International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1751
(09/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY
Data security – Big Data Security

Security guidelines for big data lifecycle management by telecommunication operators

Recommendation ITU-T X.1751

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
Distributed ledger technology security	X.1430–X.1449
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
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**
5G SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1751

Security guidelines for big data lifecycle management by telecommunication operators

Summary

Recommendation ITU-T X.1751 analyses security vulnerabilities and establishes security guidelines for big data lifecycle management by telecommunication operators.

With rapid development of big data technology, the value of data has substantially increased. Big data bring new opportunities to telecommunication services. Previously, data were siloed and managed independently in different telecommunication service systems. Data aggregation and fusion trends are inevitable with the construction of big data services. In the process of data fusion convergence, data flow on platforms and in-service processes. Data face various security vulnerabilities at different stages of their lifecycle.

Recommendation ITU-T X.1751 introduces specific characteristics of telecommunication big data services and data categories, analyses security vulnerabilities of big data lifecycle management and specifies security guidelines for telecommunication operators.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1751	2020-09-03	17	11.1002/1000/14267

Keywords

Data lifecycle management, telecommunication big data services.

* 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

Recommendation ITU-T X.1751

Security guidelines for big data lifecycle management by telecommunication operators

1 Scope

This Recommendation describes security vulnerabilities and establishes lifecycle management guidelines for telecommunication big data services. This Recommendation:

– introduces characteristics of telecommunication big data services and data categories;

– analyses security vulnerabilities of lifecycle management for telecommunication big data services;

– specifies security guidelines for data lifecycle management for telecommunication big data services.

When telecommunication operators provide big data services, the basic prerequisite is that the explicit consent of subscribers has been obtained. In addition, for telecommunication operators, provision of necessary data protection measures is recommended throughout the entire big data service process.

Protection mechanisms for various data categories lie outside the scope of this Recommendation.

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 Recommendationn.

[ITU-T X.1641]	Recommendation ITU-T X.1641 (2016), *Guidelines for cloud service customer data security*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 big data [b-ITU-T Y.3600]: A paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics.

3.1.2 big data as a service (BDaaS) [b-ITU-T Y.3600]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to collect, store, analyse, visualize and manage data using big data.

3.1.3 linkability [b-ISO/IEC 20889]: Property for a dataset that it is possible to associate (by linking) a record concerning a data principal with a record concerning the same data principal in a separate dataset.

3.1.4 pseudonymization [b-ISO/IEC 29100]: Process applied to personally identifiable information (PII) which replaces identifying information with an alias.

3.1.5 security policy [b-ITU-T X.800]: The set of criteria for the provision of security services.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 data lifecycle: The entire survival process after data are generated, including data collection, data transmission, data storage, data usage (covering data analysis and visualization), data sharing and data destruction.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2B	to Business
2C	to Consumer
API	Application Programming Interface
APP	Application
BDaaS	Big Data as a Service
BSS/OSS	Business Support System and Operation Support System
DB	Database
FTP	File Transfer Protocol
HDFS	Hadoop Distributed File System
IoT	Internet of Things
IP	Internet Protocol
JDBC	Java Database Connectivity
LBS	Location-Based Service
LDAP	Lightweight Directory Access Protocol
MPP	Massive Parallel Processor
OSS	Operation Support System
PII	Personally Identifiable Information
REST	Representational State Transfer

5 Conventions

In this Recommendation:

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

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

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

The phrase "**can optionally**" indicates an optional requirement that 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 or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Overview

With its rapid development, the value of big data has substantially increased. Big data bring new opportunities to telecommunication operators, who have held for a long time different kinds of data resources, such as call, location, personal data, mobile consumer data and terminal data, in what have been called data warehouse systems. With the rapid generation of big data, telecommunication operators are constantly innovating and investing in big data service development.

Telecommunication big data services involve terabyte or even petabyte amounts of information. Data generated are of a variety of types, such as structured, semi-structured and unstructured. The sources include private data, such as PII, and access log data. Such data can be targeted by attackers.

Previously, data were separated and managed independently in different telecommunication service systems. In addition, these systems could be situated at various locations and managed by different departments. With big data service development, telecommunication operators are breaking down departmental barriers and collecting data from various separate systems. Data convergence greatly enhances the value of big data services.

