IST-Africa 2011 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2011
ISBN: 978-1-905824-26-7

Improving the Capacity, Reliability & Life of Mobile Devices with Cloud Computing

Mzomuhle NKOSI, Fisseha MEKURIA
CSIR, Meiring Naude Road, Pretoria, 0001, South Africa
Tel: +27 12 8413986, Fax: + 27 12 8414064,Email: MNkosi@csir.co.za, FMekuria@csir.co.za

Abstract: Mobile devices are being considered as service platforms for mobile health information delivery, access to information and communication. However they face challenges with regard to delivering secure multimedia based services due to limitations in computation and power supply. The limitation in computational capacity and limited battery power renders them unusable to run heavy multimedia & security algorithms. In this paper a framework to relieve mobile devices from executing heavier multimedia and security algorithms in delivering mobile health services is described. The proposed framework uses a Cloud Computing protocol management model, which intends to provide multimedia sensor signal processing, secure storage as a service to mobile devices. The approach in this paper is to model the mobile cloud computing process in a 3GPP IMS software development and emulator environment. And show that multimedia and security operations can be performed in the cloud, allowing mobile service providers to subscribe and extend the capabilities of their mobile applications beyond the existing mobile device limitations. Reference is given to mobile health as a relevant mobile application.

Keywords: Multimedia & security Management, mobile applications, Mobile Cloud computing.

1. Introduction

Mobile phones as service platforms can provide several societal, business and governmental services. Hence, serious applications, such as bank transactions, can now be performed on a mobile device, constituents can send mobile messages to their representatives in parliament, and people can access health information through text enquiries [16]. Further developments will allow mobile devices with unique features that can sense the environment and physiological parameters to enhance quality of life and remote monitoring of patients [10,17]. However, mobile devices as compared to desktops computers have limitations in computational capacity and power consumption [2,4]. These limitations must be acknowledged when developing mobile applications and hinders them from functioning in a more or less acceptable capability and reliability like desktop computers. Users of desktop PC based online applications have become comfortable with accessing more sensitive health applications via the Internet. This is because there are established mechanisms for securing desktop based online health applications [1,8].

Securing mobile health applications running on a mobile device is therefore an important area to ensure that applications are trustworthy and reliable [1,14]. In this paper a framework and protocol based on cloud computing is proposed to enhance the capability of mobile devices for use in advanced sensor based health care and monitoring applications. The framework can be extended to include other multimedia based mobile applications in the future.

The emergence of cloud computing in the research space promises to solve some of the concerns facing mobile computing platforms. The following definition is used in this paper: Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centres that provide those services. The services can be Software, Multimedia Computation, Secure Storage, etc. The data-centre signal processing hardware and software is what we will call a Cloud Computing resource. Such a mobile cloud computing model has specific advantages to mobile applications consumers, public and private enterprise workforce. The capabilities of ubiquitous wireless devices and smart phones can be extended to unlimited regions of applications through such a mobile cloud computing framework.

Cloud computing could then be regarded as a resource that can be accessed by mobile applications anytime and anywhere in the world. This is in direct contrast to having servers inside organisation's premises to run applications. Irrespective of several concerns against mobile cloud computing, it gives an answer to the limitations in capability of mobile devices to provide multimedia ubiquitous services [4,9,11]. Security is one of the concerns raised against cloud computing. Therefore, a well defined trusted security mechanism is assumed in the cloud computing architecture proposed in this paper.

When considering multimedia health services using ubiquitous mobile devices, computationally intensive operations can be offloaded onto the cloud. Sensor signal processing, vector operations and secure storage, are some examples that can get a boost through mobile cloud computing research and development described in the following sections. In this paper a framework proposal is presented to use cloud computing resources for enhancement of mobile device capabilities used in the provision of secure and ubiquitous mobile health services [7]. An experimental setup for modelling, simulation and testing of cloud based mobile application is designed using Java software development environment and Bluetooth air interface API's to model the radio interface for signalling and data traffic.

