Future Generation Computer Systems 90 (2019) 1–19

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

An approach for the secure management of hybrid cloud–edge environments

Antonio Celesti [a,*], Maria Fazio [a], Antonino Galletta [a], Lorenzo Carnevale [a], Jiafu Wan [b], Massimo Villari [a]

[a] Department of Engineering, University of Messina, Messina, Italy
[b] School of Mechanical and Automotive Engineering, South China University of Technology, Guangzhou, China

HIGHLIGHTS

- CoT implies that applications must be moved from the center to the edge of network.
- Secure instant-messaging solutions for Cloud-to-Edge systems are required.
- We overcome such a gap following the Cloud Security Alliance (CSA) guidance.
- We improve confidentiality, integrity, authenticity and non-repudiation.
- Experiments show that security does not negatively affect the overall performances.

ARTICLE INFO

Article history:
Received 10 January 2018
Received in revised form 21 May 2018
Accepted 24 June 2018
Available online 19 July 2018

Keywords:
Cloud computing
Edge computing
Management
Communication
Security

ABSTRACT

The Cloud-of-Things (CoT) paradigm is a challenging approach to manage IoT applications exploiting Cloud resources and services. In order to avoid latency in Cloud–IoT communications, the management of time-sensitive services has to be moved to the edge of the CoT. To this aim, a secure Cloud-to-Edge environment for seamless management of IoT applications is necessary. The realization of a performing and secure Cloud-to-Edge middleware solution is a very strategic goal for future business CoT services. Thus, it needs to be deeply investigated, as highlighted by the Cloud Security Alliance (CSA). A valuable approach to develop an efficient Cloud-to-Edge system is based on an instant-message communication solution. In current Cloud environments, a Message Oriented Middleware (MOM) based on an Instant Message Protocol (IMP) provides good performance, but overlook security requirements. In this paper, we aim at overcoming such a gap following the CSA guidelines. In particular, we discuss the involved issues for improving such a kind of Cloud-to-Edge system in order to achieve data confidentiality, integrity, authenticity and non-repudiation. Moreover, we analyze a real case of study considering a MOM architectural model. Experimental results performed on a real testbed show how the introduced secure capabilities do not affect the overall performances of the whole middleware.

1. Introduction

With the advent of Cloud-of-Things (CoT) paradigm, new challenges arose, such as the real-time communication of many smart devices with a central coordination unit. However, traditional computing systems based on the Cloud paradigm do not support them. In order to avoid latency in Cloud–IoT communications, the management of time-sensitive services has to be moved to the edge of the CoT. To this aim, a secure Cloud-to-Edge environment for seamless management of IoT applications is necessary [1,2]. The communication system of a Cloud-to-Edge middleware is quite complex because it is necessary to balance performance and security management, and this is not trivial at all. In fact, considering a worldwide CoT environment, several issues need to be addressed. On one hand, the Cloud-to-Edge middleware needs to quickly react to changes. For example, according to the popular phrase of Benjamin Franklin "the time is money", a Service Level Agreement (SLA) violation might cause loss of money for a Cloud provider. On the other hand, a security leak can imply the disclosure of private data or cyber attacks. This can have also economic implications for the CoT provider. For this reason the Cloud Security Alliance (CSA) [3] has picked out the critical aspects of Cloud security. According to the CSA guidance, security and privacy have to ensure

* Corresponding author.
E-mail addresses: acelesti@unime.it (A. Celesti), mfazio@unime.it (M. Fazio), angalletta@unime.it (A. Galletta), lcarnevale@unime.it (L. Carnevale), mejwan@scut.edu.cn (J. Wan), mvillari@unime.it (M. Villari).

https://doi.org/10.1016/j.future.2018.06.043
0167-739X/

the availability of services, resource access control, vulnerability mitigation, privacy of the audited user data. As CoT is an emerging paradigm, software architects have to deal with the lack of ad-hoc security standards and of a consolidated vulnerability model as point of reference.

How usually happens in emerging ICT technologies, software architects start to face new technology issues adapting existing systems and solutions to address the new requirements. The same thing is happening with Cloud and Edge computing, but such a strategy is not resulting effective. As a consequence, researchers and software designers are looking at new innovative approach. A promising approach is the adoption of a Message Oriented Middleware (MOM) for Cloud-to-Edge management. In particular, a MOM is based on an Instant Messaging Protocol (IMP) and can considerably simplify the deployment of CoT applications and services also involving devices at the edge, because it allows separating the communication and signaling system from the business logic. At present, to the best of our knowledge, existing IMPs allow achieving a high level of reactiveness and good communication performance, but they do not offer an adequate degree of security.

