MHCP: Multimedia Hybrid Cloud Computing Protocol and Architecture for Mobile Devices

Jose M. Jimenez, Juan R. Diaz, Jaime Lloret, Oscar Romero

Universidad Politécnica de Valencia, Camino Vera, s/n, 46022, Valencia, Spain

Abstract

Multimedia cloud computing has appeared as a very attractive environment for business world in terms of providing cost-effective services with a minimum of entry costs and infrastructure requirements. There are some architecture proposals in the related literature, but there is no multimedia cloud computing architecture with hybrid features specifically designed for mobile devices. In this paper, we propose a new multimedia hybrid cloud computing architecture and protocol. It merges existing private and public clouds and combines Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Security as a Service (SECaaS) cloud computing models in order to find a common platform to deliver real time traffic from heterogeneous multimedia and social networks for mobile users. The developed protocol provides suitable levels of Quality of Service (QoS), while provides a secure and trusted cloud environment.

Keywords

Multimedia cloud computing, Mobile Device, Infrastructure as a Service (IaaS), Software as a Service (SaaS), Security as a Service (SECaaS), Multimedia streaming Protocol.

Introduction

Cloud computing systems may use one or several service models (Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)) [1]. Multimedia cloud computing allows users to store, search and process their multimedia data with minimal management effort, avoiding full software installation on users' computer or device. It alleviates multimedia software maintenance and upgrade, as well as decreases mobile devices computation time and saves battery. Multimedia services in cloud computing involve a number of challenges such as multimedia, heterogeneity or Quality of Service (QoS). Wenwu Zhu et al. discussed the QoS issues for multimedia cloud computing in [2]. A multimedia cloud, with media services such as VoIP, video streaming or videoconference, should support millions of users simultaneously, thus, QoS must be adapted to different requirements of multimedia services, networks and contents.

Nowadays, the task of integrating mobile computing and multimedia cloud computing is. Moreover, mobile devices have limited memory, computational power, and battery lifetime. An open cloud architecture supporting heterogeneous platforms is one of the most important challenges presented to system designers. Cloud computing systems are classified in four deployment models: Private cloud, Community cloud, Public cloud, and Hybrid cloud. A hybrid cloud computing model combines public and private cloud models. It introduces the complexity of determining how applications across both a public and private clouds can be distributed.

There are hundreds of multimedia providers offering many types of services such as Private VoIP communication, audio and video conference, interactive applications, online games, and online IPTV and radio. E.g. Skype, Google Talk, or PPlive. Most of these solutions are using licensed codecs and protocols. Users must install the appropriate software and libraries to connect to these networking services. Then, end users devices perform functions of rendering tasks but this is not a good solution because of limited computing capability and resources.

Multimedia service users have no control on the QoS mechanisms implemented in the service provider network. Thus, it is a difficult task to guarantee the QoS while crossing several service providers. Moreover, there are several security concerns related with protocols and devices. Most commercial multimedia service providers offer different options to achieve confidentiality and integrity in their communications but they need to rely on specific device features.

This paper proposes a scalable architecture, and its associated protocol, to improve QoS, security and mobile devices power consumption. It uses hybrid cloud computing to manage the multimedia transmission. Moreover, it is designed to be implemented by the ISP core networks in order to provide private multimedia services, such as pay per view TV or Netflix, and, in addition, public services available in Internet, such as multimedia video streaming or VoIP. The architecture takes advantage of the IaaS features to build a hardware infrastructure, and it uses SaaS to reduce resources consumption on final devices. What distinguishes our work from others is that our proposal uses a hybrid multimedia cloud computing architecture that combines IaaS and SaaS cloud computing models to implement a fully secure and trusted cloud environment, and.

The remaining of the paper is organized as follows. Next section provides the related work. Then, we describe the hybrid multimedia cloud computing architecture. The architecture protocol and the algorithms included in the architecture are described in a later section. Next, we describe the security and QoS mechanisms included in the system. In order to validate our proposal we provide some performance results in a test bench.

Related Work

Wenwu Zhu et al., in [2], provide the main concepts of multimedia cloud computing, from both multimedia-aware cloud and cloud-aware multimedia perspectives, and present a novel framework that can achieve high cloud QoS support for several multimedia services.

Multimedia cloud computing must have a robust authorization mechanism for its multi-tenancy and virtualization aspects of resources. In [3], Daniel Nurmi et al. provided an authorization system to control the execution of virtual machines in order to ensure that only administrators and owners could access them. Stefan Berger et al., in [4], promoted an authorization model based on both role-based access control (RBAC) and security labels to control access to shared data, VMs, and network resources. In [5], Jose Alcaraz Calero et al. presented a centralized authorization system that provides a federated path-based access control mechanism. Moreover, Almutairi et al., in [6], provided a distributed access control architecture for multi-tenant and virtualized environments. It uses three types of components: a virtual resource manager, a distributed access control module, and a service level agreement. In [7], Daniel Diaz-Sanchez et al. proposed Media Cloud, a middleware for Set-top boxes for classifying, searching, sharing, delivering, managing, and control media inside the home network and across the cloud. In order to take advantage of both a hybrid cloud and a peer-to-peer architecture for multimedia streaming, Irena Trajkovska et al. suggested in [8] to merge P2P and cloud computing into new distributed cloud computing network for multimedia streaming. They introduced APIs in the cloud, which permit negotiating QoS parameters between a cloud service provider and its potential clients.