2. Related Work

A number of mechanisms are being suggested to protect mobile devices and improve the reliability of mobile services. In most current systems, security management is handled by application servers [3]. The offloading approach is proposed in [7] which address the outsourcing of execution of heavy application to the surrounding systems called surrogates. In this approach, when a mobile device has to run a heavy application, it sends that application to a close by surrogate system that will execute it and sends the output to the mobile device. Byung-Gon and Petros [4] proposed a cloud based architecture that present a technique to combat problem of smart-phone limitations in terms of computation, memory, and energy reserves. In their architecture, a smart-phone is cloned and its execution offloaded to a computational infrastructure hosting a cloud of clones. In that way, a mobile device is relieved from running heavier applications. From both offloading approaches mentioned above, security concern is not addressed. The proposed model tries to enhance the security and provide mobile health services through a secure health management framework based on the 3GPP IMS secure protocol derivations [5,12].

3. Proposed Model

The mobile-cloud based model is tested using a mobile health applications development example with a JAVA-IMS platform. With the current business model, organisations spend a lot of money in buying or developing software applications to provide or access services. Furthermore, security applications must be built-in in their applications so to protect data.

And when security has been added it must be well managed from time to time to keep it up to date to fight new security threats.

The concept of cloud computing brings a new business model so that mobile health service providers can request secure data storage, computation, and other services from the cloud. The rapid growth of mobile communications technology promises mobile based health care systems which can overcome security challenges [8,9]. Therefore, organisations that have invested in building IT infrastructure will benefit if secure mobile health can be provided as a service via the cloud. Furthermore, with the advent of mobile technology, ubiquitous provision of innovative and secure health services are possible [10]. However, building a reliable and secure mechanism is required to complement the technology [14]. A secure health management mechanism is therefore essential to address security issues in cloud computing. A successful secure mobile health management framework as proposed in this paper will promote adoption of cloud computing by organizations aiming to provide mobile health services.

In Figure 1, a secure mobile health management model of mobile devices is presented. The model aims at separating applications and the management of their computational operations, storage and security. It is designed specifically for mobile computing environments with an aim to enhance the capabilities of mobile devices. However, the model can also be applicable to desktop-based applications if one wishes to minimise costs of running or implementing custom applications. The work done by Byung-Gon and Petros [4] and Kun and Shumao [7] suggest offloading technique of applications execution from a mobile device to a close by surrogate computer connected to the Internet, is possible. This approach raises a concern as to who manages security during the whole process. This issue unless resolved, can be a serious concern for those who want to adopt cloud computing for mobile applications. Consequently, in our proposed model we argue that a security can be provided as a service to protect mobile applications while a mobile device is cloned to an untrusted computational infrastructure. In so doing, there would be a security provider or vendor organisation that offers security to mobile devices. Application providers and users will not have to worry about security as it will be taken care of by security vendor.

Figure 1: Cloud-Based Mobile CSS Model

The concept of computation, storage and security (CSS) as a service has been discussed in the context of cloud computing implemented for desktop systems to support small businesses [9], however, there has been very little discussion for mobile applications. Therefore, a CSS management model is proposed as shown in Figure 1. The model can hence be used by organisations that run applications that must be protected against unauthorised access. For example, in our proposed model, when mobile devices request to access a particular health application, multimedia processing and security verification is performed in the cloud.

The proposed model intends to address computational, storage & security concerns for applications using mobile devices. Some of the CSS services provided by the secure multimedia health services (SMHS) cloud model are briefly discussed below:

- ***Secure Software Execution Environment***: Multimedia sensor signal processing, for accurate physiological information extraction, in a secure software execution environment.
- ***Secure Data Communication***: The wireless communication channel must retain privacy and integrity of data communicated to and from mobile applications.
- ***User Identification***: Authentication and prevention of unauthorized access to mobile (health) information and applications.
- ***Secure Network Access***: only registered subscribers to mobile health services will be able to connect the health network and access services.
- ***Content Security***: The content to and from the mobile device must be utilised as per the terms set by the mobile health service provider.
- ***Secure Storage***: To guarantee the security & privacy of sensitive health information, secure storage at the mobile health application server is provided. Furthermore, to protect theft and loss of data a back-up secure storage service is provided by the health services management cloud.

The above mentioned security concerns pose even more research questions in accordance with our proposed model. In this paper, we will address some of these concerns with respect to the proposed model. The following section will discuss the dimensions of security and show how the proposed model can address security issues at different levels.

