ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1644 (03/2023)

SERIES X: Data networks, open system communications and security

Cloud computing security – Cloud computing security best practices and guidelines

---

Security guidelines for distributed cloud

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.1644

Security guidelines for distributed cloud

Summary

Recommendation ITU-T X.1644 analyses security threats and challenges on distributed cloud and proposes security guidelines against threats to distributed cloud, which includes the security guidelines for core cloud, regional cloud and edge cloud.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1644	2023-03-03	17	11.1002/1000/15112

Keywords

Cloud computing, distributed cloud, 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.1644

Security guidelines for distributed cloud

1 Scope

This Recommendation analyses security threats to the distributed cloud and provides security guidelines for the distributed cloud.

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.1408] Recommendation ITU-T X.1408 (2021), *Security threats and requirements for data access and sharing based on the distributed ledger technology*.

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

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

[ITU-T Y.3508] Recommendation ITU-T Y.3508 (2019), *Distributed cloud overview and high-level requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud capabilities type [ITU-T Y.3500]: Classification of the functionality provided by a cloud service to the cloud service customer, based on resources used.

NOTE – The cloud capabilities types are application capabilities type, infrastructure capabilities type and platform capabilities type.

3.1.2 cloud computing [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.

3.1.3 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.4 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

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

3.1.5 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.6 edge cloud [ITU-T Y.3508]: A cloud computing deployed to the edge of the network accessed by cloud service customers (CSCs) with small capacity resources enabling cloud service.

NOTE 1 – Enabled cloud service on the edge cloud is lightweight cloud service provided by a cloud service provider (CSP) depending on cloud service category.

NOTE 2 – Lightweight cloud service refers to a portion of cloud service to reconfigure the functionality of cloud service to fit on edge cloud such as base station and gateway with small capacity resource.

3.1.7 threat [ITU-T X.1408]: A potential cause of an unwanted incident, which result in harm to a system or organization.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 core cloud: A centralized set of services that includes all geography-independent services, services that are not latency-sensitive, highly computing intensive services, backup and recovery services, and high security level services of a cloud computing network.

3.2.2 distributed cloud: An extension of classical cloud computing concepts, which extends the cloud computing capabilities further to the edge of the network.

3.2.3 regional cloud: A core cloud that is optionally deployed for efficient configuration between the core cloud and an edge cloud to reduce the load on core cloud.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Service Interface

CC Core Cloud

CSC Cloud Service Customer

CSP Cloud Service Provider

DDoS Distributed Denial of Service

DoS Denial of Service

EC Edge Cloud

IoT Internet of Thing

OTA Over-The-Air

REST Representational State Transfer

TLS Transport Layer Security

VPN Virtual Private Network

XML Extensible Markup Language

XSS Cross Site Scripting

5 Conventions

In this Recommendation:

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

6 Overview

The distributed cloud is emerging because more and more latency-sensitive services (such as video and Internet of Things (IoT) services) require much faster response speeds; it is an extension of traditional cloud computing and extends its capabilities further to the edge of the network. It can provide localized cloud services much closer to the customer as well as to the data source, and can interact with other clouds to provide distributed, low latency, high performance services.

The distributed cloud comprises the distribution of cloud capabilities types to the edge of the network to enable cloud service with low latency and real-time processing on a limited bandwidth by interworking among a pool of physical or virtual resources [ITU-T Y.3508]. A typical distributed cloud is described in Figure 6-1, including the core cloud, regional cloud and edge cloud.