Generally, multimedia cloud computing lacks of appropriate and serious security measures to protect users data or applications. M. Hussain et al. introduced in [9] a new architecture named Security as a Service (SECaaS) that addresses the security issues for cloud-based applications. Moreover, in [10], Selvaraj Kesavan et al. proposed a private controlled cloud architecture for the media which stores, processes and delivers the media content to the authenticated cloud users on the go.

Architecture Proposal Overview

In this section, we present a hybrid cloud computing architecture for an Internet service provider, focused on mobile devices, and aims to supply voice, video and multimedia services to end users. It is able to deliver real time traffic from heterogeneous multimedia networks, with suitable levels of QoS and security.

We propose a hybrid cloud computing architecture based on IaaS, SaaS and SECaaS [11] cloud-service models. Following the IaaS cloud model, the cloud includes multimedia components such as media gateway (MG), multipoint control unit (MCU), hardware video transcoding (GPU Cluster) and content delivery network (CDN) . On the other hand, based on SaaS cloud model, the required software to establish the connection with external multimedia networks is running above the resources of CPU/GPU and RAM of the cloud provider, and not at the end user device. In this architecture the service provider establishes and manages the multimedia channels with multimedia servers or remote users, then multimedia data is processed and encrypted to fit the mobile device features and, finally, data is sent to the end user device.

Figure 1 shows the multimedia hybrid cloud proposal. It is connected to other service providers, with their LSA agreements. The physical topology may be built over the multiprotocol label switching (MPLS) network technology. MPLS virtual private networks (VPN), and IPSec VPN when necessary, allow achieving the required QoS and security features from the provider side to the external network, where the multimedia clouds are located. In the logical topology, the hybrid cloud service provider is connected to other multimedia clouds in Internet through direct virtual links. It is able to use specific protocols and codecs for external links, thus forces the service provider to manage a big number of software components inside the hybrid cloud. The hybrid cloud architecture provides enough CPU/GPU and RAM resources to process the multimedia data before sending it to the end users while keeping low latency and jitter. Multimedia data processes adapt codecs and algorithms to heterogeneous mobile devices. End users do not take care of what signaling protocol is being used at the original connection between the hybrid cloud and the external multimedia cloud because they receive all multimedia streams encapsulated by the MHCP protocol.

In order to achieve our goal, we have designed the Multimedia Hybrid Cloud Protocol and Architecture (MHCP), that allows an ISP to provide both, a private service, i.e., pay per view TV, and at the same time, access to public external multimedia clouds through internet, such as Youtube or Skype. It is a real time signaling and transport protocol for communication between the hybrid cloud computing and end user devices. MHCP allows end users to achieve the appropriate levels of QoS and security without taking care of which multimedia service or external server are being used. When clients need to establish a new multimedia communication they create a MHCP channel with a MHCP Server. MHCP protocol, which will be detailed later, is in charge of the multimedia process and security issues, including the connection to external multimedia cloud services, filtering traffic, audio and video data transcoding and data encryption. All of them are performed by the physical resources of the service provider. The hardware and software requirements of the end user device are minimized because the MHCP Server can adapt to fit several types of mobile devices.

Finally, when multimedia channels are created and communication options established, multimedia data is exchanged between the client and MHCP Server with RTP, Secure Real Time Protocol (SRTP) or MHCP. MHCP can be used as a multimedia transport protocol, instead of RTP/SRTP, in order to increase the security level. Multimedia traffic between the hybrid cloud and an external cloud will be performed by RTP/SRTP protocol or the transport protocol chosen by the remote server instead of an intercloud protocol [12].

