APT GUIDELINES

FOR FRAMEWORK OF CLOUD ACCESS SECURITY BROKER FOR CLOUD SERVICE SECURITY

Edition: April 2023

The 35th APT Standardization Program Forum (ASTAP-35)
17 – 20 April 2023
Bangkok, Thailand

(Source: ASTAP-35/OUT-12)

No. APT/ASTAP/REPT-54

APT Guidelines for
FRAMEWORK OF CLOUD ACCESS SECURITY BROKER
FOR CLOUD SERVICE SECURITY

1. Introduction

CASB is a system that provides separate security features for SaaS applications. It serves as a platform to meet security demands from each customer effectively without public cloud service providers' burden to implement more complicated security features to meet the exact same security demands.[2]

The main components for the 4-tier CASB are a secure agent, a CASB proxy, a CASB inline gateway, and a CASB secure API. They are positioned between devices of cloud service users and cloud service servers. Therefore, if they independently operate security control without any prearranged interaction, possible duplicates of security control undermine the overall quality of cloud service. Furthermore, it would raise many problems, such as inconsistency or desynchronizing of security policy applied to a company.

For efficient CASB service, we need methods to provide stable service and to prevent overload of a specific CASB by considering the processing performance of CASB for each tier and distributing cloud service requests by CASB.

Furthermore, since each CASB component has different purposes and intents, a client of a cloud service user must pass and be checked with all CASBs provided when it accesses a cloud server. We must especially consider the way not to bypass CASB because smartphones outside in BYOD(Bring Your Own Device) environment can access to cloud server directly.

This document describes a protocol to minimize duplicated actions of security control, to improve the availability of security control, to synchronize the security policy of each CASB, and to prevent cloud service users from accessing the cloud server by bypassing CASB in 4-tier CASB environment consisting of a secure agent, CASB proxy, CASB inline gateway, and CASB secure API. Furthermore, including this, this document shows the simulation and performance evaluation results for 4-tier CASB.

Finally, this document describes the concept of SASE as one of the important fields where CASB is used, and explains the relationship between CASB used in SASE and our proposed 4-tier CASB.

2. Scope

This document is to provide a framework of 4-tier CASB with following;

- Access Control Protocol for Cloud Service Security in 4-tier CASB
- Security control process for efficient cloud service security in 4-tier CASB environments
- Secure communication protocols between CASBs in 4-tier CASB settings
- Methods to manage security control for CASB and non-CASB secure devices in BYOD(Bring Your Own Device) environments
- Simulation and performance evaluation of the framework
- Application of CASB and the relationship between CASB of the applied field and 4-tier CASB

