International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1752

(01/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Data security – Big Data Security

Security guidelines for big data infrastructure and platform

Recommendation ITU-T X.1752

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 (1)	X.1140–X.1149
Application Security (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.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
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
Cyber Defence	X.1590–X.1599
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
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	**X.1750–X.1759**
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1752

Security guidelines for big data infrastructure and platform

Summary

Recommendation ITU-T X.1752 analyses security threats and challenges for big data infrastructure and big data platform and specifies a reference framework for mapping security guidelines against threats for the big data infrastructure and platform.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1752	2022-01-07	17	11.1002/1000/14806

Keywords

Big data, infrastructure, platform, security guidelines.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1752

Security guidelines for big data infrastructure and platform

1 Scope

This Recommendation describes the big data infrastructure and platform from existing standardization works in relevant fora. This Recommendation develops a threat assessment methodology and specifies security guidelines to protect the big data infrastructure and big data platform. This Recommendation also provides a mapping between threats and security guidelines.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1279] Recommendation ITU-T X.1279 (2020), *Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms*.

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

[ITU-T X.1603] Recommendation ITU-T X.1603 (2018), *Data security requirements for the monitoring service of cloud computing.*

[ITU-T X.1605] Recommendation ITU-T X.1605 (2020), *Security requirements of public Infrastructure as a Service (IaaS) in cloud computing.*

[ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities.*

[ITU-T Y.3605] Recommendation ITU-T Y.3605 (2020), *Big data – Reference architecture.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 audit [b-ITU-T X.800]: An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

3.1.3 authentication [b-ISO/IEC 18014-2]: Provision of assurance in the identity of an entity.

3.1.4 big data analysis [b-ITU-T Y.2244]: Scrutiny performed on massive volume of data with the purpose of obtaining meaningful results, such as trends or preferences.

3.1.5 data desensitization [b-ITU-T X.1217]: A process to hide the sensitive data.

3.1.6 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.7 firewall [b-ISO/IEC 27033-1]: Type of security barrier placed between network environments – consisting of a dedicated device or a composite of several components and techniques – through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic, as defined by the local security policy, is allowed to pass.

3.1.8 load balancing [b-ITU-T Y.2052]: A scheme by which the traffic load could be separated and balanced to effectively utilize the network resources (e.g., link bandwidth).

3.1.9 intrusion detection system [b-ISO/IEC 27039]: Information systems used to identify that an intrusion has been attempted, is occurring, or has occurred.

3.1.10 intrusion prevention system [b-ITU-T X.1361]: Variant on intrusion detection systems that are specifically designed to provide an active response capability.

3.1.11 multi-factor authentication [b-ITU-T X.1158]: Authentication with at least two independent authentication factors.

3.1.12 redundancy [b-ITU-T E.800]: In an item, the existence of more than one means for performing a required function.

3.1.13 robustness [b-ITU-T J.1014]: Property of the implementation of a specified ECI secure function representing the effort and/or cost involved to compromise the security of the implemented secure function.

3.1.14 security configuration parameter [b-ITU-T X.1046]: A set of parameters which describe the features of the security function, such as maximum bandwidth, maximum number of connections, etc. supported by the security function, protected object and security actions of the security function.

3.1.15 single sign-on [b-ITU-T Y.2201]: The ability to use an authentication assertion from one network operator/service provider to another operator/provider for a user either accessing a service or roaming into a visited network.

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

3.1.17 validation [b-ITU-T Z.450]: A process of checking a specification to ensure that it is syntactically and semantically correct and represents the intended behaviour.

3.1.18 vulnerability [b-ITU-T X.1524]: Any weakness in software that could be exploited to violate a system or the information it contains

3.1.19 whitelist [b-ITU-T X.1245]: An identification list of persons or sources in communication services, where the identifications of the list are known, trusted, or explicitly permitted.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 big data infrastructure: A system composing basic physical devices and network environment in big data ecosystem to perform big data services for data collection, data processing, data management, etc.

3.2.2 big data platform: A system or a set of distributed systems in big data ecosystem to perform data analysis, data visualization, and other functions.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

BDAP Big Data Application Provider

BDIP Big Data Infrastructure Provider

DOS Denial of Service

DDOS Distributed Denial of Service

IAM Identity and Access Management

IDS Intrusion Detection System

IP Internet Protocol

IPS Intrusion Prevention System

SSO Single Sign-On

VM Virtual Machine

5 Conventions

In this Recommendation:

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required.