4. Effects of Cloud Computing

Research developments towards cloud computing will have a direct impact on a number of issues in existing technologies. Different approaches are necessary to successfully address those issues. Research efforts in cloud computing has identified services that can be delivered via the cloud. Below we list some of those services:

- Software as a Service (SaaS), Secure Data storage, Supply chain management, Hosted computational infrastructure, and Hosted services (fully operational IT environment).

Services delivered via the cloud are dependent on other factors that affect cloud computing. More research will have to be undertaken to find ways to deal with these factors. Some of the concerns that will affect cloud computing based health information monitoring and services are listed below:

- ***Volume of traffic in the network***: increased wireless broadband bandwidth and backhaul will be required to allow fast connection to the application server and the cloud.
- ***Security & Trust***: a secure way to access services through wireless internet must be ensured.
- ***Business Models***: the way business is conducted will have to change to suit the cloud computing paradigm.
- ***Accessibility***: a reliable IT infrastructure must be in place to enable discovery & access to services.

Each of these aspects is an inevitable challenge that requires innovative approaches to address it. A mobile cloud model is described in this paper, based on a mobile health monitoring service, to address the service activation, delivery, computational and business model aspects as discussed in the following sections.

5. Mobile System Components

Today's mobile health applications are limited and run in different platforms to serve diverse purposes. Future possibilities are that mobile networks will operate in an open model as the Internet [6, 9, 10, 12]. Whereby applications running over them are developed and managed by different companies. Mobile services require different levels of computational and security mechanisms depending on several factors. A mobile health service that transmits or stores sensitive information will require a security mechanism to protect applications as opposed to non-critical applications. Therefore, a varied layered security model is imperative to meet security needs of each application. Figure 2 illustrates the components of a mobile health application for remote health monitoring with cloud support. It is composed of a non-invasive sensor to measure some physiological parameter from possible patient's body, a signal processing unit to enhance the noisy sensor signal. Sensor signals obtained from non invasive sensors often are highly noisy (with –SNR) therefore the required signal processing could be intensive to extract the correct physiological information. Depending on the type of mobile device connected to the sensor and the type of sensor signal (1D or 2D multimedia), the signal processing can be performed inside the sensor unit, the mobile device or through support of the cloud. The application server is the final destination for the required health information. This is normally hosted by the mobile health provider company. The service provider can also subscribe and request secure storage services from the CHMS cloud shown in figure 1. This allows the secure back-up storage of mobile health information.

Figure 2. Proposed mobile health monitoring

A basic idea of this framework is that a strong or heavier multimedia signal processing will require increased power consumption for it to execute in a mobile device. To prevent this power drainage, the proposed model uploads a heavier algorithm to be performed in the cloud and final output is then uploaded back to the mobile device. The model framework, therefore, classifies the required service mechanisms as weak and strong classes.

a. *– Service Scheduling Protocol*

In this section we will give an example of a cloud computing service request and acknowledgement timing diagram for a secure mobile health service. When a mobile station (MS) requests for a cloud computing service, the present paradigm of wireless networks is that the request should go via a service (network) provider (SP) node. Security verification must be performed to authenticate the MS for the requested service. Assuming that in this case the smart phone MS is requesting secure software processing of a multimedia sensor signal. An assessment of the bandwidth requirement and QoS is performed by the service provider. The sensor signal is then transferred to the cloud for digital signal processing. The extracted physiological information is then transferred to the service provider applications server for further analysis and decision. This will help

preserve the MS power and extend the capability of the mobile device for other critical applications. Figure 3 shows the interaction and scheduling of processes among the actors to provide a mobile security service based on cloud computing. A cloud component of the interaction model can be a data centre with high computing capability.