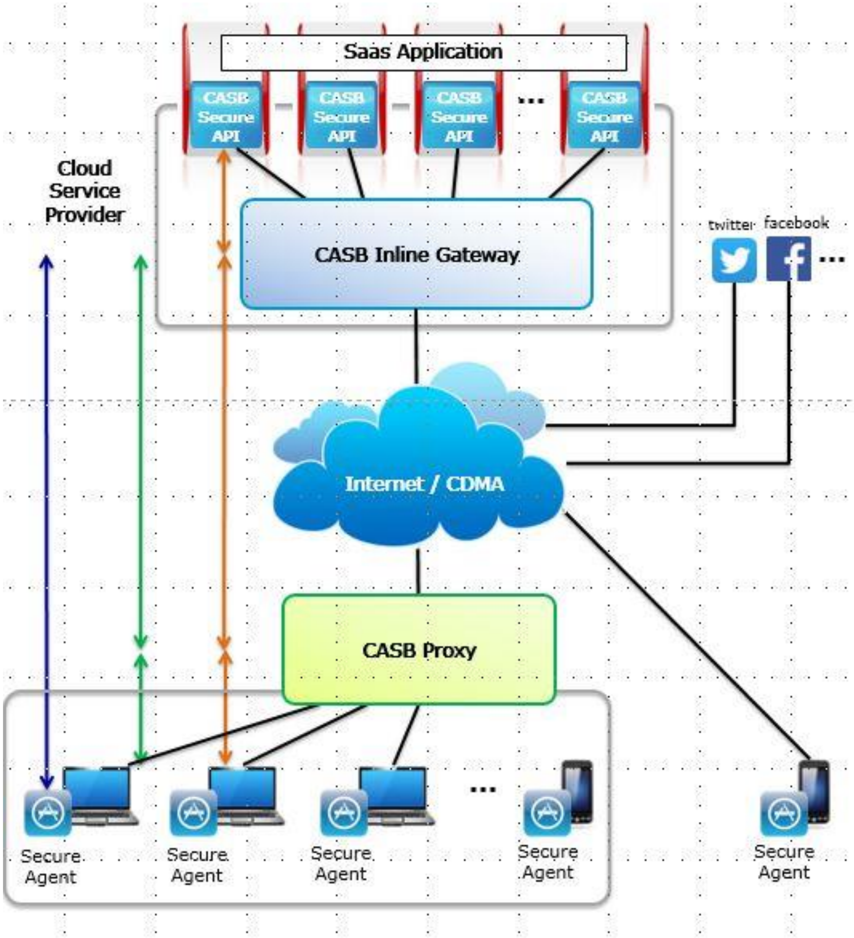
3. Terms and definitions

CASB: on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed.

SaaS(Software as a Service): software that is owned, delivered and managed remotely by one or more providers.

Public Cloud Computing: a style of computing where scalable and elastic IT-enabled capabilities are provided as a service to external customers using Internet technologies

4. Structure of 4-tier Cloud Access Security Broker



To guarantee two key requirements of CASBs, which are security of SaaS applications, and security of SaaS users, the structure needs CASB inline gateways, CASB proxies, and CASB secure APIs. Secure agents are needed to support such a structure from the client side. Thus the structure of CASBs should be formed with 4-tier of CASB secure API, CASB inline gateway, CASB proxy, and secure agent as in the figure above.

- CASB Secure API

Generally, the cloud service provider supplies service users with a huge number of SaaS applications. Because service traffic varies depending on usage frequency and usage pattern of users and consumption for each login, security controls by the CASB gateway alone may cause availability issues of SaaS service. So the provider of SaaS applications is required to supply SaaS service of his applications to users without those availability issues anytime and anywhere.

CASB Secure API satisfies such a requirement and exists inside SaaS applications as a library. Applying CASB secure API is completed when the development company of SaaS applications finishes implementing integration with the library authorized by the cloud service provider.

- CASB Inline Gateway

Generally, the public cloud service provider supplies services using SaaS applications from various vendors. The credibility of the public cloud service depends on whether users are accurately charged based on how much they have used the service. Furthermore, exact billing depends on whether to accurately measure how much each user has used certain SaaS applications, and the biggest obstacle to exact billing is usage of SaaS applications by unauthorized users or identity thieves.

CASB inline gateways control security at the gateway of the SaaS system as an appliance. While SaaS service is usually provided in encrypted data as in SSL, CASB inline gateways operate inside the system, so they do not concern with encrypted data.

- CASB Proxy

As the number of SaaS applications increases recently, the leakage of inside information through usage of not only authorized SaaS applications by company or agency but also unauthorized ones has become serious. It prompts effective control over all SaaS applications used by members of a company or an agency, and the CASB proxy fills the need. The CASB proxy is placed inside a company or an agency as a common proxy and performs security controls on all devices.

CASB registers SaaS applications authorized by company or agency. It performs security controls based on defined rules or defers them to the CASB inline gateway. Depending on security policies, it performs various security controls on unauthorized SaaS applications.

CASB proxy operates to a client like a server and to a server like a client. It can perform security controls in encrypted data of SaaS service.

- Secure Agent

Secure agents are basic client programs to manage all functions of CASB effectively. Typically, it supports settings of the CASB proxy, processes load balance of CASBs based on service type, runs encryption functionality like SSL provided by SaaS applications, handles its own encryption and decryption, and so on. For mobile devices, it provides VPN to prevent security bypass and to force the devices to access CASB.