In our previous works [4,5], we analyzed the performance of secure communications for the management of federated Cloud and IoT environments. In this paper, we analyze the impact of the security of a MOM for Cloud-to-Edge systems based on an IMP. More specifically, we will discuss how the overall communication system can be secured considering both the digital signing and data encryption mechanisms. In order to plan a security strategy, we analyze both the intra-module and the inter-module communications of a MOM based on XMPP [6].

Regarding security, although XMPP supports the SASL/TLS technologies, it presents some limitations. In order to overcome such a gap we will consider the *XEP-0373* [7] specifications, which describe the use of the XEP protocol with the Open Pretty Good Privacy (OpenPGP) encryption standard [8] for the integration of authentication and data encryption functionalities.

The rest of the paper is organized as follows. Section 2 describes related works. More detailed motivations are discussed in Section 4.2. Details about the Security Model applied are provided in 4. In Section 5, we discuss how a MOM for Cloud/Edge computing can be secured, considering in particular the MOM4Cloud architectural model [9]. Description of secure communication techniques is discussed in Section 6. Considering the CLoud-Enabled Virtual EnviRonment (CLEVER) [10] as case study, that is an implementation of MOM4Cloud, a few implementation highlights regarding the development of specific security features are discussed in Section 7. Experiments evaluating the communication overhead for security management are discussed in Section 8. Section 9 concludes the paper.

2. Related works

Security in emerging hybrid Cloud/Edge environments is an emerging topic. In fact, the need to move resources and services from the Cloud to the Edge raises several technical issues, especially from a security point of view.

The influence and impact of mobile Edge computing on existing communication systems is discussed in [11]. In particular, by analyzing existing Cloud systems, it is highlighted how even though the bind among Cloud and Edge is not so evident, there are several important features, such as security and resilience that have to be investigated. Challenges regarding the interconnection between Cloud and Edge computing environments are discussed in [12]. In particular, it is underlined that, in order to achieve real benefits, it is necessary to achieve high throughput under high concurrent accesses, real-time processing performance, mobility support, and data persistency. The need to enhance traditional Cloud security solutions for Edge computing environments is discussed in [11]. Specifically, a holistic analysis shows the presence of new security challenges, threats, and mechanisms inherent to the Edge computing paradigm, but also the presence of potential synergies with other similar paradigms. A fuzzy-based security approach for mobile Fog and Edge computing to handle a scenario in which security services change according to mobile users is presented in [13]. In particular, a multi-criteria decision making methodology that is based on an innovative extension of the hesitant fuzzy rough set theory fused with a hesitant fuzzy soft set is presented. An alternative approach based on the fuzzy security service chaining concept for sustainable mobile Fog and Edge computing is discussed in [14]. The proposed architecture decouples the needed security mechanisms from physical resources. Moreover, a security proxy enables the compatibility with traditional security functions. A biometric security through visual encryption approach for Edge and Fog computing named Zero-watermarking is discussed in [15]. It is aimed at helping to protect the ownership of multimedia contents that are easy to copy and distribute. In particular, a biometric security solution able to analyze face images that does not impact the visual quality of images by using both visual cryptography and zero-watermarking is presented. A security analysis of mobile Edge computing consisting in the context of the European funded SESAME project is discussed in [16]. In particular, the security analysis of a piece of framework deployed in virtualised small cell networks extended in the broader of a 5G wireless network environment is discussed. Always in the domain of mobile Edge computing environment whose borders are interconnected with 5G wireless network, a study on security of dense small cells, which exploit Network Functions Virtualization (NFV) and that move the intelligence into the edges of the network is discussed in [17].

Most of the aforementioned solutions do not consider the presence of firewalls (whose ports have to be opened) that represent obstacles for the secure communication between the Cloud to Edge environments and vice-versa. Instead the last one, requires the creation of overlay networks by means of NFV mechanisms that have to be configured on network devices. In this paper, we propose an alternative communication system solution for the interconnection between the Cloud and the Edge that is able to work at web layer (on port 80) and that is capable of bypassing firewalls (because port 80 is commonly opened), guaranteeing at the same time security and privacy.

3. Motivation

CoT is having a continuous growth in terms of services availability and differentiation. However, it is still not mature in definition of worldwide recognized standards. In particular, the lack of security standards represents one of the major points of weakness of CoT solutions. In this area, CSA conducted a valuable work, and further security aspects that involve Clouds and their stakeholders have been discussed during the last years. In this section, we report and analyze some hints extrapolated from the CSA guidance [18], which promotes the following:

- a common level of understanding between the consumers and providers of Cloud Computing regarding the necessary security requirements and **attestation of assurance**;
- an independent research into Best Practices for Cloud Computing security;
- educational and awareness programs on the appropriate uses of Cloud Computing and Cloud solutions;
- the creation of wide consensus lists of issues and guidance for Cloud security assurance.

Our work arises from a critical investigation of security requirements and issues reported into the CSA guidance. Specifically, we explore the Governance and Operations Domains in the following.