In a big data service process, data flow through the big data platform and go through various lifecycle stages, at each of which information faces various security threats and risks. For example, improper data collection can lead to inappropriate information disclosure. Unauthorized access can occur at the data storage stage. Use of sensitive data can create the risk of data leakage when information is shared. Therefore, it is necessary to analyse security vulnerabilities and specify lifecycle management security guidelines for telecommunication big data services.

This Recommendation analyses security risks and specifies lifecycle management security guidelines for telecommunication big data.

7 Characteristics of telecommunication big data services and data categories

7.1 Characteristics of telecommunication big data services

More and more telecommunication operators are taking big data services as an important strategic direction for their companies' innovation and development. For example, by building big data capability platforms or setting up specialized operation teams, telecommunication operators can develop big data services.

Telecommunication operators can collect a vast range of customer data related to an individual user, such as user profile, devices, usage and location. Telecommunication operators can use big data analytical techniques to take advantage of these data to develop services related to a wide variety of applications, e.g., retail, healthcare and smart cities. Telecommunication operators can use these services to enhance their own businesses or market them to third party service providers in other business sectors.

However, the breadth and types of data that telecommunication operators use for these big data services can reveal a staggering amount of detail about individuals, includingPII, sensitive data, e.g., religious beliefs or political affiliations, and trade secrets. This consideration is especially important if telecommunication operators choose to share these data with third parties. It is therefore essential that telecommunication operators recognize threats in the data lifecycle of their big data services and take security measures to protect their users.

7.2 Data categories

There are four principal categories of user data, listed in the next paragraph, in the hands of telecommunication operators. In addition, with the development of the Internet of things (IoT) and its services, the depth and breadth of data are being further expanded. This expansion results in new risks to user confidence and security that must be addressed by telecommunication operators concerning:

1) data generated from a telecommunication operator's business support system and operation support system (BSS/OSS), which consist of user identity, length of call, call target, communication bill, service types and even the type of terminal;

2) data generated from telecommunication operator's operation support system (OSS), which are mainly user behaviour data, including that generated through the mobile Internet, chatting, playing games and surfing the web;

3) data based on a user's location-based service (LBS) information, which, unlike categories 1) and 2), are closely related to the user's actual location and can be used for business marketing, population mobility, public safety and urban planning;

4) data to business (2B) or to consumer (2C) generated in the IoT scenario that consist of big data about both "things" and "people" – these data are of great value in healthcare, wearable device and smart home areas.

Big data about things include: water, electricity and gas readings collected from meters; climate and pollution data collected by sensors; and tracking data on asset shipments.

Big data about people include: data about health; personal finances; and purchase history.

Note that the linkability of certain data can yield greater implications about users than expected, based on how the data are initially categorized; e.g., anonymized category 4) data that are analysed in conjunction with other data may nevertheless make individuals identifiable, as PII of category 1). Therefore, linkability is recommended to be a key consideration when determining how to secure data, even in cases where the data are not immediately categorized as PII or other personal data.

In this Recommendation, securization of data in these four categories is recommended at all data lifecycle stages by security guidelines.

8 Lifecycle of data in telecommunication big data services

The data lifecycle of telecommunication big data services consists of six main stages: data collection; data transmission; data storage; data usage; data sharing; and data destruction. The data transmission stage can involve several stages.

The lifecycle of data in telecommunication big data services is illustrated in Figure 1.

