International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1603

(03/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cloud computing security – Cloud computing security design

Data security requirements for the monitoring service of cloud computing

Recommendation ITU-T X.1603

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	**X.1602–X.1639**
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1603

Data security requirements for the monitoring service of cloud computing

Summary

Recommendation ITU-T X.1603 analyses data security requirements for the monitoring service of cloud computing which includes 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 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 security requirements of the acquisition techniques of monitoring service. Monitoring data storage determines security requirements for CSPs to store the monitoring data.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1603	2018-03-29	17	11.1002/1000/13406

Keywords

Cloud, data security, monitoring.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation	3
4	Abbreviations and acronyms	3
5	Conventions	4
6	Overview	4
7	Scope of monitoring data for cloud computing	5
8	Monitoring data lifecycle in cloud computing	5
	8.1 Monitoring data collection	6
	8.2 Monitoring data storage	6
	8.3 Monitoring data use	6
	8.4 Monitoring data migration	6
	8.5 Monitoring data analysis	6
	8.6 Monitoring data presentation	6
	8.7 Monitoring data destruction	6
	8.8 Monitoring data backup	6
9	Security threats and challenges for monitoring data of cloud computing	6
	9.1 Security threats and challenges in monitoring data collection stage	7
	9.2 Security threats and challenges in monitoring data storage stage	7
	9.3 Security threats and challenges in monitoring data use stage	7
	9.4 Security threats and challenges in monitoring data migration stage	8
	9.5 Security threats and challenges in monitoring data analysis stage	8
	9.6 Security threats and challenges in monitoring data presentation stage	8
	9.7 Security threats and challenges in monitoring data destruction stage	8
	9.8 Security threats and challenges in monitoring data backup stage	8
10	Security requirements for monitoring data of cloud computing	8
	10.1 Security requirements for monitoring data collection	8
	10.2 Security requirements for monitoring data storage	9
	10.3 Security requirements for monitoring data use	9
	10.4 Security requirements for monitoring data migration	10
	10.5 Security requirements for monitoring data analysis	10
	10.6 Security requirements for monitoring data presentation	11
	10.7 Security requirements for monitoring data destruction	11
	10.8 Security requirements for monitoring data backup	12
Bibliography		13

Recommendation ITU-T X.1603

Data security requirements for the monitoring service of cloud computing

1 Scope

This Recommendation describes data security requirements for the monitoring service of cloud computing. The Recommendation analyses data security threats and challenges associated with the monitoring service in a cloud computing environment, and describes data security requirements of the monitoring service including data scope, data lifecycle, data acquisition and data storage. This Recommendation can be used by cloud service providers (CSPs) who provide monitoring services to cloud service customers (CSCs).

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-NIST-SP-800-53]: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.2 capability [b-ISO/IEC 19440]: Quality of being able to perform a given activity.

3.1.3 cloud computing [b-ITU-T Y.3500**]**: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.4 cloud service [b-ITU-T Y.3500**]**: One or more capabilities offered via cloud computing (see clause 3.1.3) invoked using a defined interface.

3.1.5 cloud service customer [b-ITU-T Y.3500**]**: Party (see clause 3.1.15) which is in a business relationship for the purpose of using cloud services (see clause 3.1.4).

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.6 cloud service partner [b-ITU-T Y.3500**]**: Party (see clause 3.1.15) which is engaged in support of, or auxiliary to, activities of either the cloud service provider (see clause 3.1.7) or the cloud service customer (see clause 3.1.5), or both.

3.1.7 cloud service provider [b-ITU-T Y.3500**]**: Party (see clause 3.1.15) which makes cloud services (see clause 3.1.4) available.

3.1.8 cloud service user [b-ITU-T Y.3500**]**: Natural person, or entity acting on their behalf, associated with a cloud service customer (3 see clause.1.5) that uses cloud services (see clause 3.1.4).

NOTE – Examples of such entities include devices and applications.

3.1.9 Communications as a Service (CaaS) [b-ITU-T Y.3500**]**: Cloud service category in which the capability provided to the cloud service customer (see clause 3.1.5) is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

3.1.10 community cloud [b-ITU-T Y.3500]: Cloud deployment model where cloud services (see clause 3.1.4) exclusively support and are shared by a specific collection of cloud service customers (see clause 3.1.5) who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

3.1.11 hypervisor [b-NIST-SP-800-125]: The virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware.