5. Access Control Protocol

Since cloud service is provided via HTTP, CASB may choose to request further actions of security control by adding information of its security control in the HTTP header.[1] Once CASB inline gateway and CASB proxy execute their security control, it accordingly adds the following metadata as the request message in the table below to outbound information.

Field name	Description	Example
CASB-agentID	User ID authenticated through the secure agent	CASB-agentID: ask@abc.com
CASB-agentIP	IP address from the secure agent when the device of the agent connects to CASB	CASB-agentIP: 10.8.0.3
CASB-SCAN	Whether CASB has executed an action of security control (yes/no)	CASB-SCAN:yes

When such a protocol is applied, CASB inline gateway and CASB proxy parse the HTTP header before executing their security control. If the value of CASB-SCAN is yes, then CASB determines whether further actions of security control are necessary.

And when CASB secure API executes its security control, it accordingly adds the following metadata as the reply message in the table below to outbound information.

Field name	Description	Example
CASB-API-domain	Server domain applying API	CASB-API-domain: www.abc.co.kr
CASB-agentID	User ID authenticated through the secure agent	CASB-agentID: ask@abc.com
CASB-agentIP	IP address from the secure agent when the device of the agent connects to CASB	CASB-agentIP: 10.8.0.3
CASB-API-SCAN	Whether CASB secure API has executed an action of security control (yes/no)	CASB-API-SCAN: yes

When such a protocol is applied, CASB inline gateway and CASB proxy parse the HTTP header before executing their security control. If the value of CASB-API-SCAN is yes, then CASB inline gateway and CASB proxy will skip the security control for the application.

Furthermore, we need method for load balance because the overload of specific CASB could occur if the protocol only to prevent the overlapping access control is used. CASB can share system availability information between 4-tier CASBs by adding CASB service availability information to the header of this protocol.

The CASB system availability meta information added to these HTTP headers enables the CASB to perform or bypass security control for a cloud service request based on the availability of each CASB system.

In particular, using the CASB availability information added to the HTTP header, the secure agent can designate the CASB to perform security control for a cloud service request in the 4-tier environment.

Field name	Description	Value	Example
CASB-Type	CASB information : Inline Gateway CASB, Proxy CASB or API CASB	Inline Gateway CASB, Proxy CASB, API CASB	CASB-type: Proxy CASB
CASB-Capacity	CASB service performance level	High, Mid, Low	CASB-Capacity: High
CASB-Act	CASB security control action status	Yes, No	CASB-Act: Yes
CASB-svTarget	Policy URL information of target CASB	Inline Gateway CASB, Proxy CASB, API CASB	CASB-policyCallbackURL: https://www.abc.com/policy

In a 4-tier CASB environment, the four-layer CASB system consists of secure agent, proxy CASB, inline gateway CASB, and CASB secure API, and HTTP requests of the user's cloud service are transmitted to each CASB system through secure agent installed in user PC.

Through the information included in the received HTTP header, the CASB of each layer can check the availability information of all CASB systems running in the 4-tier CASB and information on whether CASB security control is executed for the request.

HTTP requests of the user's cloud service are transmitted to the secure agent through all CASB systems in the 4-tier environment as HTTP responses. The secure agent analyzes the received HTTP header information to check the availability of all CASB systems in the 4-tier environment.

Based on the availability performance information of the CASB system, the secure agent selects the CASB system to execute the security control for the cloud service request of the user, adds information to the HTTP header, and transmits it. The CASB determines whether the CASB information for the security service target is included in the header of the corresponding HTTP and then determines whether to execute the CASB security service.

6. Security Control Process

Because security controls of CASB must work with security policy of each organization, security control process of CASB begins with setting up security policies accurately. However, it is difficult for a security officer to manage the security policies of CASBs consistently when organization uses multiple CASBs.

When user uses cloud service, multiple heterogeneous CASBs can located in service flow. And then, if the security policies of each CASB are set differently, it can cause serious problems. So, when one CASB security policy is updated, other CASB security policy must be automatically updated.