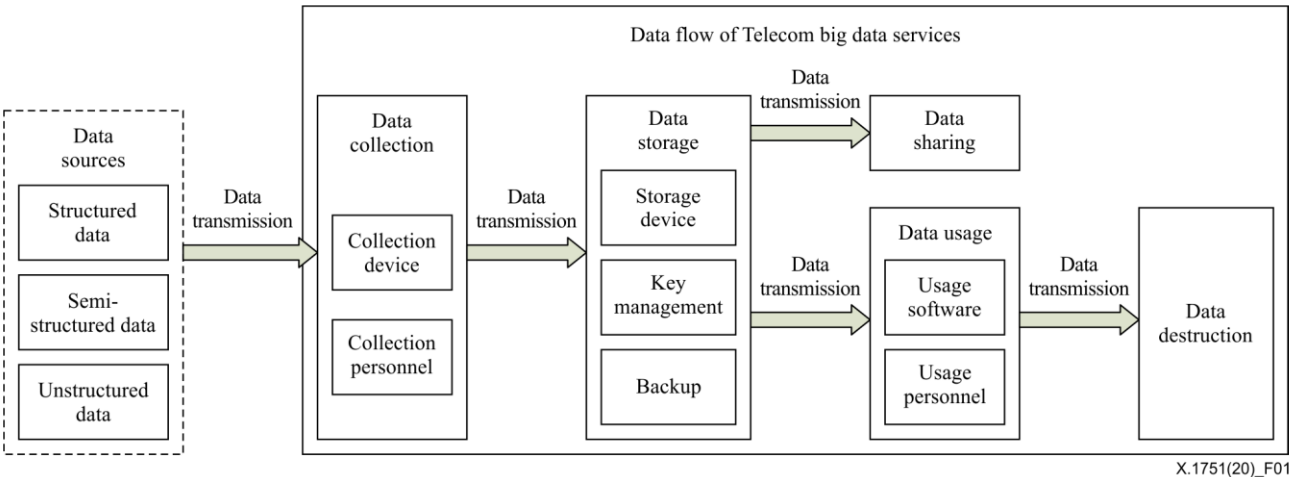

Figure 1 – Data lifecycle of telecommunication big data services

In the lifecycle of telecommunication big data services, data collection is the beginning and data destruction is the end. After collection, data can be transmitted, stored, used and shared. Data transmission can occur between different stages, e.g., after collection, data can be transmitted to specialized storage devices; during usage, data can be transmitted from storage devices to usage software or entity; after usage, expired or useless data require destruction.

Data collection: With specialized data collection devices or entities, different types and categories of data are collected into a specific directory or temporary directory for storage.

Data transmission: This process involves data transfer from a collection device to a storage device and from storage to usage and sharing. Sometimes the data destruction stage also involves data transmission.

Data storage: Data are stored in dedicated devices, e.g., databases (DBs), distributed file systems and disk arrays. Encryption and data backup are also necessary for important data.

Data usage: Data analysis software and applications access and process data to provide various big data services. Various personal sensitive data can be involved in this process.

Data sharing: The data service provider or data owner shares its own data analysis processing results or even the source data with other providers or third parties.

Data destruction: Expired data, especially those in devices that store important or sensitive information, require complete destruction by a security mechanism dedicated to the purpose.

9 Security vulnerabilities in data lifecycle of telecommunication big data services

In the process of telecommunication big data services, data flow in every step of the service. The security vulnerabilities can arise from inside or outside the process. Inner security vulnerabilities are related to devices and systems, such as collection devices, storage devices and usage devices. Outside security vulnerabilities occur because of misconfiguration or misuse. Descriptions of data-related vulnerabilities can be found in [b-ITU-T X.1040].

9.1 Data collection stage

9.1.1 Security vulnerability of device and system

The device and systems are vulnerable or infected by viruses or trojans, causing security problems.

9.1.2 Security vulnerability of configuration and management

1) Personnel management

Data collection devices can be improperly operated or used without authorization, resulting in the risk of data leakage.

2) Device management

Malicious or erroneous configuration of collection devices can lead to unauthorized collection and data leakage.

Data accumulate from a number of different business systems that are situated in various locations and managed by different departments. A malicious node can break into the device cluster to perform unauthorized data collection operations.

3) Data management

Data not related to the stated purpose of use is over-collected, and this may result in data leakage.

During the collection stage, a temporary data storage area, such as a random path of a file transfer protocol (FTP) server, is uncontrolled by collection personnel and increases the risk of data disclosure or unauthorized alteration.

9.2 Data transmission stage

9.2.1 Security vulnerability of configuration and management

1) Personnel management

The administrator modifies the transmission port or transmission configuration without authorization, which may cause data leakage.

2) Device management

Collected data are transmitted over an insecure channel, which leaves data susceptible to eavesdropping, or alteration.

The transmission interface is not authenticated therefore a misconnection or malicious connection occurs.

A transmission mechanism between different nodes does not protect the confidentiality and integrity of the data, which results in data leaks and increases the risk of alteration, eavesdropping and interception.