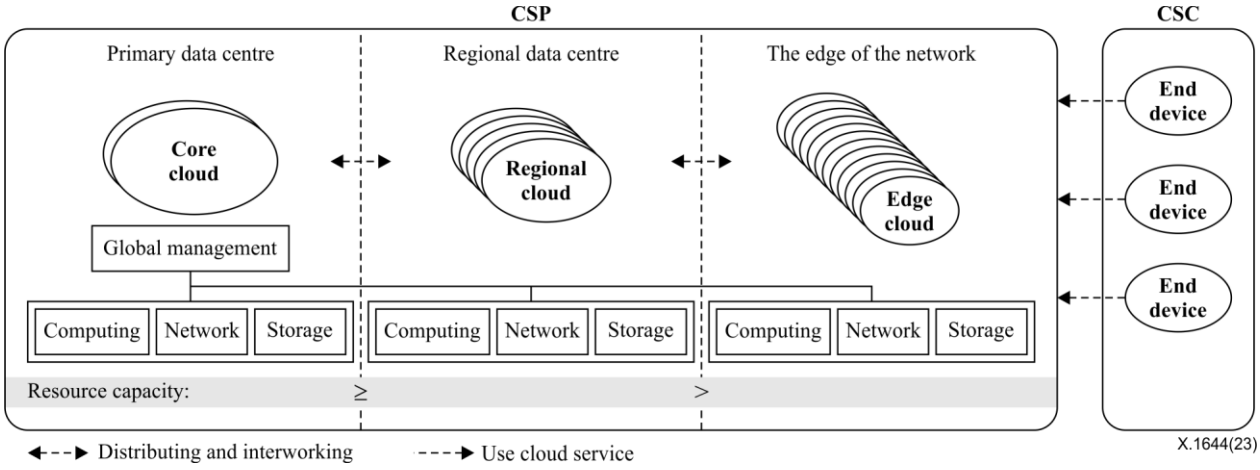

Figure 6-1 – Concept of distributed cloud

The core cloud has a large resource capacity and global management point to control cloud resources in the distributed cloud. The core cloud supports cloud services with high computing intensity and geographic independence.

The regional cloud is optionally deployed in particular regions from the core cloud for load sharing and service quality enhancement. The regional cloud handles cloud service requests from the region controlled by the global management of the core cloud.

NOTE 1 – The regional cloud supports lower latency than the core cloud by executing customized cloud services for cloud service customers (CSCs) in a particular region. It is assumed that the network latency from the CSC to the regional cloud is lower than from the CSC to the core cloud and that the difference of cloud service execution time between the core and regional cloud is negligible.

NOTE 2 – The regional cloud performs buffering for the load of the cloud service and data cacheing from the core cloud, and provides them to CSCs in the region.

The edge cloud is deployed at the edge of the network accessed by CSCs and has a small resource capacity. The edge cloud requires specialized hardware resources on purpose; i.e., the resources in the edge cloud are constrained due to limitations of space or power. The edge cloud may have different configurations of resources and cloud capabilities types with physical and virtual resources depending on a CSC's requirements of cloud services and conditions in the deployment environment.

7 Security challenges and threats to the distributed cloud

The use of a distributed cloud provides advantages in terms of high speed, efficiency and performance. The core cloud, regional cloud and edge cloud in a distributed cloud bring new security challenges and threats [ITU-T X.1601].

7.1 Security challenges and threats to the core cloud

The distributed cloud has infrastructures of different scales with large resource capacity in the core or regional cloud and small resource capacity in the edge cloud. The core cloud utilizes a heterogeneous infrastructure as a single system to provide various services to CSCs in distributed cloud. The security challenges and threats to the core cloud are as follows:

a) **System vulnerabilities:** The distributed cloud infrastructure contains system vulnerabilities, especially in networks that have complex infrastructures and multiple third-party platforms, and a vulnerability in core cloud also affects the regional cloud and the edge cloud.

b) **Physical damage:** The distributed cloud infrastructure may be deployed in untrusted physical environments, and may be physically damaged by malicious users, bad weather or earthquakes. Physical damage to the core cloud may also affect the security of the regional cloud and the edge cloud.