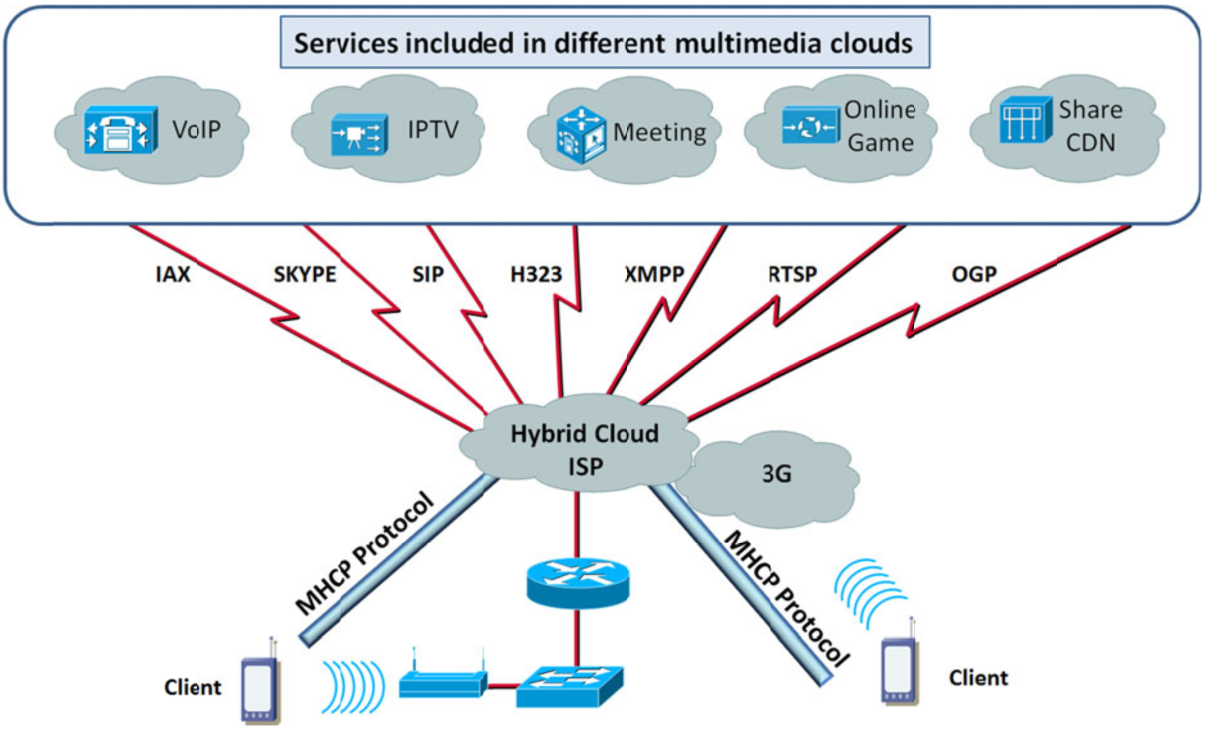

Figure 1.Multimedia hybrid cloud proposal

The combination of the hybrid cloud topology with the MHCP protocol provides QoS provisioning for multimedia applications and services, reduces the delivery latency and maximizes the bandwidth available for clients. Service provider establishes dedicate trunk connections with external service networks, which may be physical or virtual links, with the following requirements: high capacity, bandwidth guarantee, high availability and fault tolerance. Optimum QoS values for real time communications are achieved by the service provider based on the requirements of each multimedia cloud.

This architecture provides many advantages such as identity access, data-center monitor and management, data-loss prevention, end-point protection, rapid provisioning of users, applications threat analysis, VPN services, data encryption, key management and website security.

Figure 2 shows the components in our hybrid cloud and how they are connected in order to improve the security and QoS of the system. Modular architecture integrates independent components for different services and remote servers, thus allows the cloud provider to deliver any type of multimedia service to the end user. Minimizing hardware and software requirements at the end user side decreases the risk of incompatibility with the user device and increases the system efficiency. An end user will only need a web browser to receive multimedia data.

The hardware components inside the hybrid cloud architecture are described as follows. Server virtualization software joins several physical servers to build a server cluster that is represented like a big virtual server in Figure 2. The amount of memory and CPU resources of this virtual server is the sum of memory and CPU of the physical servers. There are a CPU pool and a RAM pool to be assigned to the Virtual Machine (VM) running into the sever cluster. Server virtualization provides dynamic resource allocation of CPU and RAM memory. A scalable server cluster provides enough resources to process multimedia traffic from external multimedia clouds. Cloud computing manages these resources efficiently and balances the load between physical servers. This structure provides a scalable solution because we can monitor resources consumption in real time, increasing the physical system capabilities when necessary. The cloud also supplies a GPU pool for multimedia data computing. The functions performed by the GPU cluster includes video transcoding, rendering and image adaptation to heterogeneous devices, such as mobile or tablet devices with different screen resolution. Multimedia data is stored in a CDN into a disk pool implemented by a disk array. Multimedia Control Unit (MCU) allows the cloud to create audio and video conferences between local users and between local and remote users. Latency and jitter is minimized by reducing the path between end users and the MCU system. MCU implements appropriate transcoding to fit the capabilities of the user devices. MCU component allows registered users at different cloud VoIP networks to communicate with different protocols and codecs. Hybrid cloud computing is connected to PSTN through the media gateway (MG). To improve security and QoS, the path for external calls is finished at the provider’s network. End user sends encrypted VoIP traffic to the media gateway in the hybrid cloud, while maintaining the QoS. Then, MG decrypts, decodes and sends the voice signal through regular telephone lines.