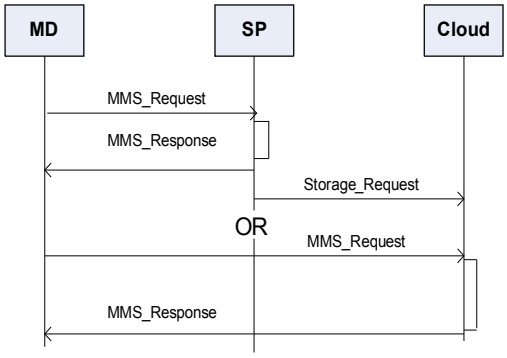

Figure 3. Cloud Service Scheduling flow diagram

1. A user of mobile device (MD) initiates communication by requesting a service from a service provider (SP).
2. The SP authenticates and sends an acknowledgement message to the MD. With the available QoS parameters (bandwidth, realtime/non-realtime service.)
3. Depending on the available QoS, the MD then requests a service. There two ways of doing this, having a clone of the MD in the cloud [4], or connecting to the cloud for online services.
4. Depending on the type of service request by the MD, the SP requests a link to the cloud directly from the MD, the requested computation is then forwarded to the cloud for execution.
5. A response from the cloud is sent to SP which is then routed to MD if it's a real-time service. Immediate authentication is required for real-time services, while delayed service could be re-routed as an application that must completely run in the cloud and later be uploaded to MD.

A framework is built around this mobile service management model. Different modalities can be implemented between the Service provider (SP) and mobile service requests from MDs. A model between the SP and the CHMS cloud could be negotiated to promote secure back-up storage, and data mining and analysis work on the collected mobile data, for mobile advertisement.

6. Mobile Network Security in the Cloud

Mobile devices connect to application providers via wireless or mobile network which is an enabler of communication. It would be a mistake to assume that all mobile network access points are trusted, to an extent that no security measures are put in place to protect mobile devices that connect through them. Therefore, in the case of proposed cloud computing based mobile security management, security would be ensured in every hop that a mobile goes through. This would be achieved through management of security that is done as an independent process run by dedicated company. Furthermore, security verification will be optimized as security providers do best to satisfy needs of their customers. All mobile applications that are subscribed for security management will be tracked down to ensure protection from any malicious attacks. For example, middle man security threat can be

detected and prevented. Authentication and authorization of mobile devices will also be performed in the case of peer-to-peer communication. A solution by 3GPP [5], the Generic Authentication Architecture (GAA) can be applied to solve security problems in a cloud based mobile security management.

7. NGN & Mobile Security

The all-IP network vision of next generation networks (NGN) allows support for authentication of mobile services based on the IP multimedia subsystem (IMS) standard [5]. The convergence of fixed and mobile networks in the IMS architecture raises an important issue that must be solved: i.e, whether the SIM (subscriber identity module) based authentication defined in 3GPP is suitable for:

1- Easy mobile health service creation and integration of convergent services.
2- The definition and allocation of authentication keys for the various mobile services, a single device or subscriber wants to access.

The 3GPP Generic bootstrap authentication (GBA) architecture, allows for different kinds of authentication based on service requirements [5]. A service oriented scalable security architecture will be required, for this to be effective [5,12]. The question: who should be responsible to define the level of authentication needed for each service, is crucial. Should service providers who develop the content and services do the job or the network operator, who owns the network? This is a contentious issue which requires regulatory intervention and the setting up of a general guideline for promoting successful launch of the myriad of innovative mobile services expected to appear in the market [9].