3.1.12 Infrastructure as a Service (IaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (see clause 3.1.5) is an infrastructure capabilities type.

NOTE – The cloud service customer (see clause 3.1.5) does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer (see clause 3.1.5) may also have limited ability to control certain networking components (e.g., host firewalls).

3.1.13 multi-tenancy [b-ITU-T Y.3500]: Allocation of physical or virtual resources such that multiple tenants (see clause 3.1.24) and their computations and data are isolated from and inaccessible to one another.

3.1.14 Network as a Service (NaaS) [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer (see clause 3.1.5) is transport connectivity and related network capabilities.

NOTE – NaaS can provide any of the three cloud capabilities types.

3.1.15 party [b-ISO/IEC 27729**]**: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.16 personally identifiable information [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

3.1.17 Platform as a Service (PaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (see clause 3.1.5) is a platform capabilities type.

3.1.18 private cloud [b-ITU-T Y.3500]: Cloud deployment model where cloud services (see clause 3.1.4) are used exclusively by a single cloud service customer (see clause 3.1.5) and resources are controlled by that cloud service customer (see clause 3.1.5).

3.1.19 public cloud [b-ITU-T Y.3500]: Cloud deployment model where cloud services (see clause 3.1.4) are potentially available to any cloud service customer (see clause 3.1.5) and resources are controlled by the cloud service provider (see clause 3.1.7).

3.1.20 security domain [b-ITU-T X.810]: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.

3.1.21 security incident [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

3.1.22 service level agreement (SLA) [b-ISO/IEC 20000-1]: A documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.23 Software as a Service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (see clause 3.1.5) is an application capabilities type.

3.1.24 tenant [b-ITU-T Y.3500]: One or more cloud service users (see clause 3.1.8) sharing access to a set of physical and virtual resources.

3.1.25 threat [b-ISO/IEC 27000]: A potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.26 vulnerability [b-NIST-SP-800-30]: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 monitoring data: Monitoring data is the output of the cloud monitor service, which helps cloud service provider (CSP) and cloud service customers (CSC) manage cloud platforms and cloud resources.

3.2.2 monitor service: The monitor service activity monitors the delivered service quality with respect to service levels as defined in the service level agreement (SLA) between cloud service customer and cloud service provider.

3.2.3 necessary monitoring data: Necessary monitoring data is used to maintain service level agreements (SLA). Necessary monitoring data could help cloud service provider (CSP) to keep cloud computing platforms security and stable. Necessary monitoring data could include, but is not limited to, management system monitoring data, physical resources monitoring data, network monitoring data and etc. Necessary monitoring data is mainly used by CSPs but could also be shared with cloud service customers (CSCs).

3.2.4 optional monitoring data: Optional monitoring data is provided on the demand of cloud service customers (CSCs) and to provide cloud monitor service. Optional monitoring data could include, but is not limited to, virtual machine monitoring data, data storage service monitoring data, CSCs' application on cloud monitoring data and etc.

3.2.5 virtual machine (VM): An efficient, isolated, logical duplicate of a real machine.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

BCP Business Continuity Plan

CaaS Communications as a Service

CPU Central Processing Unit

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

CSU Cloud Service User

DDOS Distributed Denial of Service

DNS Domain Name System

DOS Denial of Service

IaaS Infrastructure as a Service

IAM Identity and Access Management

ICT Information and Communication Technology

IP Internet Protocol

IT Information Technology

NaaS Network as a Service

OS Operating System

PaaS Platform as a Service

PII Personally Identifiable Information

PKI Public Key Infrastructure

SaaS Software as a Service

SIM Subscriber Identity Module

SLA Service Level Agreement

VM Virtual Machine

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview

This Recommendation analyses data security requirements for the monitoring service of cloud computing including monitoring data scope, monitoring data lifecycle, security threats and challenges, and monitoring data security requirements of cloud computing.

Monitoring data scope describes two types of cloud monitoring data: necessary and optional, and also explains the use cases.

Monitoring data lifecycle, and the security threats and challenges, describe the content and security threats and challenges of cloud monitoring data collection, storage, use, migration, analysis, presentation, destruction and backup.

Monitoring data security requirements describes the detailed requirements for each lifecycle stage of cloud monitoring data.