6 Security threats and challenges to big data infrastructure and platform

As defined in [ITU-T Y.3600] and shown in Figure 6-1 (i.e., adapted from Figure 7-1 of [ITU-T Y.3600]), big data platform is provided by big data application provider (BDAP) to perform data analysis, data visualization, and other functions. Big data infrastructure is provided by big data infrastructure provider (BDIP) to perform big data services including data collection, data processing, data management, etc.

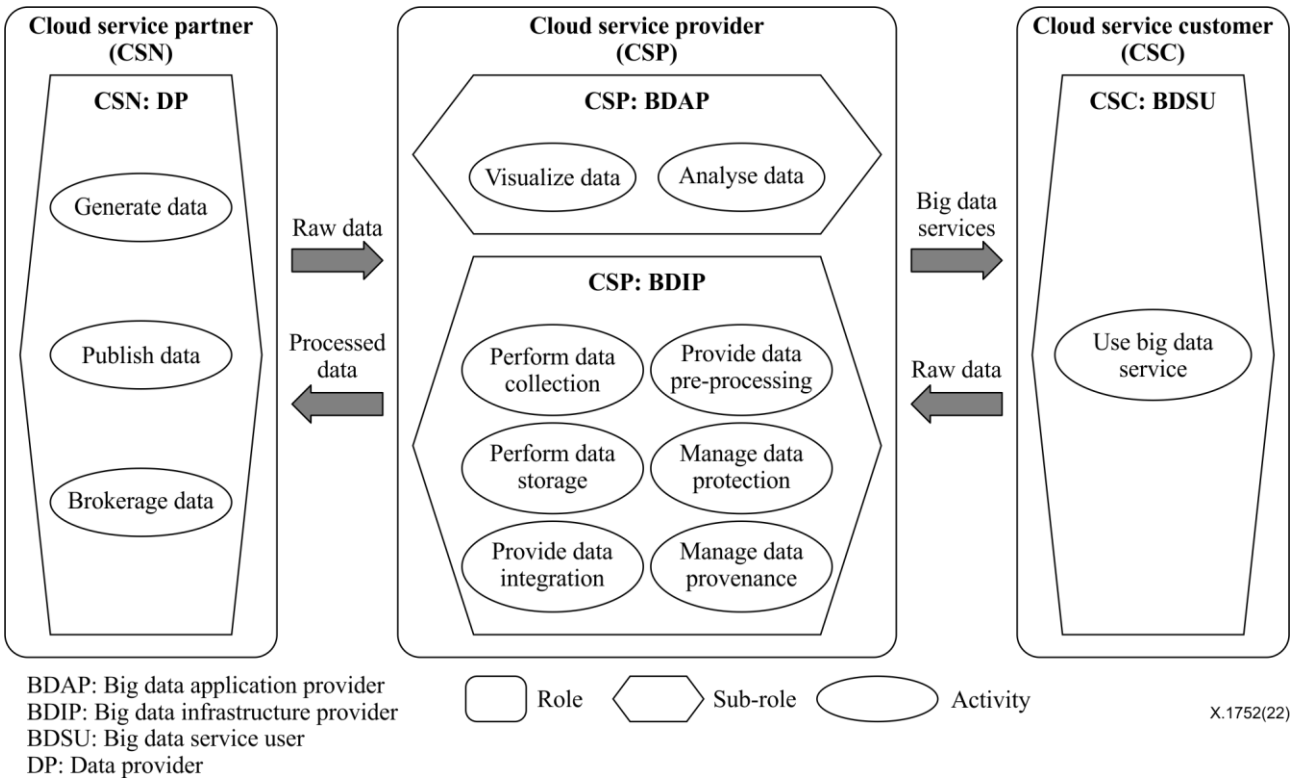

Figure 6-1 – Cloud computing based big data system

6.1 Security threats and challenges to big data infrastructure

Security threats and challenges to big data infrastructure include those to data collection, data storage, data integration, data pre-processing, and data management.

6.1.1 Security threats and challenges to data collection

Regarding data collection security, security threats and challenges include:

a) Data collection without authorization: attackers may collect the data without user's permission or authorization.

b) Data collection interface vulnerability: attackers may use data collection interface vulnerability to access the process of collection and cause data loss.

c) Unauthorized administration access: unauthorized administration access to data collection system could result in data loss. For example, attackers may use a system vulnerability to gain unauthorized administration access to the data collection system and modify the collection destination Internet protocol (IP) address to that of the attackers.