Since cloud service uses HTTP, CASB can synchronize policies by adding information of security policies to the HTTP header. For the synchronization, the version of security policy, the date when security policy is set, and the CallbackURL address must be shared within CASB. In order to synchronize the latest CASB policies, the following metadata is included in the HTTP header.

Field name	Description	Example
CASB-policyVER	The Policy version	CASB-policyVER: 1.0.1.2
CASB-policyDATE	The date when the policy is set	CASB-policyDATE: 2017-07-24 13:22:30
CASB-policyCallbackURL	The Callback URL address to be used when an update of policy information is required	CASB-policyCallbackURL: https://www.abc.com/policy
CASB-type	CASB inline gateway or CASB Proxy	CASB-type: CASB Proxy

When policies change in a CASB proxy or a CASB inline gateway during network communication with SaaS applications, the corresponding component adds new metadata of such changed policies in an HTTP header. A CASB inline gateway or CASB secure API parses the HTTP header for CASB-policyVER or CASB-policyDATE before executing security control. If the currently applied version turns out to be an older version, the component that detects it requests policy information at the value of CASB-policyCallbackURL and updates the information.

7. Method to manage security control in BYOD

When a CASB proxy is used, client devices in a corporation or an organization forcibly go through CASBs when accessing to a cloud server, but in a BYOD environment, a cloud server user can access using a smart phone or the like, so that access by a non-CASB secure device(secure agent was installed, but not used) occurs.

In this case, although access control can be done through secure API, a security vulnerability may appear when a company using cloud service uses CASB proxy for protecting information inside company from exposure to cloud service such as Facebook.

Therefore, access to the cloud server should be applied to ensure that the client is checked or passed through the CASB. A method for preventing bypassing by non-CASB is to mount VPN(Virtual Private Network) and MDM(Mobile Device Management) function on secure agent.

In other words, the VPN and MDM modules are embedded in the secure agent, and it is registered in the management system at the initial installation. The management system checks whether the secure agent is running. In this case, it is possible to force the device to access to the cloud server through the CASB proxy under VPN while the secure agent is running.

In addition, it is possible to prevent bypass access with the secure agent removed. In case of security sensitive devices, security incidents can be prevented by initializing the smart phone through MDM when the secure agent is deleted or turned off.

8. Simulation and Performance evaluation

Since CASB is placed between SaaS application user and SaaS application server, latency would occur. So it is very important to minimize it for cloud service quality. We had proposed framework of 4-tier CASB as the method to reduce latency. And now we show the result of simulation test and its performance.

To verify effect of protocol we proposed for 4-tier CASB framework, we tested the performance of CASB for 5 cloud services we developed

We compared the cases with and without CASB, and in the case of “with CASB”, we compared the case where each CASB operates completely independently and the case where we use protocol we proposed.

First, the test environment is summarized as follows.

- Test overview and environment

- Test Period : 2018. 7.1 ~ 2018. 9.30.(3 months)
- Number of testers: 20 Users
- User Test Environment

	PC	Mobile
Processor	Intel Core i5, i7	Exynos 9810, 8895

System type	32-bit, 64-bit	64-bit
Memory	4GB, 8GB, 32GB	4GB, 6GB
Operating System	Windows 7, 8, 8.1ProK, 10	Android 8.0

- Cloud Service Operating Environment

Processor	Intel Xeon E5-2609, E5-2630
Memory	16GB, 32GB
Operating System	CentOS 6.6, Ubuntu 14.04
Cloud Operating S/W	OpenStack(ver. Icehouse, ver. mitaka)

- Cloud Services for Test
  - File sharing Cloud Application : SeaFile, Pydio
  - RSS feed Reader Cloud Application: Sismics Reader
  - SNS Cloud Application : GNU Social, ELGG
  - HRM Cloud Application : Orange HRM
  - Web Blog Cloud Application : Solo