7 Scope of monitoring data for cloud computing

In a cloud computing environment, there are two types of monitoring data: necessary monitoring data and optional monitoring data.

Necessary monitoring data is that which is used to maintain service level agreements (SLAs). Necessary monitoring data can help the CSP run the cloud computing platform securely and stably. Necessary monitoring data may include, but is not limited to, management system monitoring data, physical resources monitoring data and network monitoring data. Necessary monitoring data is mainly used by CSPs but could also be shared with CSCs.

Optional monitoring data is that which is provided at the request of the CSC to provide the monitoring service by the CSP. Optional monitoring data may include, but is not be limited to, virtual machine monitoring data, data storage service monitoring data and the CSCs' data associated with the monitoring of their own application on cloud.

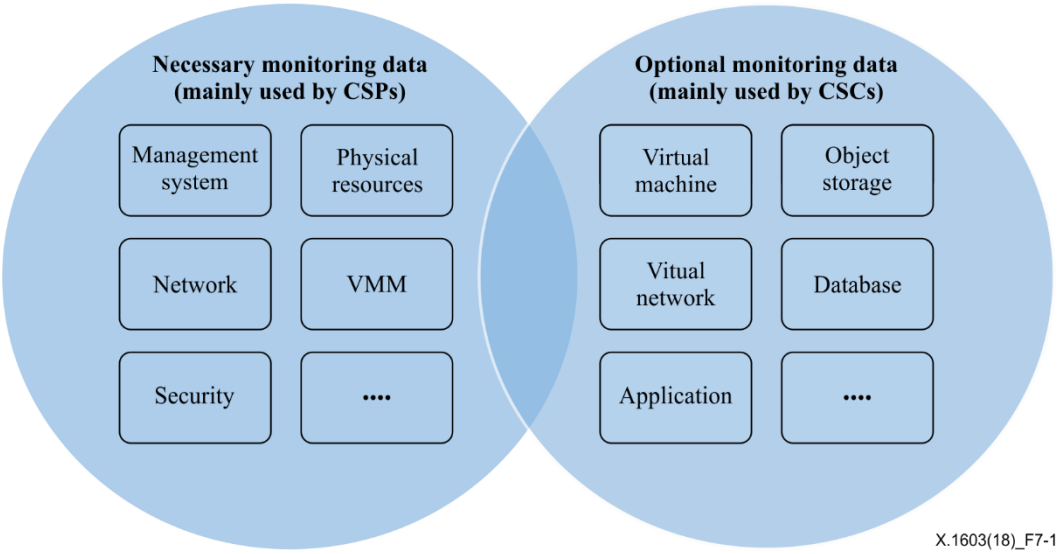

Figure 7-1 – Use cases of two types of monitoring data

Necessary monitoring data is mainly used by CSPs, but could also be used by CSCs. For example, monitoring data of cloud physical resources is mainly used by CSPs to maintain the stability of the cloud platform, but could also be used by CSCs if the cloud-related physical resources were provided to the customers as a service.

Optional monitoring data is provided as the request of CSCs and also mainly used by CSCs. CSPs could also use optional monitoring data to maintain SLAs. For example, CSCs could require the CSCs' data associated with the monitoring of their own applications in the cloud. This data is provided by CSP, and used to better manage their applications in the cloud. For example, a CSP could use database as a service (DBaaS) monitoring data to maintain the security and stability of database resources and service in cloud.

The relationship of these two types of monitoring data is illustrated in Figure 7-1.

8 Monitoring data lifecycle in cloud computing

This clause describes the lifecycle of monitoring data in cloud computing and clarifies the main differences between it and lifecycle of other data in cloud computing.

8.1 Monitoring data collection

Monitoring data collection results from the acquisition of monitoring data and the transmission of that data to a storage server. Most monitoring data is created by the use of the cloud service by the CSC. Necessary monitoring data can also be created by other cloud service monitoring activities.

8.2 Monitoring data storage

After creating a monitoring data collection, cloud monitoring data can be stored in the CSC cloud resources locally, or in monitoring data storage servers of the CSP.

8.3 Monitoring data use

Monitoring data can be used to maintain the performance and security of the cloud platform and the cloud service by the CSP; it can also be used to maintain cloud resources performance and security by CSCs.

8.4 Monitoring data migration

When cloud resources are migrated, monitoring data can migrate along with the cloud resources.

