Question 8/17 – Cloud computing and big data infrastructure security

(Continuation of Question 8/17)

1 Motivation

Cloud computing is a model for enabling service user's ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud computing model is defined by five essential characteristics (on-demand, delivery over a broad network access, resource pooling, rapid elasticity, self and measured services), five cloud computing service categories, i.e., Software as a Service (SaaS), Communication as a Service (CaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Network as a Service (NaaS), different deployment models (public, private, hybrid…), and flexible extension of service delivery types (core, regional, edge…). The advent of the cloud computing approach as the preferred vehicle for discovering, externalizing, composing, service re-use within workflows, applications, communication enabled applications places new emphasis on the need for security.

Forecasted benefits of cloud computing include flexible and dynamic resource provisioning, and simpler and automated administration of IT infrastructure. Virtualization makes possible to share of nearly unlimited resources, with scalability improvements and massive cost reductions for infrastructure management. The introduction of edge computing enables distribution of cloud capabilities to the edge of the network. This introduces cloud service implementations which have low and deterministic latency and high reliability. However, open systems, shared resources, and inherent interworking of cloud and edge raise many concerns about security, which is perhaps the most important barrier to the adoption of cloud computing. Moving to the cloud implies to shifting from safe, traditional, in-house IT systems to unsafe, "cloudified", open infrastructures. It thus requires in-depth rethinking of security.

Cloud computing was considered for several years as service-centric IT and controlled by Internet players. However, telecommunication players have an important role to play in the emerging cloud computing market and ecosystem. As cloud services are delivered through telecommunication networks, telecommunication players should guarantee a high assurance level. Strong but flexible security protection will be a key enabler for the whole cloud market and ecosystem. Especially when edge computing provides more local distribution of cloud resources. This leads to more complicated relationships between implementations of edge, regional and core implementations of the cloud.

In addition, the flexible use of rich resources in cloud computing environments will enable new security services that the current premise defences cannot provide (e.g. anti-malware services as a cloud service).

Big Data is considered as the technologies, the set of tools, the data and the analytics used in processing large amount of data. Furthermore, as data grow exponentially and become a key asset of telecommunication/ICT networks, massive datasets are analysed with the support of cloud computing to reveal patterns and relationships that would otherwise remain hidden. The core processes of big data such as data collection, storage, analysis, management and visualization are achieved on the basis of cloud computing, without which big data cannot be rapidly transferred and analysed using traditional technologies (e.g. Big Data as a Service). Thus, there is need to examine what kind of security measures cloud computing can offer in the near future.

Recommendations ITU-T X.1601, X.1602, and X.1631 provide a set of Recommendations on security service for cloud security overview, architecture, and framework, cross-layers cloud security and specific security of network services. Currently there is a strong need for securing cloud computing enabled critical voice, multi-media, identity-based services, information assurance

services, identity and data services, and emergency-based services. This Question is intended to develop new Recommendations based on the Focus Group Cloud Technical Report Part 5 for:

– best practices and guidelines development to guide on how to provide security in a cloud computing-based environment;

– responsibility clarification, and security requirements and threats definition for the main actors and related roles in the cloud computing ecosystem;

– security architecture based on the reference architecture provided by Q18/13;

– security management and audit technologies for the trust management.

Question 8/17 will collaborate with related Questions such as Qs 2/17, 3/17, 4/17, 7/17, 10/17 and 11/17 to develop Recommendations on cloud computing security.

Recommendations and Technical Reports under responsibility of this Question as of 7 January 2022: X.1601, X.1602, X.1603, X.1604, X.1605, X.1606, X.1631, X.1641, X.1642, X.1643, X.1750, X.1751, X.1752, and Technical Report TR.XAASL.

Texts under development as of 7 January 2022: X.BaaS-sec, X.gecds, X.nssa-cc, X.sa-ec, X.sgcnp, X.sgdc, X.sgmc, and X.sr-cphr.

2 Question

Study items to be considered include, but are not limited to:

a) What new Recommendations or other type of documents should be developed for main actors like service providers, service users and services partners, and other key industry stakeholders to advance the security of the entire cloud computing ecosystem, including cloud computing security, edge computing security, interworking security, etc.?

b) What new Recommendations should be developed for security architecture and security functionalities organization in line with the reference architecture?

c) What new Recommendations should be developed for assurance mechanisms, audit technologies, and associated risks assessment to establish trust among different actors?

d) What new Recommendations should be developed for security solutions, best practices or guidelines to big data platform and infrastructure security?

e) What collaboration is necessary to minimize duplication of efforts with other Questions, study groups, and SDOs?

f) How security as a service should be developed to protect telecommunication/ICT systems?

3 Tasks

Tasks include, but are not limited to:

a) Developing Recommendations or other type of documents to advance cloud computing security.

b) Developing Recommendations to identify security requirements and threats to secure cloud computing services based on the general requirements of cloud computing specified by ITU-T Study Group 13.

c) Developing Recommendations to define security architecture and to organize security functions based on the reference architecture specified by ITU-T Study Group 13.

d) Developing Recommendations to define a strong, flexible, and elastic security architecture and implementation for cloud computing systems.

e) Developing Recommendations to identify assurance mechanisms, audit technologies, risk assessment with the objective of achieving trustworthy relationships within the cloud computing ecosystem.

f) Study and develop big data platform and infrastructure security Recommendations aligned with reference architecture specified by ITU-T Study Group 13.

g) Taking charge of all the Study Group 17 activities on cloud computing security and big data platform and infrastructure security.

h) Representing the work of Study Group 17 related to cloud computing security in the Joint Coordination Activity on cloud computing.

An up-to-date status of work under this Question is contained in the SG 17 work programme at https://www.itu.int/ITU-T/workprog/wp_search.aspx?sp=17&sg=17.

4 Relationships

WSIS Action Lines:

– C5

Sustainable Development Goals:

– 8 (Decent Work and Economic Growth)

– 9 (Industry, Innovation and Infrastructure)

– 11 (Sustainable Cities and Communities)

Recommendations:

– Y-series Recommendations on cloud computing

Questions:

– ITU-T Qs 1/17, 2/17, 3/17, 4/17, 7/17, 10/17, 11/17 and 15/17

Study Groups:

– ITU-T SGs 2, 13, 16 and 20

Standardization bodies:

– Internet Engineering Task Force (IETF); ISO/IEC JTC 1/SCs 27 and SC 38; Organization for the Advancement of Structured Information Standards (OASIS); and other relevant bodies as identified

Other bodies:

– Cloud Security Alliance (CSA); Distributed Management Task Force (DMTF)