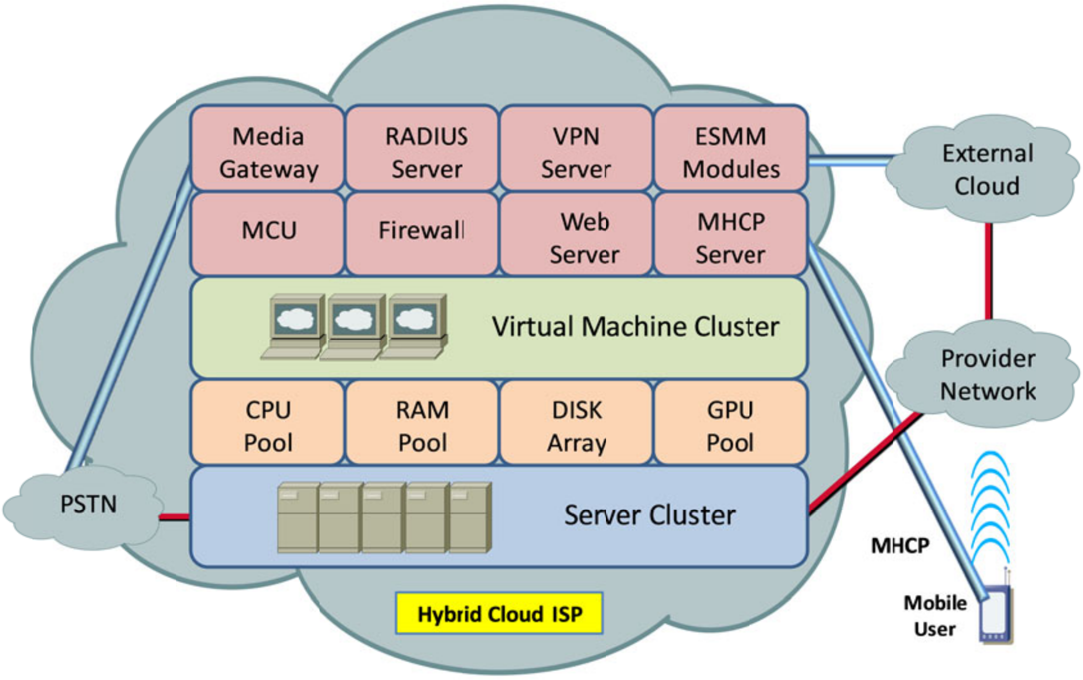

Figure 2.IaaS cloud computing scheme

Figure 3 shows the SaaS cloud computing scheme. MHCP is the key component of the system. Thanks to the combination of the cloud architecture with MHCP protocol, the mobile user only has to establish a single connection with a single protocol. Software requirements of the end user device are few. It only has to execute a java applet application, which runs MHCP protocol, to establish a multimedia connection with the cloud. All multimedia signaling between users and the MHCP Server is exchanged using MHCP protocol. MHCP Sever is running above the server cluster and to achieve fault tolerance it is distributed between different physical servers. MHCP Server only shows a public IP address or DNS name for mobile users connections. Existing services from external multimedia clouds are reached by the MHCP connection. It unencapsulates processes and encapsulates the information of any MHCP request in order to translate it to the multimedia protocol used by the external multimedia cloud.

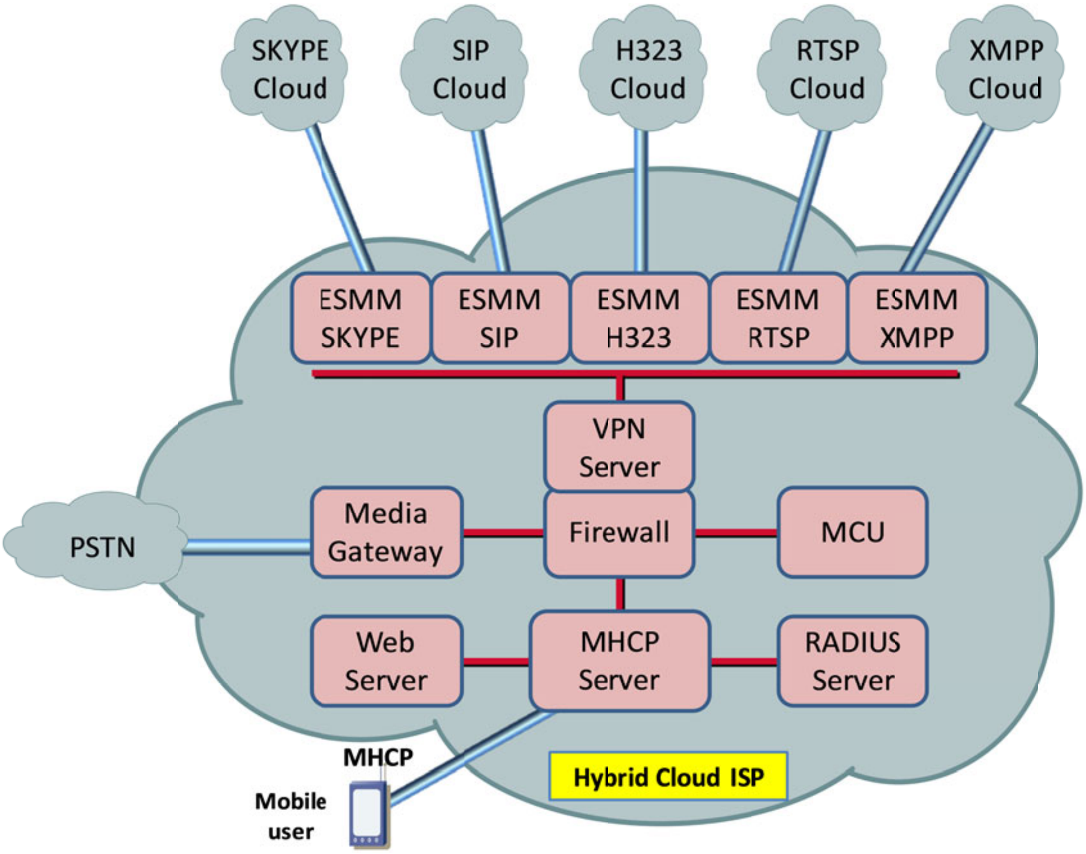

Figure 3. SaaS cloud computing scheme

In order to provide scalability to the architecture and have a flexible system to be able to adapt to all types of multimedia clouds, including emerging services in the future, the relationship with each kind of external multimedia cloud is managed by the appropriate External Service Multimedia Module (ESMM). Each ESMM module depends on the protocol of the external multimedia cloud and communicates with the MHCP Server to exchange the information. There is an ESMM module for each signaling multimedia protocol: ESMM-SIP, ESMM-H323, ESMM-SKYPE, ESMM-XMPP, etc.