8.5 Monitoring data analysis

Monitoring data can be analyzed by the CSP and CSC to understand the status of the cloud platform resources in order to better manage and secure them.

8.6 Monitoring data presentation

It is recommended that monitoring data be presentable in meaningful ways in order to be useful for better management of SLAs and cloud security. Since the volume of cloud monitoring data can be very large, is recommended that these data be summarized in a manageable and understandable way.

8.7 Monitoring data destruction

To maintain monitoring data security, the CSP is required to destroy monitoring data as CSCs demand.

CSPs can optionally destroy monitoring data after an appropriate period of time after monitoring data creation.

8.8 Monitoring data backup

It is required to create monitoring data backups and to restore data from backups.

9 Security threats and challenges for monitoring data of cloud computing

The security threats and challenges for cloud computing, clauses 7 and 8 respectively in [b-ITU-T X.1601], have provided the security threats and challenges for the CSC and CSP in cloud computing; cloud monitoring data also faces similar security threats and challenges that are defined in [b-ITU-T X.1601. Some of these security threats and challenges for cloud monitoring data include but are not limited to those shown below:

a) data loss and leakage;

b) insecure service access;

c) unauthorized administration access;

d) insider threats;

e) loss of trust;

f) loss of governance;

g) loss of confidentiality;

h) service unavailability;

i) misappropriation of intellectual property;

j) shared environment;

k) jurisdictional conflict;

l) bad migration and integration.

For each monitoring data lifecycle stage, cloud monitoring data face some particular security threats and challenges.

9.1 Security threats and challenges in monitoring data collection stage

a) data collection without authorization: A CSP or attackers may collect the CSC's monitoring data without permission or authorization.

b) acquisition interface vulnerability: Attackers may use a monitoring data acquisition interface vulnerability.

c) spoofing: Attackers could masquerade as the management system, or data storage server, of cloud monitoring service, and cause the loss of monitoring data.

d) tampering and intercepting: Attackers could use man-in-the-middle or other network attacks to tamper with, or intercept monitoring data.

e) insecure service access: In the monitoring data collection stage, insecure access to the data collection interfaces could cause monitoring data loss.

f) unauthorized administration access: Unauthorized administration access to the CSP's monitoring data collection system, or the CSC's system could result in monitoring data loss. For example, attackers may use a system vulnerability to gain unauthorized administration access to the CSC's system and modify the monitoring collection destination IP address to that of the attackers.

9.2 Security threats and challenges in monitoring data storage stage

a) data loss and leakage: As the cloud service environment is typically a multi-tenant one, loss or leakage of data is a serious threat to both the CSC and CSP. A lack of appropriate management of cryptographic information, such as encryption keys, authentication codes and access privilege, could lead to significant damages, such as data loss and unexpected leakage to the outside. For example, insufficient authentication, authorization, and audit controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data centre reliability; and disaster recovery, can be recognized as major threats.

b) service unavailability: A monitoring data storage server can be attacked by a denial of service (DoS) or distributed denial of service (DDoS) attack; in addition, the monitoring data storage hardware could fail and cause data loss or destruction.

9.3 Security threats and challenges in monitoring data use stage

a) data misuse: CSC monitoring data could be misused by the CSP. Monitoring data could be used by a CSP to maintain SLA and the operation of cloud computing platform and resources; however, CSC monitoring data could also be used for other purposes by the CSP without CSC permission.

b) insider threats: An employee of a CSP or CSC could misuse the CSC's monitoring data for other than intended purposes.

c) system vulnerability: Monitoring data could be lost during data usage due to system vulnerabilities.

d) eavesdropping: Monitoring data could be subject to eavesdropping by attackers.

9.4 Security threats and challenges in monitoring data migration stage

a) data misuse: Monitoring data could migrate between different physical locations. It is very important not to allow data to be misused as a result of monitoring data being transmitted to different locations.

b) spoofing: Attackers could masquerade as the management system or data storage server of a cloud monitoring service, and cause the loss or misuse of monitoring data.

c) tampering and intercepting: Attackers could use man-in-the-middle or other network attacks to tamper and intercept monitoring data.

9.5 Security threats and challenges in monitoring data analysis stage

a) data misuse: CSC monitoring data could be misused by the CSP during data analysis.

b) system vulnerability: Monitoring data could be lost due to a data analysis system vulnerability.

c) DoS attack: A monitoring data analysis server could be attacked by DoS or DDoS attack.