6.1.2 Security threats and challenges to data storage

Regarding data storage security, security threats and challenges include:

a) Data loss and leakage: 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. In addition, the massive convergence of multi-source data increases the difficulty of access control of data storage. The complex scenarios of big data storage and flow make the implementation of data encryption difficult to implement.

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

c) Security threats and challenges to physical facilities of data storage: regarding physical facilities security, it faces similar security threats and challenges as specified in clause 9.3 of [ITU-T X.1601] and clause 7 of [ITU-T X.1605].

d) Service threats and challenges to the terminal of data storage terminal: regarding the terminal of data storage, security threats and challenges focus on the security configuration parameter of the hardware and software of terminals which includes security configuration parameters of operating system, office software, browser, and mail system, etc. The main security threats and challenges include false set of security configuration parameters, late updates of security configuration parameters, vulnerabilities in security configuration parameters, etc.

6.1.3 Security threats and challenges to data integration

Regarding data integration security, security threats and challenges include:

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

b) Spoofing: as defined in [ITU-T X.1279], spoofing is the pretence assumed by an entity to be a different entity, by presenting a recorded image or other biometric data sample, or an artificially derived biometric characteristic, in order to impersonate an individual. Attackers could masquerade as the management system or data storage server and cause the loss or misuse of data during data integration.

c) Network security threats during data integration: it faces similar security threats and challenges as specified in clause 9.5 of [ITU-T X.1601]. In addition, the particular security challenges in big data infrastructure focus on the integrated security management across the physical network, virtual network, and cloud environments.

6.1.4 Security threats and challenges to data pre-processing

Regarding data pre-processing security, security threats and challenges include:

a) Insider threats: an employee of the BDAP could misuse the user's data for other than intended purposes during data pre-processing without the user's permission.

b) System vulnerability: data could be lost during data pre-processing due to system vulnerabilities.

6.1.5 Security threats and challenges to data management

Regarding data management security, security threats and challenges include:

a) Software vulnerabilities: potential security vulnerabilities of the software used in big data management could be exploited by attackers. Technical defects of system virtualization could cause several security risks; in addition, immature operation and maintenance technology could result in risks being more serious. Additionally, large-scale distributed storage and computing models of big data infrastructure and platform cause higher risks of security configuration parameters to the software used in big data management.

b) Broken access control: broken access control of data management could cause data to be lost, leaked, or misused.

c) Unauthorized administration access: unauthorized administration access to the big data management system could result in data being lost, leaked, or misused. For example, attackers may use a system vulnerability to gain unauthorized administration access to the big data system and modify the data collection destination Internet protocol (IP) address to that of the attackers.

d) Insider threats: careless or inadequately trained users (or family members in a consumer setting), or malicious action by disgruntled employees could cause data loss.

6.2 Security threats and challenges to big data platform

Security threats and challenges to big data platform include those to data visualization and data analysing.

6.2.1 Security threats and challenges to data analysing

Regarding data analysing security, security threats and challenges include:

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

b) DoS/DDoS attack: data analysis server could be attacked by DoS or DDoS attack.

c) Shared use of data analysing applications: data analysing applications are normally used by different users, which could cause virtual machine (VM) escape, data leakage, etc.

d) Insecure access: insecure access to big data analysing could cause application data to be lost, leaked or misused.

e) Unauthorized administration access: unauthorized administration access to the big data analysing could result in data loss.

6.2.2 Security threats and challenges to data visualising

Regarding data visualising security, security threats and challenges include:

a) Data misuse: data could be misused (or be presented without user's permission) by the BDAP during data visualising.

b) System vulnerability: reporting and analysis data could be lost due to a data visualising system vulnerability.

c) Misrepresentation: data could be misrepresented during data visualising without user's permission because of the failure of access control policies.

7 Security guidelines for big data infrastructure and platform

As defined in [ITU-T Y.3605], the layering framework used in big data reference architecture has four layers, plus a set of functions which span across the layers. These four layers are:

– Access layer;

– Application layer;

– Processing layer; and

– Data source layer.

The functions which span the layers are called the multi-layer functions.

The layering framework is shown in Figure 7-1 (i.e., adapted from Figure 8-2 of [ITU-T Y.3605]).