- Test method
  - Access to test target cloud service and attempt various actions
  - Modify the security policy for cloud service in case of each access onto the service
  - Access cloud service with 2-tier, 3-tier and 4-tier CASB and without CASB
  - Distinguish the status of the function that prevents duplex check of security control and execute test
  - Distinguish the status on each system structure and the function that prevents duplex check of security control and measure latency about the cloud service use

- Test data
  - Number of requests : 1,851,258 cases
  - Cloud System without CASB : 329,275 cases
  - Cloud System with 2-tier CASB : 471,233 cases
  - Cloud System with 3-tier CASB: 553,622 cases
  - Cloud System with 4-tier CASB: 497,128 cases
  -
  - Volume of Network Traffic : about 12.7 TB(including FileStream data)
  - Cloud System without CASB : about 2TB
  - Cloud System with 2-tier CASB: about 3TB
  - Cloud System with 3-tier CASB: about 4.1TB
  - Cloud System with 4-tier CASB: about 3.6TB

- Test result

Before CASB was applied, the cloud service use latency appeared as an average of 37ms in 3 months. When CASB was applied but there was no access control protocol, which is the security control duplex preventive protocol, around 3~12 times greater latency resulted every time CASB system was added. However, in the case with access control protocol, around 3 times greater latency results even in the 4-tier CASB system so it appeared to be effective in the multi tier system.

	No use of protocol we propose	Use of protocol we propose
System without CASB	37ms	
System with 2-tier CASB	362ms	323ms
System with 3-tier CASB	836ms	340ms
System with 4-tier CASB	1203ms	369ms

9. Applied field of CASB and its relationship with 4-tier CASB

SASE (Secure Access Service Edge) is a product that implements various security functions on one edge and provides it as a service.[3] Recently, many global network companies are conducting research and development on SASE.

Since SASE includes various security functions, the CASB function is also included as one of the security functions provided by SASE, and the CASB function included here is the CASB inline gateway among the 4-tier CASBs (Secure Agent, CASB inline gateway, CASB proxy, CASB Secure API) presented by us.

Because SASE is an edge, it is located in the infrastructure, and the CASB included in SASE operates at the network layer to provide public cloud service security functions.

Therefore, since the CASB functions provided by SASE perform only some of the functions of our proposed 4-tier CASB, the need for efficient operation according to our proposed CASB structure is still valid.

10. Conclusion

This document introduced CASBs developed by various security companies as a way to safely use cloud services, classified CASBs released in the market into four types, and introduced the comprehensive construction method.

And the problem of inefficiency that may occur inevitably when users of cloud service use various types of CASBs was introduced, and solutions were presented.

In addition, CASB was applied to various cloud services, tested, and the performance results were analyzed.

Finally, SASE was introduced as an application example of CASB, and the relationship between CASB included in SASE and our proposed 4-tier CASB was explained.

We hope that as many people as possible can safely use cloud services by referring to this document.

11. References

[1] https://en.wikipedia.org/wiki/List_of_HTTP_header_fields

[2] http://www.gartner.com

[3] http://www.trendmicro.com

Annex 1

GAP ANALYSYS OF STANDARD ACTIVITY
ON CLOUD ACCESS SERVICE BROKER

1. CASB Vendors

CASB vendors develop solutions in one of the next five elements.

− Shadow IT

Shadow IT in cloud services poses hidden threats and potentially incurs costs as a result. Companies typically use hundreds of cloud services, many of which are impacted by shadow IT and represent a security blind spot. As a result, employees may not comply with their company's security requirements and may be using vulnerable and expensive cloud services. A CASB should be able to identify cloud services operating in shadow IT and detect any attempts to access them. It should also be capable of analyzing cloud service usage and estimating the risk index of each application. While some CASB vendors offer analysis of usage and estimation of risk index as part of their solutions, other CASB solutions only check for unknown cloud applications and their accessibility.

− Compliance Monitoring

Cloud service customers need to comply with certain rules in order to protect their data and personal information when transferring it to a cloud service. A CASB should be able to retrieve and organize company data, and understand the policy template which includes regular expressions. Additionally, it should be capable of supporting policy execution and exception policies such as data blocking, encryption, and deletion. Most CASB vendors offer these features except for the policy template, which requires further standardization work.