9.6 Security threats and challenges in monitoring data presentation stage

a) data misuse: CSC monitoring data could be misused (or be presented without CSC permission) by the CSP during data presentation.

b) system vulnerability: Reporting and analysis data could be lost due to a data presentation system vulnerability.

c) misrepresentation: CSC monitoring data could be misrepresented during a data presentation.

9.7 Security threats and challenges in monitoring data destruction stage

a) spoofing: Attackers could masquerade as the management system of the cloud monitoring service and cause the loss of other monitoring data.

b) operating system vulnerability: Monitoring data could be lost during data usage due to a system vulnerability.

9.8 Security threats and challenges in monitoring data backup stage

a) operating system vulnerability: Monitoring data could be lost during the data backup and result in the inability to restore data due to a system vulnerability.

10 Security requirements for monitoring data of cloud computing

This clause identifies the data security requirements for the monitoring service of cloud computing.

10.1 Security requirements for monitoring data collection

The data security requirements for the monitoring data collection include the following:

a) optional monitoring data is required to be created only by CSC request;

b) it is recommended to provide notification to the CSC when necessary monitoring data is created;

c) it is recommended to notify the CSC of the scope of monitoring data;

d) it is required to maintain integrity and accuracy of monitoring data;

e) it is recommended to use standard data acquisition techniques;

f) it is recommended to provide access control methods to the interfaces of monitoring data acquisition such as white list, black list, etc.;

g) it is recommended to provide cryptographic methods to ensure the security of the monitoring data acquisition interface;

h) it is recommended to use standard network protocols between the cloud resources and monitoring data storage servers.

Table 10-1 provides a summary mapping of monitoring data collection security threats to security requirements.

Table 10-1 – Monitoring data collection: security threats mapping to security requirements

Security threats	Security requirements
Data collection without authorization	a), b), c)
Acquisition interface vulnerabilities	d), e), f), g)
Spoofing	d), e), f), g), h)
Tampering and interception	h)
Insecure service access	b), d), e), f), g), h)
Unauthorized administrative access	d), e), f), g), h)

10.2 Security requirements for monitoring data storage

The data security requirements for the monitoring data storage include the following:

a) it is recommended that the CSP provide the appropriate access control methods to the monitoring data storage servers;

b) it is recommended that the CSP identify the maximum period of time for monitoring data retention;

c) it is recommended that the CSP provide appropriate encryption methods for monitoring data.

Table 10-2 provides a summary mapping of monitoring data storage security threats to security requirements.

Table 10-2 – Monitoring data storage: security threats mapping to security requirements

Security threats	Security requirements
Data loss and leakage	a), b), c)
Service unavailability	a), c)

10.3 Security requirements for monitoring data use

The data security requirements for the monitoring data use include the following:

a) it is required that the CSP clearly identify how the monitoring data is going to be used to the CSC;

b) it is recommended that the CSP provide a formal monitoring data use declaration to the CSC, such as that illustrated in Figure 10-1.

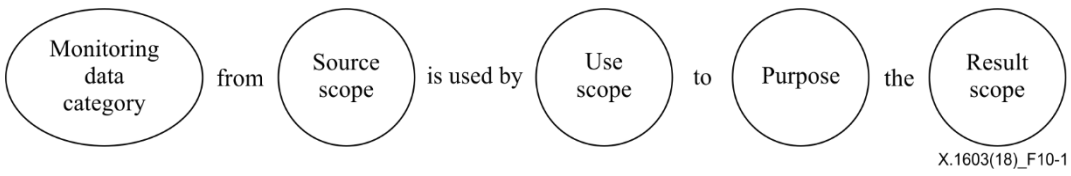

Figure 10-1 – Recommended monitoring data use declaration

c) it is required that the CSP provide notification and obtain CSC permission prior to the use of monitoring data for other than intended purpose;

d) it is required that the CSP support logging and auditing of monitoring data usage.

Table 10-3 provides a summary mapping of monitoring data use security threats to security requirements.