From the SECaaS perspective, in order to implement cloud computing security features, the security server implements the security functions such as VPN Server, RADIUS Server, firewall and IPS protection. It provides encryption capabilities for IPSec users and remote systems, user control for local clients and traffic analysis. The advantages of our proposal from the point of view of an ISP are that the MHCP architecture improves the QoS and security issues. First, when ISP users are connected with external server that provides authentication and encryption features, the MHCP protocol keeps these security schemes. Although the packet is encrypted by an external server, the MHCP is still useful because some information about multimedia flow is translated, at the user device, from the original protocol to the MHCP header in order to add QoS improvements. This information never will include user private data. Second, when the external server does not provide security capabilities, the MHCP architecture set up a VPN tunnel between the user and the ISP in order to guarantee the security. Finally, when the users are connected with ISP internal servers, the security is managed by the ISP RADIUS and VPN servers. This allows the ISP to manage the QoS and security.

Protocol and Algorithm

The mechanism and functionalities of MHCP protocol are described in this section. MHCP divides the multimedia network in two parts:

- **End user to the MHCP server:** This part is managed by MHCP protocol. End user device only establishes a single MHCP connection with the MHCP server. It manages the security and connectivity concerns at users side. Firewalls and NAT routers can be tuned to permit traffic addressed to the MHCP server IP address and UDP port. QoS configuration is simplified and the device efficiency increases because it only has to manage a single UDP connection, despite of the number of multimedia flows and protocols used by the external multimedia cloud. QoS is guaranteed between mobile device and service provider using a class based weighted fair queueing.
- **ESMM to the Multimedia Server:** Each QoS is implemented taking into account the service providers LSAs. Security concerns are managed by the cloud architecture. Each ESMM self-adapts to fit the external multimedia cloud requirements. Based on the external multimedia cloud features, the software interface ESMM performs decompression, multiplexing and transcoding.

MHC protocol manages the information using type-length-value (TLV) format inside the protocol header. Then, MHCP header is encapsulated over UDP datagram and the information is exchanged between the user device and the MHCP server. MHCP protocol manages the user account, user device, multimedia service, security requirements, QoS and QoE requirements. The information required by the MHCP about the mobile device specifications are screen size, screen resolution, amount of memory, CPU and available codecs (example shown in [13]). TLV used by MHCP servers includes the external multimedia cloud computing network information such as type of service, signaling protocol, IP address and port of the multimedia server. The implemented mechanisms to meet the security requirements and specification features are encryption, authentication and hashing. In order to meet QoS and QoE requirements, the system gathers real time measurements of bandwidth, latency, jitter and packet loss (more details in [14]). When a media channel is established between the mobile device and the MHCP server, multimedia data is delivered. As a transport protocol, the system can use the standard RTP/SRTP protocol or, when it needs to increase the security level, it can use MHCP protocol. By using MHCP, service providers can achieve maximum efficiency, because they do not have to add new physical resources when offering a new multimedia service.

Security and QoS Issues

Security and QoS are very important when a new protocol for multimedia communications is designed. Security can be improved by applying encryption techniques, but it may affect the real-time transfer because of QoS restrictions. MHCP protocol includes authentication and encryption techniques to improve the communications security, and it is flexible enough to guarantee the QoS. Depending on the situation, the security can be reduced by selecting a faster and less secure encryption algorithm but keeping the appropriate QoS level. .

In our proposal, the security is improved for protocols and services that natively do not include security mechanisms, i.e., http video streaming or SIP service. In other situations, such as https where security is natively provided, the original security is kept, but, in addition, some features as anonymity are improved, because MHCP protocol is working between network and the transport layers..

MHCP Server works as a Network Access Server (NAS) Client into the Authentication, Authorization and Accounting (AAA) model. In order to join the system, a user sends a MHCP Request Connection message to the MHCP Server. Then, a RADIUS Access-request message is sent from the MHCP server to the RADIUS Server to authenticate the new user. Only when the authentication is successful, the new user can establish an UDP communication with the MHCP Server. Once the client is authenticated, MHCP Client and Server negotiate the cryptosystem used to protect the multimedia information. MHCP Client sends to the MHCP server a MHCP Security Scheme message with its available encryption algorithms. MHCP Server chooses the highest level of security that guarantees the QoS, according to a predefined list headed by AES 256 algorithm. All communication will be encrypted. If there are no common encryption or if the MHCP client chooses sending unencrypted multimedia information, the communication between MHCP Server and Client will be clear text. To achieve the best balance between security and QoS, the security information carried by the multimedia packet has been reduced to fit the ID Security Profile header field, that contains the information about the used security algorithms and an index to link the stateful security table.

MHCP Server monitors all managed multimedia flows in order to keep balance between security and QoS for each communication. We have implemented two QoS mechanisms for the MHCP protocol. First, if the QoS parameter values are growing and they reach the predefined thresholds,, the MHCP Server stops accepting new multimedia connections. The second mechanism uses the QoS priority bit inside the ID Security Profile field to manage preference traffic. Flows with higher request of QoS are marked with the QoS priority bit. When traffic congestion happens, the system delays the packets without the Qos priority bit activated to enforce sending priority packets.

