cloud services

For the tests results, certain checks have been made like the size of data stored, visibility, data security and breach protection in the Cloud systems with CABS. The result from the simulation confirms that objectives have been achieved by the algorithm discussed in above section .

7.1 Recovery Of Data Even If Some Number Of Servers Are Damaged

The servers attacked by hacker can vary. It can be one server or more than one server. Different attacks have been generated to verify whether first objective of this research "Recovery of data even if some (within a limit) number of servers are damaged" has been achieved or not. As studied earlier, at least, k servers are required to reconstruct the file from its shares, two tests have been performed

For instance, we have taken sample.txt file having size of 815 bytes. We have divided the files into the shares of 200 characters each. So we get 5 shares. These shares are then encrypted using the keys. For retrieval of the same sample.txt file from the servers, all the shares are concatenated after decryption. The file retrieved have the size 815 bytes. For prevention with the breaches image file(for key for encryption of the data) is used as a signature. This fills the gaps made by SaaS Vendors Encryption of data, identifying the cloud usage and risks in data storage

7.2 Results Concluded From Different Algorithms

Table: 4 Comparison of the proposed algorithm with few talked algorithm

Parameters / Algorithms	Recovery of data	Integrity of data	Confidentiality of data
Shamir's Algorithm [7]	✗	✗	✓
Distributed Fingerprints and Secure Information Dispersal [8]	✓	✓	✓
A Tree Based Recursive Information Hiding Scheme [9]	✗	✓	✓
PROPOSED ALGORITHM	✓	✓	✓

According above results , In Shamir's Algorithm the data recovered is not as per saved on the server, confidentiality is maintained. Using this algorithm the integrity is violated. , In Tree Based Recursive Information Hiding Scheme the data recovered is not as saved on the server, confidentiality and integrity is maintained. In the proposed algorithm, data recovered is same as saved on the server and Integrity and confidentiality is maintained. It is important to maintain confidentiality, integrity and recovery of complete data.

8. CONCLUSION

Security is considered as a primary component in this study that should be tracked between enterprise infrastructure and cloud service providers. It is identified with access control and authorization. This paper emphasized on the privileges, size of the data stored in cloud by the enterprise, secure data storage and its retrieval.

Cloud Access Security Brokers (CASB) play a central role in discovering security issues within a SaaS cloud service model as it logs, audits, provides access control, and oftentimes includes encryption capabilities. This paper also introduced an experiment to evaluate the performance of CASBs for storing data on cloud servers.

REFFERENCES

[1] Chuanyi Liu , Guofeng Wang , Peiyi Han , Hezhong Pan ,Binxing Fang, "A Cloud Access Security Broker Based Approach For Encrypted Data Search And Sharing", IEEE Xplore,2017

[2] Eduardo B. Fernandez, Nobuka ZU Yoshioka, Hironori Washizaki , "Cloud Access Security Broker (CASB): A Pattern For Secure Access To Cloud Services", 4th Asian Conference on Pattern Languages of Programs (Asianplop 2015)

[3] Guofeng Wang , Chuanyi Liu , Yingfei Dong , Hezhong Pan , Peiyi Han , Binxing Fang, "Safebox: A Scheme For Searching And Sharing Encrypted Data In Cloud Applications", 2017 International Conference On Security, Pattern Analysis, And Cybernetics, IEEE

[4] Opeyemi Osanaiye, Shuo Chen , Zheng Yan, "From Cloud To Fog Computing: A Review And A Conceptual Live Vm Migration Framework", IEEE, April 12, 2017

[5] Fog Computing And Internet of Things: Extend The Cloud to Where The Things Are, Accessed On Apr. 18, 2017. [Online]. http://Www.Cisco.Com/ C/Dam/En_Us/Solutions/Trends/Iot/Docs/Computing-Overview.Pdf/

[6] Nareshvurukonda, B.Thirumala Rao, "A Study On Data Storage Security Issues In Cloud Computing",2nd international conference on intelligent computing", Communication & Convergence (ICCC-2016)

[7] Vivek Kumar Prasad, Viraj M Mavawala,"Enhancement in Fiat Shamir Cryptography Algorithm", International Journal of Innovations & Advancement in Computer Science, September 2015.

[8] Preeti Kumari, Parmeet Kaur,"A survey of fault tolerance in cloud computing", Journal of King

Saud University - Computer and Information Sciences,October 2018

[9] Nabeel khan a, Adil Al-Yasiri,"Identifying Cloud Security Threats To Strengthen Cloud Computing Adoption Framework" The 2 Nd International Workshop On Internet Of Thing: Networking Applications And Technologies (IOTNAT- 2016)

[10] Tulin Atmaca , Thomas Begin , Alexandre Brandwajn ,Hind Castel-Taleb, "Performance Evaluation Of Cloud Computing Centers With General Arrivals And Service" IEEE Xplore Digital Library 2016

[11] Shichao Guan, "A Multi-Layered Scheme For Distributed Simulations On The Cloud Environment", IEEE XPLORE,2016

[12] Dan Gonzales, Jeremy M. Kaplan, Evan Saltzman, Zev Winkelman, Dulani Woods, " Cloud-Trust—A Security Assessment Model For Infrastructure As A Service (Iaas) Clouds", IEEE Transactions On Cloud Computing (Volume: 5 , Issue: 3 , July-Sept. 1 2017)

[13] Kwang Mong Sim ,"Agent-Based Approaches For Intelligent Intercloud Resource Allocation", IEEE Transactions on Cloud Computing ,2018

[14] Blesson Varghese , Massimo Villari , Omer Rana , Philip James , Tejal Shah , Maria Fazio , Rajiv Ranjan, " Realizing Edge Marketplaces: Challenges And Opportunities" Published in: Ieee Cloud Computing (Volume: 5 , Issue: 6 , Nov./Dec. 2018)

[15] P.Ravi Kumar, P.Herbet Raj, P.jeliciana, "Exploring Data Security Issues And Solutions In Cloud Computing", 6th international conference on smart computing and communications, ICSCC 2018.

[16] B. Hari Krishna, Dr.S. Kiran, G. Murali, "Security Issues In Service Model Of Cloud Computing Environment", International Conference on Computational Science,2016