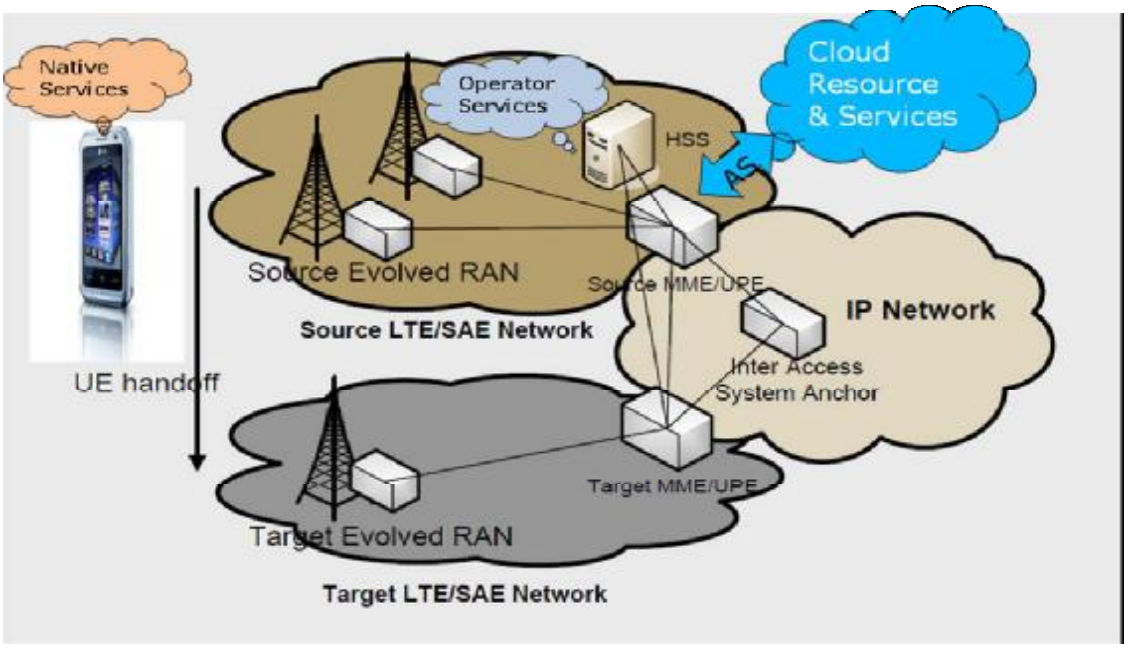

Figure 4, Mobile Cloud Computing: Native, Operator and Cloud Service Paradigm

Figure 4, describes the native, operator and cloud computing resource utilization in the proposed mobile cloud computing model. The main idea is that if a mobile application requires less computation, and then it is natively executed using the user equipment (UE) capabilities. If a service requires its computation or if device capabilities are limited, then it is either executed using an operator "cloud" resource or through an application server (AS) by an external cloud service provider. The advantage of the external cloud services are

network operator independence and ubiquity. However, a number of network operators have proposed cloud like services with roaming possibilities and a quality of service guarantee that matches the external cloud service providers such as Google and Microsoft.

A mobile computing simulation model, for working with IMS based Java API's described in [12,5] is used in this paper to make possible the various service types described in figure 4. Such a framework will handle functions and applications for circuit/packet switched voice/data services and web services [5]. At the same time Next Generation mobile broadband services require multimedia content and the involvement of service providers to set the required level of security [9,14]. The use of cloud computing architectures is expected to complement the 3GPP standards in improving the execution of multimedia algorithms and security mechanisms for increased reliability and provision of next generation innovative mobile services [4,9].

In the next section the experimental setup used for modelling and testing of mobile cloud based services will be shortly described.

8. Simulation & Modelling

Any modelling of mobile cloud services has to start from an understanding of the 3GPP IP multimedia subsystem (IMS), which describes a merger of the internet and telecom protocols. Modelling, simulation and testing of mobile cloud computing services is based on the open-source Java mobile wireless toolkit and the Java Mobile Edition (J2ME) software development and emulator environment[12]. Models for different client and server architectures can be designed using these tools. The J2ME Bluetooth Application interface modules are used to model the air interface between client and server devices. The reason for using the Bluetooth radio interface is because it is an open and free resource and suitable for the modelling environment we use. The Java wireless toolkit and Java for mobile edition (JME) programming environment, has several open-source Bluetooth API's which helps in modelling the secure access control system. The experimental platform is designed as generic as possible to be able to develop software and test mobile cloud algorithms in a reliable fashion. As the J2ME environment is platform independent, prototyping of mobile cloud based health applications, using a mobile hardware platform can be easily performed by generating downloadable executable code.

9. Conclusions & Future Work

Mobile service management performed in the cloud is expected to reduce the burden of running heavy computation, securing data stored in mobile devices and enhance service delivery using even low-end mobile devices. This will improve mobile-Government, Health and Banking services to be provided without limitations of device capabilities and security concerns. The paper discussed the research areas in IP multimedia system protocol management, service activation and support of mobile cloud computing APIs for societal services such as mobile health, banking. Furthermore, the paper discusses on standards and a framework to extend the capacity, reliability and life of mobile devices through a common service provider and network operator platform. This will allow people with even low cost mobile phones to have access to advanced services. The transitional execution and performance of hosted mobile cloud services will require more research and testing, to look at which part of an application needs to be performed natively in the mobile device or the cloud. Synchronization of processes to make sure that a security protection and access to services is completed correctly. Finally a test of the services management system for a proposed mobile health service with cloud support is demonstrated.