Table 10-3 – Monitoring data use: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a), b), c), d)
Insider threats	a), b), c), d)
System vulnerabilities	d)
Eavesdropping	d)

10.4 Security requirements for monitoring data migration

The data security requirements for the monitoring data migration include the following:

a) it is recommended that the CSP provide notification to the CSC of monitoring data migration;

b) it is required that the CSP ensure secure transmission during monitoring data migration;

c) it is required that the CSP support logging and auditing of monitoring data migration operations.

Table 10-4 provides a summary mapping of monitoring data migration security threats to security requirements.

Table 10-4 – Monitoring data migration: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a), c)
Spoofing	b), c)
Tampering and intercepting	b), c)

10.5 Security requirements for monitoring data analysis

The data security requirements for the monitoring data analysis include the following:

a) it is required that the CSP provide notification regarding the purpose of monitoring data analysis to the CSC;

b) it is required that the CSP implement defenses against the vulnerabilities of monitoring data analysis system, for example the CSP should prevent data loss and leakage in the monitoring data analysis system;

Table 10-5 provides a summary mapping of monitoring data analysis security threats to security requirements.

Table 10-5 – Monitoring data analysis: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a)
System vulnerability	b)

Table 10-5 – Monitoring data analysis: security threats mapping to security requirements

Security threats	Security requirements
DoS attack	b)

10.6 Security requirements for monitoring data presentation

The data security requirements for the monitoring data presentation include the following:

a) it is required that the CSP maintain the integrity and accuracy of presented monitoring data;

b) it is required that the CSP implement authentication methods to protect access the monitoring data presentation;

c) it is required that the CSP support defenses against the vulnerabilities of the monitoring data presentation system, for example the CSP could use penetration testing methods to prevent vulnerabilities of the monitoring data presentation system.

Table 10-6 provides a summary mapping of monitoring data presentation security threats to security requirements.

Table 10-6 – Monitoring data presentation: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a), b)
System vulnerability	b), c)
Misrepresentation	a), b), c)

10.7 Security requirements for monitoring data destruction

The data security requirements for the monitoring data destruction include the following:

a) it is required that the CSP provide appropriate destruction methods for monitoring data;

b) it is required that the CSP prevent the unintended destruction of monitoring data;

c) it is required that the CSP prevent the incomplete destruction of monitoring data;

d) it is required that the CSP erase any CSC specific keys for encrypted data;

e) it is required that the CSP destroy copies of monitoring data;

f) it is required that the CSP provide notification of monitoring data destruction to the CSC.

Table 10-7 provides a summary mapping of monitoring data destruction security threats to security requirements.

Table 10-7 – Monitoring data destruction: security threats mapping to security requirements

Security threats	Security requirements
Spoofing	a), b), c), d), e), f)
Operating system vulnerability	b), c), d), e), f)

10.8 Security requirements for monitoring data backup

The data security requirements for the monitoring data backup include the following:

a) it is required that the CSP provide backup methods to prevent monitoring data loss;

b) it is required that the CSP maintain the integrity and accuracy of restored monitoring data;

c) it is required that the CSP support logging and auditing of monitoring data restoration.

Table 10-8 provides a summary mapping of monitoring data backup security threats to security requirements.

Table 10-8 – Monitoring data backup: security threats mapping to security requirements

Security threats	Security requirements
Operating system vulnerability	a), b), c)

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995), *Information technology – Open System Interconnection – Security frameworks for open system: Overview*.

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[b-ISO/IEC 19440] ISO/IEC 19440 (2007), *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/IEC 19944] ISO/IEC 19944 (2016), *Information technology – Cloud services and devices: data flow, data categories and data use*.

[b-ISO/IEC 20000-1] ISO/IEC 20000-1 (2011), *Information technology – Service management – Part 1: Service management system requirements*.

[b-ISO/IEC 27000] ISO/IEC 27000 (2016), *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27729] ISO/IEC 27729 (2012), *Information and documentation – International standard name identifier (ISNI)*.

[b-ISO/IEC 29100] ISO/IEC 29100 (2011), *Information technology –Security techniques – Privacy framework*.

[b-NIST-SP-800-30] NIST Special Publication 800-30 (2012), *Guide for Conducting Risk Assessments*.

[b-NIST-SP-800-53] NIST Special Publication 800-53 Rev. 3 (2013), *Recommended Security Controls for Federal Information Systems and Organizations*.

[b-NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies*.

[b-NIST-SP-800-145] NIST Special Publication 800-145 (2011), *The NIST Definition of Cloud Computing*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2018