7.2 Security challenges and threats to the regional cloud

a) **Transmission interception:** The core cloud needs to transmit data with regional clouds, and these transmission links may be intercepted.

b) **Counterfeit order or request:** Malicious order or request from a counterfeit core cloud, regional cloud or edge cloud may cause data leakage.

c) **Interface attack:** As a core cloud links with multiple regional clouds through open interfaces, it may be attacked through these interfaces.

d) **Sinkhole attack:** An intruder can compromise a device or introduce a counterfeit device inside the network and then use it to launch a sinkhole attack. A sinkhole attack is a type of network layer attack where a compromised device sends fake routeing information to its neighbour to attract network traffic to itself.

e) **Rogue gateways:** It is easy for an attacker to deploy a rogue gateway. Once a legitimate device is deceived into connecting to a rogue gateway, confidential connection information can be gathered. This will effectively circumvent many security measures in place and may cause radio interference with the official organization installation.

f) **Unauthorized access to IoT gateways:** An attacker may use unauthorized access to IoT gateways, which can cause the disclosure of sensitive information, data modification and illicit use of some resources in the edge cloud.

7.3 Security challenges and threats to the edge cloud

a) **Multi-tenancy issues:** Many cloud solutions do not provide necessary security protection between clients, leading to shared resources, applications and systems. In this situation, threats can originate from other clients within the cloud computing service, and threats targeting one client could also have an impact on other clients.

b) **Counterfeit request:** If a request is proposed from a counterfeit regional cloud or edge cloud, and the core cloud fails to recognize it, it may lead to data leakage and so on.

c) **Cross site scripting (XSS) attack:** A cross site scripting attack can be used to exploit vulnerabilities that exist in websites by injecting malicious codes in clients' machines, and user credentials are impersonated to engage in malicious activities.

d) **Extensible Mark-up Language (XML) wrapping:** XML is the underlying mark-up language that enables origin authentication to the applications in edge cloud. Hackers can launch account hijacking attacks using XML rewriting or signature wrapping techniques.

e) **Employee negligence:** Employee negligence remains one of the biggest security issues for all systems, but the threat to distributed cloud management is particularly acute. Employees

may log into distributed cloud management platforms from their mobile phones, home tablets and home PCs, potentially leaving the system vulnerable to many external threats.

f) **Phishing and social engineering attacks:** Due to the openness of a distributed cloud system, phishing and social engineering attacks have become particularly common. Once login information or other confidential information is acquired, a malicious user can potentially break into the system with ease.

g) **Loss of control:** When an organization's services are put on the distributed cloud, they lose control and awareness of where they can be stored in the cloud. Meanwhile, from the user's perspective, it becomes a serious security issue as the user is unaware of any security mechanism to safeguard their services.

h) **Impersonation of devices:** An attacker may masquerade as a legitimate device, and send fake or malicious data to the edge cloud or steal data from users.

i) **Edge device capture:** There are many end devices near the edge cloud that can collect data, transfer data to the edge cloud and receive results or commands from the edge cloud. An end device can be easily compromised because of its weak security protection.

j) **Distributed-denial-of-service (DDoS) attack:** DDoS attacks against distributed clouds have greatly increased in viability. If enough malicious traffic to a cloud computing system is initiated, the computing system can either crash entirely or experience difficulties. In particular, an edge cloud is a relatively smaller cloud entity with relatively weaker security protection, thus it is more likely to be attacked by hackers and used for DDoS attacking or other illegal activities.

k) **Virtualization security:** Under the edge cloud environment, virtualization security includes implementing security isolation and enhancement for edge gateways, controllers and servers based on virtualization technology. Compared with the core cloud and regional cloud, these edge nodes with limited storage and computing resources face more complex and extensive attack vectors.

8 Security guidelines for the distributed cloud

This clause gives security guidelines related to the core cloud, regional cloud and edge cloud for distributed cloud systems as described in clause 6.

8.1 Security guidelines for the core cloud

Security guidelines for the core cloud consist of guidelines for core cloud system security, physical security, denial-of-service security and edge device security.

8.1.1 Core cloud system security

The guidelines for core cloud system security are as follows:

a) It is recommended to employ vulnerability incident response tools.

b) It is recommended to prevent malware from entering cloud services by using techniques such as file-scanning, application whitelisting, machine learning-based malware detection, and network traffic analysis.

c) It is recommended to review and update risk assessments to include cloud services. Identify and address risk factors introduced by core cloud environments and providers. Risk databases for cloud providers are available to expedite the assessment process.