3) Data management

Lack of confidentiality protection during data transmission may result in data being intercepted or data leakage.

Lack of integrity protection during data transmission may result in malicious manipulation or damage of data.

Lack of availability protection during transmission may result in data being intercepted or tampered with.

9.3 Data storage stage

9.3.1 Security vulnerability of device and system

Deploying no anti-virus software or an expired security software results in the disclosure and poisoning of sensitive data.

A misconfigured or unmaintained security software leaves data unprotected, which can lead to disclosure, poisoning and adversarial attacks on datasets.

9.3.2 Security vulnerability of configuration and management

1) Personnel management

Access control measures are improperly configured so that stored data are exposed to the risk of unauthorized access or alteration. Individuals that are authorized to access certain stored datasets are able to infer PII or other personal data that they are unauthorized to access, due to linkability.

2) Device management

A relational DB, Hadoop distributed file system (HDFS) and massive parallel processor (MPP) data warehouse coexist in a storage environment. Poor permission management causes unauthorized access and data disclosure.

Many unstructured data are stored in different nodes separately, which makes it difficult to enforce the same security policy. Inconsistent security policies or conflicts can result in lack of security protection and data leakage.

3) Data management

Stored data are not encrypted, whether in full or in part, which increases the exposure of users in the event of a passive or active data breach.

Stored data are encrypted; however, vulnerabilities related to the encryption algorithm or key management increase the risk of unauthorized access to or alteration of stored data.

The integrity of data is not actively protected while it is stored, which exposes the data to unauthorized modification even after it has been collected.

Stored data includes data that is outdated or not directly relevant and necessary to the stated purpose of use. As the number of stored data increases, so does user exposure in the event of any passive or active data breach.

Incomplete data backup and recovery mechanisms may result in data not being available.

9.4 Data usage stage

9.4.1 Security vulnerability of device and system

Data analysis software that is networked or cloud based has vulnerabilities that put data exposed to the software at risk.

The visualization application of data analysis software has security issues that can be exploited by attackers.

9.4.2 Security vulnerability of configuration and management

1) Personnel management

If there is a lack of authentication and authorization capabilities for users or visualization applications, then a fake user or visualization application can obtain visual data, resulting in data leakage.

2) Device management

A lack of identity authentication for data usage devices results in an unauthorized device joining the big data platform. As a consequence, data leakage or unavailability to business occur.

3) Data management

When used by visualization applications, personal data, including any PII and sensitive data, are not properly anonymized or masked and increase the potential for identifiability.

Visualized data are highly linkable, which increases the potential for inferring identity or other personal data.

Output data that result from data analysis processes are not stored in a secure environment, or output data that are outdated or not directly relevant or necessary to the purpose of use are retained. As the number of retained data increase, so does user exposure in the event of any passive or active data breach.

Data logs that are produced during this stage are not securely stored, which may be used to infer personal data in the event of a data breach.

9.5 Data sharing stage

9.5.1 Security vulnerability of device and system

The data sharing device and system are vulnerable or infected by viruses or trojans, causing security problems.

9.5.2 Security vulnerability of configuration and management

1) Personnel management

Security responsibilities and abilities of users of shared data are inadequately specified, resulting in improper data protection and data leakage.

2) Device management

The scope and boundaries of data sharing are not clear; in addition, there is a lack of security control measures, which leads to sensitive data being directly exposed to partners.

A data-sharing channel lacks security protection, giving rise to disclosure or tampering with important data.

3) Data management

Data-sharing log records are incomplete, making it difficult to determine the cause once a security incident occurs.

9.6 Data destruction stage

At the end of this stage, if the data have not been completely destroyed, sensitive data can be recovered by malicious personnel, resulting in data leakage.

9.7 Relationship of security vulnerability to data lifecycle

Security vulnerabilities appear at different lifecycle stages of a big data service. An overview of the relationship between security vulnerability and the data lifecycle of a big data service is shown in Table 1.

In Table 1, the letter "Y" (Yes) in a cell indicates that the security vulnerability exists at that stage.