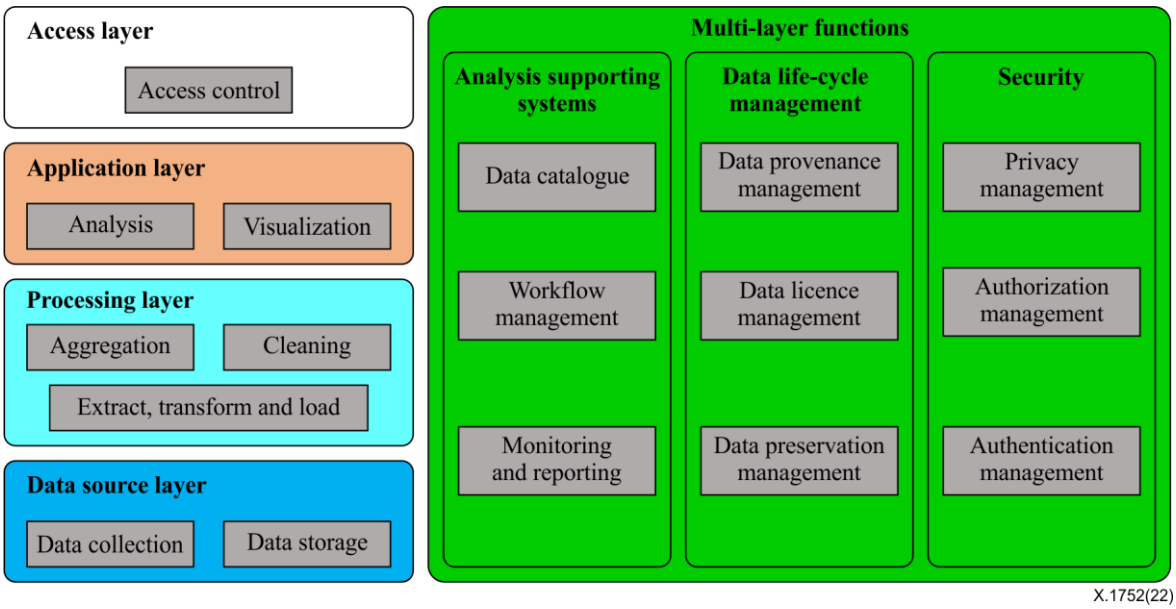

Figure 7-1 – Big data layering framework

Based on the layering framework shown in Figure 7-1, this Recommendation uses an architecture for big data infrastructure and platform security as shown in Figure 7-2.

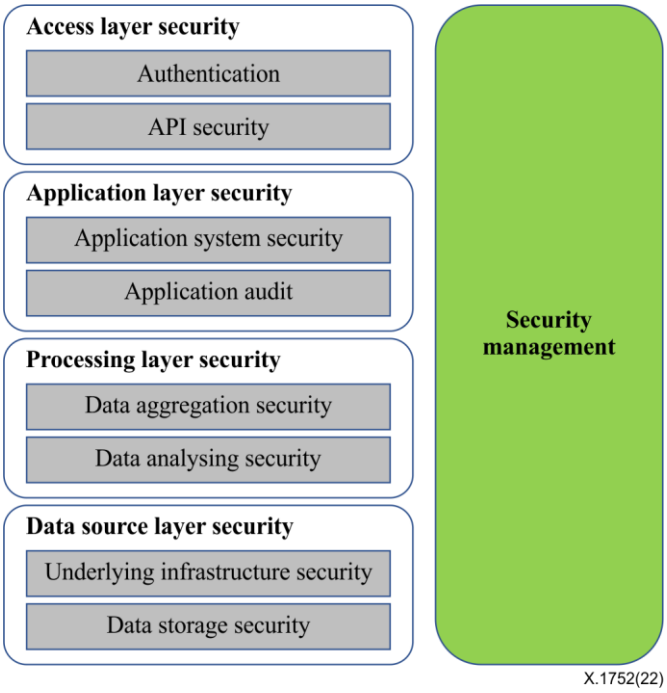

Figure 7-2 – Architecture for big data infrastructure and platform security

This Recommendation specifies security guidelines for big data infrastructure and platform and includes:

a) Security guidelines for data source layer;

b) Security guidelines for processing layer;

c) Security guidelines for application layer;

d) Security guidelines for access layer;

e) Guidelines for security management.

7.1 Security guidelines for data source layer

Security guidelines for data source layer focus on underlying infrastructure security and data storage security.