8.1.2 Physical security

The guidelines for physical security are as follows:

a) It is recommended to build core cloud infrastructure in an appropriate location instead of locations such as airport landing paths, power plants, flood plains, earthquake fault lines or other areas commonly experiencing natural disasters.

b) It is recommended to provide processes for changing, maintaining and monitoring physical environmental conditions for infrastructures built underground.

c) It is recommended to provide cooling systems and compliance standards for infrastructures built underground.

d) It is recommended to limit entry points from the core cloud infrastructure to decrease the risk of physical break-ins.

e) It is recommended to provide multiple check points throughout the core cloud infrastructure to minimize the risk of malicious intruders gaining access.

f) It is recommended for a surveillance monitoring system to provide additional physical security.

g) It is recommended for redundancy to help core cloud infrastructure weather any incident with minimal downtime.

8.1.3 Anti denial of service

The guidelines for denial of service are as follows:

a) It is recommended for core cloud server capacity to handle heavy traffic spikes and have the mitigation tools needed to address security problems.

b) It is recommended to update and patch the firewalls and network security program regularly.

8.2 Security guidelines for the regional cloud

Security guidelines for the regional cloud consist of guidelines for transmitted data and static data security, open interface security and IoT gateway security.

8.2.1 Transmitted data and static data security

The regional cloud provides partial or complete core cloud services for a certain geographical region. The security guidelines of transmitted data and static data in regional cloud include the following:

a) It is required that the regional cloud uses encryption with a certain strength to encrypt communications and data. It is also recommended that secure transmission protocol services be supported to avoid protocol-based attacks from undermining confidentiality.

b) It is required that the regional cloud authenticate and identify service identities, and strict security isolation and access control strategies to be adopted. It is required to support the customization and management of access control strategies.

c) It is recommended that the regional cloud support a secure data exchange system, to achieve real-time monitoring and control of data format, content and flow, and so on.

d) It is recommended that the secure data exchange system meet various elastic requirements in the cloud environment, including providing flexible deployment methods, flexible resource scheduling modes, and secure data exchange methods based on business-based strong security isolation, and so on.

e) It is recommended that the regional cloud support malicious code detection and removal of transmitted data.

f) It is required to adopt encryption and verification mechanisms to ensure the integrity and confidentiality of local storage, including system management data (such as index files, cloud service information and keys), authentication information and important business data (such as user privacy data).

g) It is recommended to support role-based identity authentication for data accessing, and adopt strict access control measures against illegal access.

8.2.2 Open interface security

The cloud service provider (CSP) needs to provide network interfaces and application programming interfaces (APIs) to be able to configure, manage, coordinate and monitor various cloud services, and also to provide services directly. Third parties usually develop to provide additional services on the basis of these interfaces. The guidelines for secure APIs of the regional cloud are as follows:

a) It is required to use encryption such as transport layer security (TLS) or other encryption methods for a Representational State Transfer (REST) API to encrypt data during transmission and prevent tampering. It is also required to use a signature mechanism to ensure only users with access rights can decrypt and modify data.

b) It is recommended to establish trusted identities of APIs through tokens, and then for only the trusted identity with the token to be able to access and control services and data resources and so on.

c) It is recommended to conduct real-time monitoring and issue warnings of the calling behaviours of the open API interface and abnormal data transmission, such as restricting the access frequency of the API interface.

d) It is recommended to actively identify vulnerabilities of APIs. Detection tools might be used to detect API security and data leakage, and track whether APIs have been attacked and if any vulnerability is being exploited in real-time.

e) It is recommended to use API security gateways as the API security gateway has been used as a key technology to protect API security. Since the API security gateway can be used to control and manage the use of API interfaces, it can also authenticate users that use API interfaces and services.