− Threat Protection

Organizations have a responsibility to protect their members who use cloud storage services and their clients from malicious code or security threats. They must also detect and prevent their members from uploading files infected with malicious code or unauthorized users attempting to access cloud services or data. Members should be able to receive protection against various security threats and malicious code. A CASB can assist with detecting and removing malicious code, analyzing user actions and network traffic, and detecting security threats and other types of threats. However, not all CASB solutions offer all of these functionalities. Therefore, standardization of threat protection is needed.

− Encryption

Maintaining confidentiality is crucial when storing data in cloud service storage. A CASB should protect this data from unauthorized access, sniffing during data transmission, and hidden threats such as backdoors. CASB should have the ability to support not only file-level encryption and field-level encryption but also a stronger encryption module. It should also be responsible for maintaining encryption keys. Most CASB vendors offer solutions that support file-level encryption and maintenance of encryption keys. However, the encryption algorithm and protocols for key exchange need to be included in CASB standardization.

- IAM(Identity and Access Management)

The fundamental principle of IAM, which is ensuring that the right people have access to the right resources at the right time, also applies to cloud services. A CASB should guarantee appropriate access to data stored across various cloud services. It can do this by supporting context-based access control, DRM technology, single sign-on for cloud services, and integrating with third-party IAM technology. Currently, most CASB vendors only include context-based access control in their solutions, while a few others with IAM support include the rest. Standardization efforts are necessary so that CASB systems with different configurations can share context-based access control policies.

2. Organizations for Standardization

Currently there is no standards organization for CASB. But we have progress of standards for some CASB technologies, and we would like to describe such efforts further.

- NIST(National Institute of Standards and Technology)

NIST (National Institute of Standards and Technology) is a research institute that supports science, technology, and development for the US federal government, and provides standards and guidelines in various fields. While NIST mentioned CASB as a cloud security solution in its SP-800-146 document, it has not published any standardization documents related to CASB. However, various standardization documents for cloud security are being published as follows:

NIST SP 500-292(NIST Cloud Computing Reference Architecture, 2011) : The adoption of cloud computing into the Federal Government and its implementation depend upon a variety of technical and non-technical factors. A fundamental reference point, based on the NIST definition of Cloud Computing, is needed to describe an overall framework that can be used government-wide. This document presents the NIST Cloud Computing Reference Architecture (RA) and Taxonomy (Tax) that will accurately communicate the components and offerings of cloud computing[1].

NIST SP 800-144(Guidelines on Security and Privacy in public Cloud Computing, 2011) : Cloud computing can and does mean different things to different people. The common characteristics most interpretations share are on-demand scalability of highly available and reliable pooled computing resources, secure access to metered services from nearly anywhere, and displacement of data and services from inside to outside the organization. While aspects of these characteristics have been realized to a certain extent, cloud computing remains a work in progress. This publication provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data, applications, and infrastructure to a public cloud environment[2].

NIST SP 800-145(The NIST Definition of Cloud Computing, 2011) : Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models[3].

NIST SP 800-146(Cloud Computing Synopsis and Recommendations, 2012) : This document reprises the NIST-established definition of cloud computing, describes cloud computing benefits and open issues, presents an overview of major classes of cloud technology, and provides guidelines and recommendations on how organizations should consider the relative opportunities and risks of cloud computing[4].

NIST SP 500-291 revision 2(NIST Cloud Computing Standards Roadmap, 2013) : NIST has been designated by the Federal Chief Information Officer (CIO) to accelerate the federal governments secure adoption of cloud computing by leading efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders. Standards are critical to ensure cost-effective and easy migration, to ensure that mission-critical requirements can be met, and to reduce the risk that sizable investments may become prematurely technologically obsolete. Standards are key elements required to ensure a level playing field in the global marketplace. The NIST Cloud Computing Standards Roadmap Working Group has surveyed the existing standards landscape for interoperability, performance, portability, security, and accessibility standards/models/studies/use cases/conformity assessment programs, etc., relevant to cloud computing. Using this available information, current standards, standards gaps, and standardization priorities are identified within this document[5].