7.1.1 Security guidelines for underlying infrastructure

Security guidelines for underlying infrastructure include the following:

a) It is recommended to divide virtual infrastructures into internal and external security domains and implement different security policies on demand. It is recommended to provide effective isolation mechanisms between internal and external security domains.

b) It is recommended to implement strict access control policies between security domains of virtual infrastructures. It is recommended to use the least privilege principle, thus user authentication and authorization to be assigned on the basis of role responsibilities to allow access control to virtual infrastructures.

c) It is recommended to deploy security software, such as antivirus software, on virtual infrastructures to enhance security protection, and periodically update virus and malicious code databases.

d) It is recommended to deploy network attack detection and protection equipment, for example, intrusion prevention system (IPS)/intrusion detection system (IDS), firewall, DDoS protection, etc., at the boundary between internal and external networks, and periodically update attack signature databases to latest versions.

e) It is recommended to implement strict isolation and access control policies at internal and external network boundaries to prevent unauthorized accesses for underlying infrastructures.

f) It is recommended to monitor network traffics for underlying infrastructures and perform deep inspections, including key information such as network flow statistics, abnormal network traffic, etc.

g) It is recommended to display attack information, such as attack type, source/destination IP addresses, timestamp, etc. when attacks are detected.

h) It is recommended to undertake centralized real-time security monitoring, which includes the running status of various physical and virtual resources.

7.1.2 Security guidelines for data storage

Security guidelines for data storage include the following:

a) It is recommended to implement secure data storage components, such as secure distributed file system, secure indexed storage, etc., to ensure security of storage environment.

b) It is recommended to support isolation strategies for the data of different users in a multi-tenant environment.

c) It is recommended to formulate security policies and management regulations of data storage, such as access control policy, secure data transmission policy, data integrity policy, multiple copies consistency policy, personal information and essential data encryption policy, etc.

d) It is recommended to support a variety of data desensitization mechanisms.

e) It is recommended to support file system encryption, in order to prevent data corruption and leakage. Additionally it is recommended to support classified encryptions based on the data sensitivity levels: no encryption, partial encryption, complete encryption, etc.

f) It is recommended to provide functions for detecting the damages to storage data integrity and restoring data integrity after the damages occurred.

g) It is recommended to support optional security configuration parameters of encryption for users to choose.

h) It is recommended to support users in the selection of a third-party encryption mechanism to encrypt the key data.

i) It is recommended to support data encryption using secure keys and support storage and maintenance of the secure keys locally.

j) It is recommended to support an appropriate encryption algorithm for long-term storage media backup, such as the use of long encryption keys and planning for replacement with an improved encryption algorithm.

k) It is recommended to define the timeliness and rights of data sharing, data usage authorization and data deletion.

l) It is recommended to authorize the validity period of data usage and notify associated big data providers and users.

m) It is recommended to support the data deletion, backup, and recovery functions.

7.2 Security guidelines for processing layer

Security guidelines for processing layer focus on data aggregation security and data analysing security.

7.2.1 Security guidelines for data aggregation

Security guidelines for data aggregation include the following:

a) It is recommended for the data aggregation components to support an authentication mechanism, and the terminal of data source and operators of the big data platform is recommended to be authenticated and authorized.

b) It is recommended to implement strict security regulations in the data aggregation process, which includes classification, transmission, and temporary storage.

c) It is recommended for various data sources to establish a data classification strategy with a corresponding security management policy, which should cover the process of transmission and temporary storage. For each class of data source, the corresponding security management policy is recommended to be defined by the confidentiality, integrity, and availability.

d) It is recommended to support restricted access control functions to access of a temporary storage folder in the data aggregation process, so that the access of unwanted processes or users' data, unauthorized modification to the storage address of data aggregation components could be prohibited.

e) It is recommended to provide the load balance functions for data aggregation components, so that the load pressure of large data flow could be relieved by multiple channels.

f) It is recommended to provide detection and protection functions such as IPS/IDC for data aggregation components, so that the restrictions on the excessive or unwanted collection of data could be made.

g) It is recommended to provide the failover and recovery mechanisms for data aggregation components, so that the data flows being transmitted could be switched over to a standby component.

h) It is recommended to provide logging for data aggregation and give alarms for abnormal situations including where: data were collected repeatedly, data flows were larger than the set threshold, data flows were interrupted or the amount of collected data storage exceeded.