8.2.3 IoT gateway security

IoT devices connect to the Internet via IoT gateways, which becomes the primary targets of malware and network attacks. The security guidelines for IoT gateways are as follows:

a) It is recommended that IoT gateways support device authentication and access control; only authorized users and devices are allowed access and implement secure storage or vaults in order to protect confidential information such as keys and certificates.

b) It is recommended that IoT gateways support policy management to configure access rights and control the device's access to application services (technical services, business services, data services), files (configuration files, log files, mirror files) and other objects according to security policies, and the gateway be able to interrupt illegal connections and sessions in time.

c) It is recommended that IoT gateways enable over-the-air (OTA) update to ensure that the gateway runs the latest software and firmware, avoiding common vulnerabilities and risks. Secure boot can ensure that the gateway is booted with a firmware image whose integrity and authenticity have been encrypted and verified, preventing the use of malicious firmware to boot the gateway.

d) It is recommended that IoT gateways support various security control measures to protect IoT devices. For example, when an IoT gateway is used as a security proxy for networks and devices, it is recommended that firewalls, rule-based traffic filtering and whitelist functions to be implemented in the gateway.

e) It is recommended that IoT gateways support fine-grained event logs, to have a deeper understanding of the processes running in the gateway for security audits.

8.3 Security guidelines for the edge cloud

Security guidelines for edge cloud consist of guidelines for edge cloud infrastructure security, transmitted data and static data edge cloud network security, web security and security of end devices near the edge cloud.

8.3.1 Edge cloud infrastructure security

Edge cloud infrastructure provides both hardware and software foundations, and edge infrastructure security is a fundamental requirement of the edge cloud. The security guidelines for edge cloud infrastructure are as follows:

a) It is recommended to provide a lightweight hardware-independent virtualization framework and implement security isolation and enhancement mechanisms.

b) It is recommended to enhance the security protection of the hypervisor itself and to reduce attack vectors.

c) It is recommended to cooperate with edge cloud servers and provide OS malicious code detection and prevention, strong security isolation of applications, support trusted execution environment and other key mechanisms, to ensure the confidentiality and integrity of various applications running on the OS, which suffer from limited computing or storage resources, and security policies and mechanisms may not synchronize in time with the core or regional cloud.

d) It is recommended that edge cloud providers implement processes of identification and authentication automatically, transparently and in a lightweight manner. Because edge nodes and dynamic network structure of distributed cloud may result in repeating identification and authentication.

8.3.2 Edge cloud network security

Due to the large number of edge nodes and the complex network topology, which increases attack paths, attackers may easily send malicious network packets to edge cloud nodes or launch denial of service attacks, which affect the reliability of the edge cloud network. The security guidelines for edge cloud network are as follows:

a) It is recommended to ensure protocol security in both design and implementation stages, which the edge cloud uses to satisfy different data transmission requirements for CSCs.

b) It is recommended to add additional security policies for potential vulnerable protocols, for example, by implementing data transmission through virtual private network (VPN), TLS or other secure channels by adding modules in gateways.

c) It is recommended to perform integrity and security verifications for network transmission between virtual machines that belong to different domains, to ensure effective insolation between different business communication units. Further, isolation modules can be scheduled by controllers in the visualized environment to provide isolation capabilities.

d) It is recommended to perform security monitoring on network traffic to alarm security events in time and perform incident responses efficiently. Additionally, protection systems can directly block malicious traffic.

8.3.3 Edge cloud web security

Guidelines for web security are as follows:

a) It is recommended to ensure effective remote monitoring of the facilities of an edge cloud system.

b) It is recommended that edge cloud security is accompanied by extensive education efforts. Employees are informed what they can and what they cannot do with their devices as well as helped to identify security risks.

c) It is recommended to ensure that older, outdated devices are not situated alongside more sophisticated ones to reduce vulnerability points within the network.

8.3.4 Security of end devices in the edge cloud

Guidelines for the security of end devices in the edge cloud are as follows:

a) It is recommended to block access when a personal, unauthorized device tries to access edge cloud data.

b) It is recommended to configure edge with capabilities that include features such as strong authentication and encrypted authentication nodes.

c) It is recommended that IT security protocols manage what devices can access the edge cloud system network and under what conditions.

d) It is recommended to implement and continuously monitor the edge cloud environment.

e) It is recommended to assume that edge devices is already compromised rather than automatically trusting the information coming from a device, all data may be malicious unless proven otherwise.

f) It is recommended that only authenticated edge devices can connect and transmit data to the core cloud.

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

Published in Switzerland
Geneva, 2023