Testbench

In order to verify our proposed architecture, we have implemented a typical multimedia cloud scenario delivering VoIP and video services. The software application has been developed in Java programming, under Linux, which emulates the client behavior. Thus, mobile devices are emulated by java applets, running in VMWare ESX software. This allows comparing our hybrid cloud using MHCP protocol with the results obtained by the same scenario using a traditional cloud configuration.

Figure 4 shows the test bench. We have used CPU and RAM resources from five physical servers configured as a cluster to set up one logical machine. Over this platform, we have created several virtual machines in order to perform the test. VMWare ESX software and Linux Operating System were used. The test included two external multimedia clouds, one offering VoIP service through SIP protocol (Asterisk servers) and another offers IPTV service (VLC video servers). The scenario has been designed to analyze the behavior of multimedia flows under both congested and not congested situations. To achieve this behavior, we will modify the number of simultaneously connected users. When the number of users is higher than 80, congestion will happen. The MHCP protocol uses a specific selective packet discard algorithm to guarantee minimum values of jitter and delay. Because of this improvement, we should obtain better results in QoS parameter when MHCP is used.

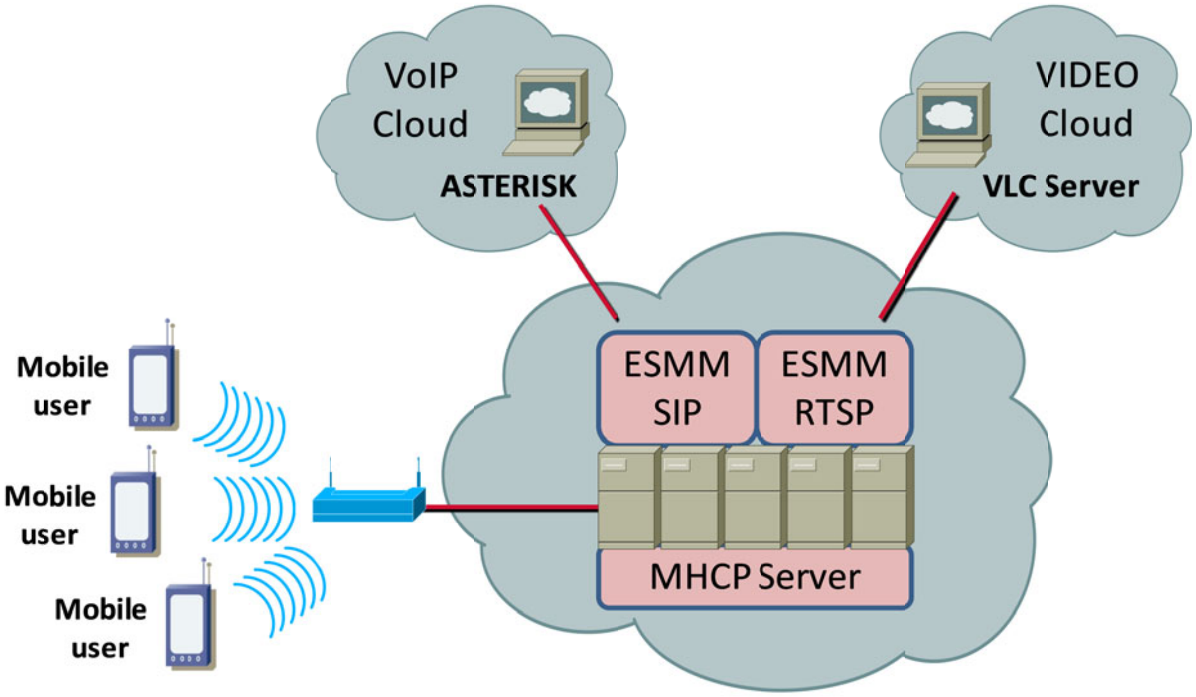

Figure 4.Performed Test bench

We have developed a java applet application to emulate smart phones and tablets, which runs MHCP protocol. Mobile devices connect with MHCP server through an IEEE 802.11g wireless connection. Each mobile device is able to start a number of VoIP and video connections by sending a MHCP request message to the MHCP server, which translates and forwards them to the correct ESMM module. Then, ESMM module contacts the Asterisk server using SIP protocol for VoIP connections and with VLC Server using SRTP protocol for IPTV connections.