7.2.2 Security guidelines for data analysing

Security guidelines for data analysing include the following:

a) It is recommended to provide authentication methods to ensure that only legitimate users or applications could initiate data analysing requests.

b) It is recommended to implement an access control module for data analysing according to the big data user identification policy and user authentication policy, including the management and validation of access control timeliness, and the validation mechanism of the legality of accessing data.

c) It is recommended to support a security audit of analysing distributed data, and for which the audit information is recommended to be stored and controlled protectively.

d) It is recommended to provide a desensitization mechanism to maintain security and robustness of data analysing, and the business continuity is recommended to not be affected. Additionally, the system performance is recommended to not be greatly affected after the use of the desensitization mechanism.

e) It is recommended to be able to set different desensitization mechanisms according to different users' demands and different data.

f) It is recommended to support configuration of the desensitization algorithm after users are queried or demanded.

g) It is recommended that the desensitization mechanisms could be dynamically added or deleted, which could support the system's smooth upgrading without a business interruption.

7.3 Security guidelines for application layer

Security guidelines for application layer focus on application system and application audit.

7.3.1 Security guidelines for application system

Security guidelines for application system include the following:

a) It is recommended to provide detection and protecting methods for application system, such as firewall, antivirus system, and IDS/IPS.

b) It is recommended to implement defences against the vulnerabilities of application system.

c) It is recommended to provide authentication methods to prevent unauthorized access to application system.

d) It is recommended to maintain isolation between different applications, to avoid data leakage caused by data association analysis initiated by different applications.

7.3.2 Security guidelines for application audit

Security guidelines for application audit include the following:

a) It is recommended to audit administrators' operations of applications, which could trace events and extract evidences for security incidents.

b) It is recommended to audit users' operations of application to enable detecting, alerting and quick responding to malicious behaviours.

c) It is recommended to audit modification of security configuration parameters about alerting, quick responding to malicious behaviours, etc.

7.4 Security guidelines for access layer

Security guidelines for access layer focus on authentication mechanism and application programming interface (API).

7.4.1 Security guidelines for authentication mechanism

Security guidelines for authentication mechanism include the following:

a) It is recommended to support enhanced authentication services, such as single sign-on (SSO) authentication, multi-factor authentication, etc.

b) It is recommended to enforce strong password policies, such as increasing the complexity of passwords, updating passwords regularly, etc.

c) It is recommended to support the whitelist authentication mechanism, such as IP address whitelisting, etc.

7.4.2 Security guidelines for API

Security guidelines for API include the following:

a) It is recommended to enable administrators to authorize access for APIs, such as being able to configure maximum times that a user could access APIs, total number of connections that APIs could support, etc.

b) It is recommended to support real-time monitoring characteristics of network flows between clients and API interfaces, generate alerts and enable incident response for abnormal network traffic.

c) It is recommended to validate APIs' input to prevent various security attacks.

d) It is recommended to support transferring essential data over a secure channel, such as via an encrypted channel, etc.

e) It is recommended to enforce examination and desensitization bi-directionally between clients and APIs before data is transferred.

f) It is recommended to support data integrity checking and detect data corruption or loss during transmissions.

7.5 Security guidelines for security management

Security guidelines for security management include the following:

a) It is recommended to use identity and access management (IAM) and access control audit, including operation and maintenance records, data access logs, access behaviour inspection, key management, and data encryption.

b) It is recommended to use rational and effective detection and protection mechanisms including security redundancy of infrastructure, vulnerability scanning, IPS/IDS, firewalls, and virtualization security devices.

c) It is recommended to use security reinforcement techniques to reduce the attack surface of infrastructure and platform.

d) It is recommended to upgrade patches and versions regularly for big data infrastructure and platform.

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[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.1158] Recommendation ITU-T X.1158 (2014), *Multi-factor authentication mechanisms using a mobile device*.

[b-ITU-T X.1217] Recommendation ITU-T X.1217 (2021), *Guidelines for applying threat intelligence in telecommunication network operation*.

[b-ITU-T X.1245] Recommendation ITU-T X.1245 (2010), *Framework for countering spam in IP-based multimedia applications*.

[b-ITU-T X.1361] Recommendation ITU-T X.1361 (2018), *Security framework for the Internet of things based on the gateway model*.

[b-ITU-T X.1524] Recommendation ITU-T X.1524 (2012), *Common weakness enumeration*.

[b-ITU-T X.1631] Recommendation ITU-T X.1631 (2015), *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

[b-ITU-T Y.2052] Recommendation ITU-T Y.2052 (2008), *Framework of multi-homing in IPv6-based NGN*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

[b-ITU-T Y.2244] Recommendation ITU-T Y.2244 (2019), *Service model for a cultivation plan service at the pre-production stage*.

[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 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[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.*

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, 2022