NIST SP 800-210(General Access Control Guidance for Cloud Systems, 2020) : This document presents cloud access control characteristics and a set of general access control guidance for cloud service models: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). Different service delivery models require managing different types of access on offered service components. Such service models can be considered hierarchical, thus the access control guidance of functional components in a lower-level service model are also applicable to the same functional components in a higher-level service model. In general, access control guidance for IaaS is also applicable to PaaS and SaaS, and access control guidance for IaaS and PaaS is also applicable to SaaS. However, each service model has its own focus with regard to access control requirements for its service[6].

- ITU-T(International Telecommunication Union Telecommunication Standardization Sector)

ITU-T Recommendation classifies X.1600-X.1699 as Cloud Computing Security and while there are no standardization documents related to CASB, various cloud security-related technologies are being published as standardization documents.

ITU-T X.1601(Security framework for cloud computing, 2015) : Recommendation ITU-T X.1601 describes the security framework for cloud computing. The Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing. Appendix I provides a mapping table on how a particular security threat or challenge is addressed by one or more corresponding security capabilities[7].

ITU-T X.1602(Security requirements for software as a service application environments, 2016) : Recommendation ITU-T X.1602 analyses the maturity levels of software as a service (SaaS) application and proposes security requirements to provide a consistent and secure service execution environment for SaaS applications. These proposed requirements originate from cloud service providers (CSP) and cloud service partners (CSN) as they need a SaaS application environment to meet their demands on security. The requirements are general and independent of any service or scenario specific model (e.g. web services, or representational state transfer (REST)), assumptions or solutions[8].

ITU-T X.1603(Data security requirements for the monitoring service of cloud computing, 2018) : Recommendation ITU-T X.1603 analyses data security requirements for the monitoring service of cloud computing which include monitoring data scope requirements, monitoring data lifecycle, security requirements of monitoring data acquisition and security requirements of monitoring data storage. Monitoring data scope requirements include the necessary monitoring scope that cloud service providers (CSPs) should provide to maintain the cloud security and the biggest monitoring scope of CSPs. Monitoring data lifecycle includes data creation, data store, data use, data migrate, data present, data destroy and data backup. Monitoring acquisition determines the security requirements of the acquisition techniques of monitoring service. Monitoring data storage determines the security requirements for CSPs to store the monitoring data[9].

ITU-T X.1604(Security requirements of Network as a Service(NaaS) application environments, 2020) : Recommendation ITU-T X.1604 analyses security threats and challenges on Network as a Service (NaaS) in cloud computing and specifies security requirements of NaaS in NaaS application, NaaS platform and NaaS connectivity aspects based on corresponding cloud capability types[10].

ITU-T X.1605(Security requirements of Infrastructure as a Service(IaaS) application environments, 2020) : Infrastructure as a Service (IaaS) platforms and virtualized services face different, and perhaps more, challenges and threats than traditional information technology infrastructure and application. IaaS platforms that share computing, storage and networking services need protections specific to threats in an IaaS environment. Recommendation ITU-T X.1605 documents security requirements of public IaaS in order to help IaaS providers to improve security of the IaaS platform throughout the planning, building and operating stages[11].

ITU-T X.1606(Security requirements for communications as a Service application environments, 2020) : Recommendation ITU-T X.1606 identifies security threats and recommends security requirements for communications as a service (CaaS) application environments. The Recommendation describes scenarios and features of CaaS containing multi-communication capabilities. Then it identifies specific threats arising from unique CaaS features and recommends appropriate CaaS security requirements[12].

ITU-T X.1631(Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services, 2015) : Recommendation ITU-T X.1631 | ISO/IEC 27017 provides guidelines for information security controls applicable to the provision and use of cloud services[13].