We have studied how MHCP works compared with a traditional cloud configuration (NO MHCP protocols, such as RTP or http streaming). Figure 5 (a) shows the number of UDP/TCP connections required when there are the same number of mobile users. With MHCP protocol the number of connections matches the number of mobile devices. But in a traditional network the number of connections is higher and proportional to the number of clients multiplied by the number of multimedia connections of each mobile device. In Figure 5 (b), it is shown the bandwidth consumed. There are few differences between MHCP scenario and traditional configuration when the number of users grows, because the same amount of multimedia data in both scenarios is sent. Thus, we are improving QoS and security issues with low impact on the bandwidth. Figure 5(c) shows the delay behavior when the number of clients grows. With MHCP protocol we can see that the delay has a linear growing. . Under the same conditions, when the MHCP protocol is not used we get an exponential rise of delay.. Similar results can be found for jitter values in Figure (d). With MHCP protocol, jitter values are kept under 20 msec., so it can be controlled by using jitter suppression buffers in the end user application. Under congestion, MHCP protocol incorporates a discard packet mechanism that increases a little the packet loss rate, but as advantage the latency and jitter are limited. These results show how the MHCP protocol improves the multimedia traffic QoS when the number of clients and multimedia flows exceeds the number of users. When there is no congestion, we have obtained similar results in both scenarios

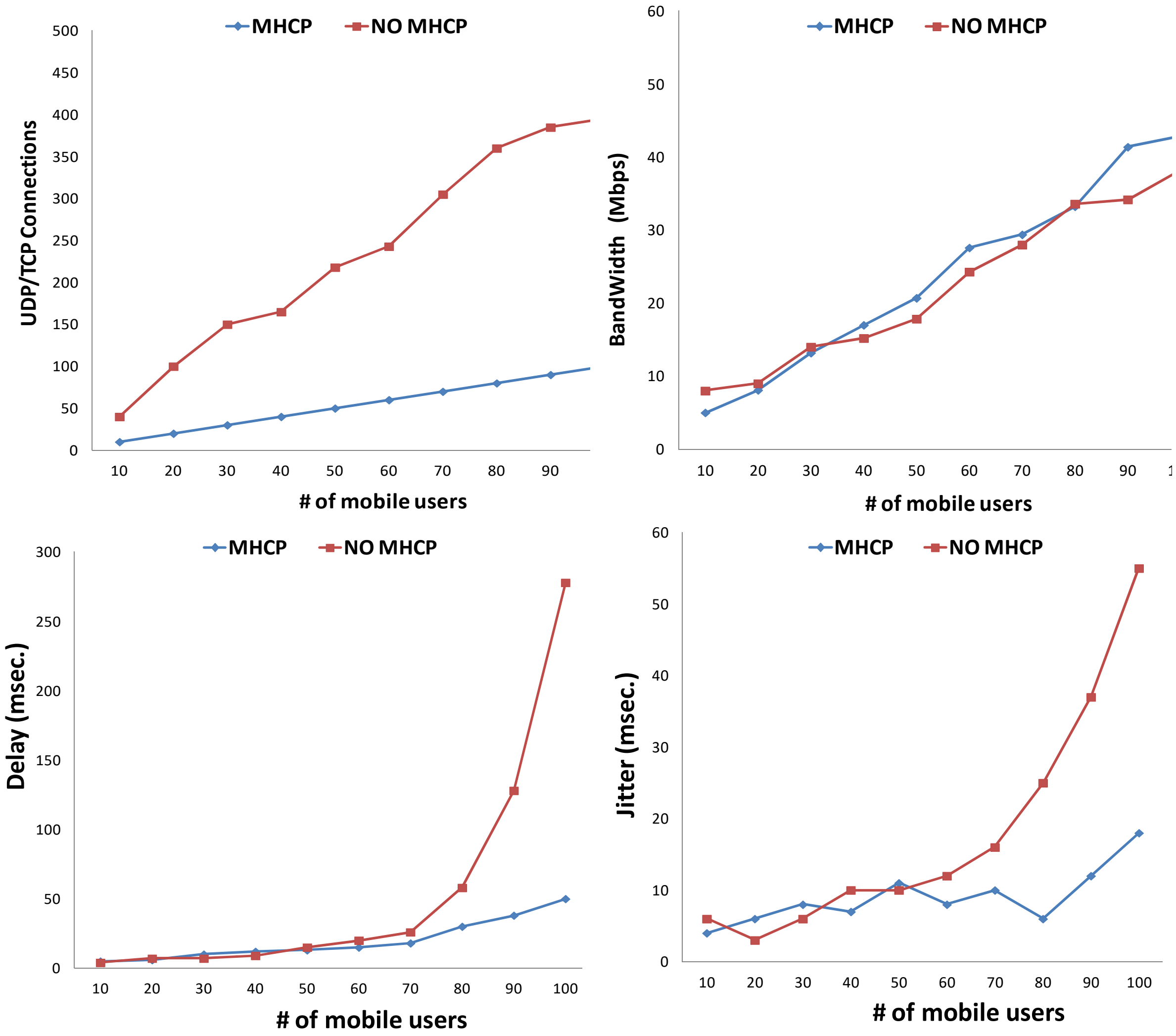

Figure 5(a) top on the left: UDP/TCP Connections Comparison; (b) top on the right: Bandwidth Consumption Comparison; (c) down on the left: Delay Comparison; (d) down on the right: Jitter Comparison

We have also measured CPU and RAM consumption of the virtual server running in our hybrid cloud. Figure 6 shows how fast the resources of the server cluster are being consumed when up to 120 mobile devices establish MHCP connections. The increase is proportional to the number of mobile devices. Thus, it is easy to calculate the amount of expected physical resources. We have observed that the proposed protocol performance is not affected by the number of services and the kind of offered services by the cloud.