Table 1 – Relationship between security vulnerability and data lifecycle stage

Vulnerability		**Lifecycle stage**					
		Data collection	**Data transmission**	**Data storage**	**Data usage**	**Data sharing**	**Data destruction**
Device vulnerability		Y		Y	Y	Y	
Configuration and management vulnerability	Personnel management	Y	Y	Y	Y	Y	
	Device management	Y	Y	Y	Y	Y	
	Data management	Y	Y	Y	Y	Y	Y

10 Security guidelines for data lifecycle of telecommunication big data services

This Recommendation describes detailed mechanisms, which are suitable for all data categories described in clause 7.2.

10.1 Data collection stage

10.1.1 Security guidelines for device and system

The software on the device and system used for data collection are required to be up to date and to have no public vulnerabilities.

The device and system used for data collection requires installation of security software, such as that against viruses and malware, compatible with the device operating system.

10.1.2 Security guidelines for configuration and management

1) Personnel management

Users are recommended to be informed about which data are being collected and why, and the explicit consent of users obtained before collection begins.

When performing data collection, authentication and authorization of collection personnel are necessary.

2) Device management

Specification of security mechanisms and countermeasures for data collection is recommended, e.g., for strict authentication and authorization of collection devices. The data category is recommended to comply with collection principles.

The set-up of a big data service is required to fulfil the intended service purpose. Determination of the data that are strictly relevant and necessary for collection to fulfil the purpose of use is required.

The data collection device, collection channels, data formats, collection processes and collection methods require specification.

Enforcement of access authentication of the collection device and collection personnel is required; provision of detection and warning of abnormal collection behaviour is required.

The temporary data storage area requires strict restriction, such as prohibition of unauthorized data export from such areas to other storage resources, and authorization of the modification of the storage area is recommended.

Protection of the transmission of collected data, including metadata, using encryption algorithms that are widely used and tested by trusted third parties is recommended.

Securely manage and store encryption keys and, wherever possible, give preference to cryptographic protocols that feature forward secrecy.

3) Data management

According to its importance and sensitivity, determination of the various classifications of data collected is recommended.

Log records and warning of the following abnormal behaviour is required when:

- repeated collection and transmission exceeds the set threshold;
- transmission is interrupted during the collection process;
- the set threshold of storage capacity is exceeded.

10.2 Data transmission stage

10.2.1 Security guidelines for configuration and management

1) Personnel management

Prevent administrators from modifying the transmission port or interface configuration parameters arbitrarily.

2) Device management

Data transmission via an end-to-end encrypted channel is required.

The transport interface provides authentication capabilities to prevent malicious connections from occurring.

3) Data management

Implementation of confidentiality and integrity protection of data is recommended during the data transmission stage.

Prompt detection of damage to data integrity is recommended during transmission; implementation of necessary measures is recommended to restore it after errors are detected.

10.3 Data storage stage

10.3.1 Security guidelines for device and system

The software on the storage device and system is required to be up to date and to have no public vulnerabilities.

The storage device requires installation of up-to-date security software.

10.3.2 Security guidelines for configuration and management

1) Personnel management

Implementation of access control for user or application is required, such as the secret-key network authentication protocol, Kerberos, and fine-grained authorization.

Integration of important data operations into the multi-person operation vault control mode is recommended, so that a single person cannot have full operational authority for important data, such as its batch output, copying, destruction, publication and usage.

2) Device management

Authorization methods must restrict access to individuals who are essential to the performance of the stated purpose of use for which data are collected. Permissions must be set to prevent individuals from accessing more data than is absolutely necessary for performance of their specific duties and to take into account the potential for the inference of personal data arising from linkability between any stored datasets and separate permissions between individuals.

3) Data management

a) Data minimization

Restriction of the storage of data, including outputs of processes carried out during the data usage stage, is recommended, so that only data that are relevant and necessary for the stated purpose of use are retained.

The setting of clear maximum retention periods is recommended for all data, based on the minimum possible amount of time that data must be retained to fulfil their stated purpose of use.

b) Data encrypted storage

Encrypted storage is necessary to ensure the confidentiality of important data. Support of a hierarchical data encryption model is recommended; different security storage mechanisms are used according to the data secrecy level.

Use of encryption algorithms that are widely deployed and tested by trusted third parties is recommended. Securely manage and store encryption keys and, wherever possible, employ in preference cryptographic protocols that feature forward secrecy.

c) Data integrity protection

Provision of an integrity detection mechanism is recommended to determine the damage and loss of data due to data storage.