ITU-T X.1641(Guidelines for cloud service customer data security, 2016) : Recommendation ITU-T X.1641 provides generic security guidelines for the cloud service customer (CSC) data in cloud computing. It analyses the CSC data security lifecycle and proposes security requirements at each stage of the data lifecycle. Furthermore, the Recommendation provides guidelines on when each control should be used for best security practice[14].

ITU-T X.1642(Guidelines for the operational security of cloud computing, 2016) : Recommendation ITU-T X.1642 provides generic operational security guidelines for cloud computing from the perspective of cloud service providers (CSPs). It analyses the security requirements and metrics for the operation of cloud computing. A set of security measures and detailed security activities for the daily operation and maintenance are provided to help CSPs mitigate security risks and address security challenges for the operation of cloud computing[15].

ITU-T X.1643(Security requirements and guidelines for virtualization containers in cloud computing environments, 2022) : Recommendation ITU-T X.1643 analyses security threats and challenges for virtualization containers in cloud computing environments and specifies a reference framework with security guidelines for virtualization containers in the cloud[16].

Currently, there are no standardization documents published related to X.1660-X.1679 (Cloud Computing Security Implementation) and X.1680-X.1699 (Other Cloud Computing Security).

- ISO/IEC(international Organization for Standardization/International Electrotechnical Commission)

Also ISO/IEC does not have any ongoing research or standardization on CASB. As for a standard related to cloud technology, it provided an overview of cloud computing with definitions of cloud computing in “ISO/IEC 17788:2014” on October 2014.

ISO/IEC 17788(Overview and vocabulary, 2014) : ISO/IEC 17788:2014 provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards. And This is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations)[17]

ISO/IEC 17789(Reference architecture, 2014) : ISO/IEC 17789:2014 specifies the cloud computing reference architecture (CCRA). The reference architecture includes the cloud

computing roles, cloud computing activities, and the cloud
computing functional components and their relationships[18].

ISO/IEC 27036-4(Guidelines for security of cloud services, 2016) : ISO/IEC 27036-4 defined guidelines that enable cloud service provider to effectively manage information security risks by identifying such risks associated with cloud service usage. Those guidelines also enable organizations using cloud service to address risks associated with the import and use of cloud services that can impact information security[19].

ISO/IEC TS 23176(Common technologies and techniques, 2020) : ISO/IEC TS 23167 provides a description of a set of common technologies and techniques used in conjunction with cloud computing[20].

3. Reference

[1] NIST SP 500-292 “NIST Cloud Computing Reference Architecture”
[2] NIST SP 800-144 “Guidelines on Security and Privacy in Public Cloud Computing”
[3] NIST SP 800-145 “The NIST Definition of Cloud Computing”
[4] NIST SP 800-146 “Cloud Computing Synopsis and Recommendations”
[5] NIST SP 500-291 “NIST Cloud Computing Standards Roadmap”
[6] NIST SP 800-210 “General Access Control Guidance for Cloud Systems”
[7] ITU-T X.1601“Security framework for cloud computing”
[8] ITU-T X.1602 “Security requirements for software as a service application environments”
[9] ITU-T X.1603 “Data security requirements for the monitoring service of cloud computing”
[10] ITU-T X.1604 “Security requirements of Network as a Service (NaaS) in cloud computing”
[11] ITU-T X.1605 “Security requirements of public Infrastructure as a Service (IaaS) in cloud computing”
[12] ITU-T X.1606 “Security requirements for communications as a service application environments”
[13] ITU-T X.1631 “Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services”
[14] ITU-T X.1641 “Guidelines for cloud service customer data security”
[15] ITU-T X.1642 “Guidelines for the operational security of cloud computing”
[16] ITU-T X.1643 “Security requirements and guidelines for virtualization containers in cloud computing environments”
[17] ISO/IEC 17788:2014 “Overview and vocabulary”
[18] ISO/IEC 17789:2014 “Reference architecture”
[19] ISO/IEC 27036-4:2016 “Guidelines for security of cloud services”
[20] ISE/IEC TS 23716 “Common technologies and techniques”
”