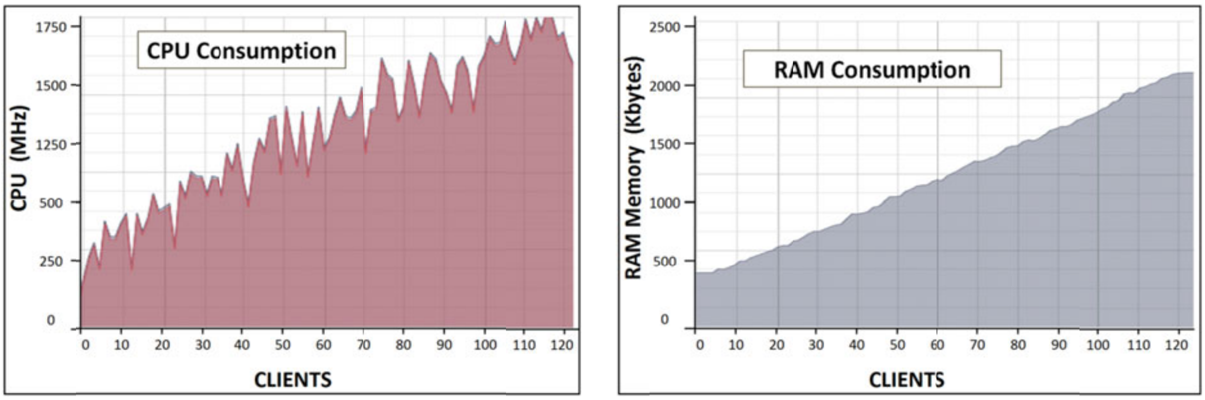

Figure 6. (a) on the left: CPU Consumptions; (b) on the right: RAM Consumption.

Conclusion

This paper presents a hybrid multimedia cloud computing architecture and protocol called MHCP. It is a scalable solution for service providers that offer the mobile users a wide range of multimedia services with QoS and security. It combines IaaS, SaaS and SECaaS cloud computing models. Its functionality and scalability has been shown in the test bench. MHCP allows service providers to efficiently control QoS and security of each user and for each multimedia service. MHCP features improve battery usage since the mobile device is not performing some tasks.

In future works, we will deploy the ESMM multimedia modules in hardware devices in a real scenario. Moreover, we will improve the efficiency by using adaptive algorithms to extract more accurate QoE values from QoS parameters and device specifications. Using dynamic QoE values, measured in real time, the system can interact with the MHCP server in order to adapt multimedia services and reconfigure the QoS policies. Also we are planning to introduce SDN capabilities in our cloud computing architecture to improve the management and scalability.

REFERENCES

[1] P Mell, T Grance, The NIST Definition of Cloud Computing, from NIST Information Technology Laboratory, October 7, 2009, http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, [Last access December 1, 2017]

[2] W Zhu, et al., “Multimedia cloud computing”, IEEE Signal Processing Magazine, Volume 28, Issue 3, Pp. 59- 69. May 2011.

[3] D Nurmi, et al., “The Eucalyptus Open-Source Cloud-Computing System”, Proc. 9th IEEE/ACM International Symposium on Cluster Computing and Grid (CCGRID 09), Shanghai, China, 18-21 May 2009. Pp. 124–131.

[4] S Berger, et al., “Security for the Cloud Infrastructure: Trusted Virtual Data Center Implementation”, IBM Journal of Research and Development, Vol. 53, Issue 4, Pp.1-12. July 2009.

[5] J M Alcaraz Calero, et al., “Toward a Multi-tenancy Authorization System for Cloud Services”, IEEE Security & Privacy, Vol. 8, Issue 6, Pp. 48–55, 2010.

[6] A Almutairi, et al, “A Distributed Access Control Architecture for Cloud Computing”, IEEE Software, Vol. 29, Issue 2. Pp. 36 – 44. March/April 2012.

[7] D Díaz-Sánchez, et al., “Media cloud: an open cloud computing middleware for content management” IEEE Transactions on Consumer Electronics,Vol. 57, Issue 2. Pp. 970-978, May 2011.

[8] I Trajkovska, J Salvachúa Rodrígues, A Mozo Velasco, “A Novel P2P and Cloud Computing Hybrid Architecture for Multimedia Streaming with QoS Cost Functions”, ACM International Conference on Multimedia 2010, Firenze, Italy, October 2010.

[9] M Hussain, H Abdulsalam, “SECaaS: security as a service for cloud-based applications”, Second Kuwait Conference on e-Services and e-Systems (KCESS '11), Kuwait, April 5-7, 2011.

[10] S Kesavan, J Anand, J Jayakumar, “Controlled Multimedia Cloud Architecture and Advantage”, Advanced Computing: An International Journal, Vol. 3, Issue 2, Pp 29-40, March 2012.

[11] J Archer, et al., “Cloud Security Alliance: Secaas: Defined Categories of Service”. Cloud Security Alliance, September 2011. Available at: https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf, [Last access December 1, 2017]

[12] J Lloret, et al, “Architecture and protocol for intercloud communication”, Information Sciences 258, 434-451. 2014

[13] J Lloret, et al., “A Network Management Algorithm and Protocol for Improving QoE in Mobile IPTV”, Computer Communications, Vol. 35, Issue 15, Pp. 1855-1870. September 2012.

[14] J Lloret, et al., “A QoE management system to improve the IPTV network”, International Journal of Communication Systems, Vol. 24, Issue 1, Pp. 118-138. January 2011.