Implementation of necessary measures is recommended to restore data integrity after errors are detected [ITU-T X.1641].

Audit logs that document any alteration to stored data must be maintained. Logs must be securely stored, and capture and reporting of attempts to alter them are recommended.

d) Data backup and recovery

Provision of complete data backup and restore mechanisms is recommended to ensure data usability and integrity.

10.4 Data usage stage

10.4.1 Security guidelines for device and system

The software on the device and system is recommended to be up to date and to have no public vulnerabilities.

The device and system is recommended to have up-to-date security software installed.

10.4.2 Security guidelines for configuration and management

1) Personnel management

Provision of unified authentication is recommended for use by different (data usage) applications to access big data platforms, no matter what kind of interfaces the applications use, such as the resource representational state transfer application programming interface (REST API) and Java database connectivity (JDBC). The detailed authentication mechanism can be Kerberos, the lightweight directory access protocol (LDAP) or others.

Provision of fine-grained authorization is recommended for use by different applications to access big data platforms, including the following methods:

a) fine-grained authorization to access big data platforms by user names, Internet protocol (IP) address and application (APP) names;

b) fine-grained authorization to access storage resources, such as: the data warehouse software, Hive; the open-source non-relational distributed database, Hbase; HDFS; and DBs;

c) fine-grained authorization by different operations of the DB or file system (e.g., SELECT, INSERT and CREATE);

d) fine-grained authorization for data import and export permissions;

e) fine-grained authorization to access the file and directory of HDFS;

2) device management.

Provision of malicious activity monitoring and enforcement mechanisms is recommended at the data usage stage.

Provision of security audit trails is recommended to test for adequacy of data usage, to ensure compliance with established security policy and operational procedures, to aid in damage assessment and to recommend any changes in security controls, security policy and procedures for data usage.

A security audit policy is recommended to consider which information about data usage is required to be logged and under which conditions, as well as the syntactic and semantic specification to be used for the interchange of the security audit information.

3) Data management

In order to protect sensitive data, data pseudonymization is necessary at the data usage stage. Detailed guidelines for data pseudonymization will be unified and considered in the subsequent data sharing stage.

Auditing of utilization of sensitive data is recommended, with audit logs generated as specified in [ITU-T X.1641].

10.5 Data sharing stage

10.5.1 Security guidelines for device and system

The software on the user's device and system is recommended to be up to date and to have no public vulnerabilities.

The device and system is recommended to have up-to-date security software installed.

10.5.2 Security guidelines for configuration and management

1) Personnel management

Users must be informed about which data, including metadata and any data that results as the output of processes carried out during the data usage stage, will be shared with third parties and who these third parties are. Explicit consent must be obtained from the user before sharing any data, including output data.

2) Device management

Control of the behaviour of data export is recommended.

When data are shared with external services, limitation of the usage of data is recommended to avoid data reselling.

Security protection mechanisms are recommended to be negotiated among the relevant stakeholders (e.g., operators between which data are transferred), and to include a security policy for shared data transfer, storage, access, destruction and the backup scheme if shared data are disclosed.

3) Data management

Data pseudonymization is the process of hiding the original PII and sensitive data with characters or data. The purpose is to protect PII and sensitive data.

Different applications can be configured with different pseudonymization algorithms. Data pseudonymization is recommended to:

a) support the addition and removal of pseudonymization algorithms dynamically;

b) support fine-grained pseudonymization, which means pseudonymization can be configured by an administrator to a particular table or columns of a DB;

c) use public algorithms, avoiding third-party proprietary algorithms;

d) not significantly affect business continuity and system performance.

10.6 Data destruction stage

10.6.1 Security guidelines for data management

Data must be both erased and overwritten in the solid state.

After data are deleted, it is recommended that the storage space of resources, e.g., files, directories and DB records, in the system be completely cleared without possibility of restoration.

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.1040] Recommendation ITU-T X.1040 (2017), *Security reference architecture for lifecycle management of e-commerce business data*.

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

[b-ISO/IEC 20889] ISO/IEC 20889:2018, *Privacy enhancing data de-identification terminology and classification of techniques*.

[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, 2020