Institute of Advanced Engineering and Science

International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.3, No.1, February 2014, pp. 53~66
ISSN: 2089-3337

A Survey on Mobile Cloud Computing with Embedded Security Considerations

***Waziri Onomza Victor, **Joshua Abah, ***Olumide Sunday Adewale, ****Muhammad Bashir Abdullahi, **Arthur Ume**
* Departement of Cyber Security, Federal University of Technology Minna, Nigeria,.
** Departement of Computer Computer Science, Federal University of Technology Minna, Nigeria,
*** Departement of Computer Computer Science, Federal University of Technology Akure, Nigeria,
**** Departement of Information and Media Technology, Federal University of Technology Minna, Nigeria,

Article Info

Article history:

Received Nov, 20th, 2013
Revised Dec 25th, 2013
Accepted Feb 10th, 2014

Keyword:

Cloud computing
Mobile Applications
Mobile cloud computing
Mobile devices
Security

ABSTRACT

The emergence of cloud computing hold a promise to computing where software is provided as a services (SaaS) via the Internet. Mobile cloud computing integrates cloud computing with mobile devices. By this architecture, certain challenges (e.g., battery life, storage, and bandwidth) of mobile devices are addressed. Cloud computing provides the foundation for mobile cloud computing through the delivery of services, software, storage and computational capacity over the Internet, thereby reducing cost, increasing storage, improving battery life of mobile devices and providing flexibility and mobility of data and information. However, the realization of some of these benefits is far from reality in mobile applications, as a result, opens new areas of research such as security of privacy and services. To better understand how to facilitate the development of mobile cloud computing, we surveyed existing work in mobile cloud computing in the context and principles of its foundational cloud computing technology. We provided a definition of mobile cloud computing and gave a summary of results from this review, in particular, the models, architecture, applications and challenges of mobile cloud computing. We concluded with recommendations for how this better understanding of mobile cloud computing can assist in the development of better and stronger mobile applications.

Corresponding Author:

Corresponding Author: Victor Onomza Waziri,
Department of Cyber Security Science,
School of ICT,
Federal University of Technology,
Minna-Nigeria
Email: victor.waziri@futminna.edu.ng

1. INTRODUCTION

Cloud computing is a paradigm shift to the traditional computing whose capabilities are often confused. Cloud computing encapsulates several layers of computing provisioning that include the hardware resources located at the data centres of cloud providers, the operating system and virtualization software on top of that hardware, and the applications that are delivered as services over the internet [2]. These models are generically referred to as Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as aservice (SaaS) [3]. It is a general term that includes almost any kind of outsourcing of hosting and computing resources [1]. Cloud computing is a model for enabling convenient, on-demand network access to computing resources that can be rapidly provisioned and released with minimal management effort [1].

Mobile devices have become an integral part of information and communication technology (ICT) and its growth in recent years have had tremendeous impact. Mobile devices allow users to run applications that take advantage of the growing availability of in-built sensing and robost data exchange capabilities of mobile devices [1]. As a result of these characteristic, mobile applications seamlessly integrate with real time data streams and web 2.0 applications like social networking, mobile commerce, open collaboration and mashups [4]. As mobile devices hardware and mobile networks continue to evolve and improve, the mobile execution platform is being used for more computing task leading to mobile applications in areas that include mobile gaming, mobile commerce, mobile healthcare, mobile banking, and mobile learning [5].

As mobile devices hardware and mobile networks continue to evolve and improve, mobile devices will always be constraint and resource-poor, less secure, with less energy as they are powered by battery cells and with unstable and unreliable network connectivity. This resources poverty striken is identified as the most challenging issue for many applications [1], [6]. As a result of this challenge, computation on mobile devices will always involve a trade-off since mobile devices are regarded as entry points and interface to cloud online services [1].

The integration of cloud computing, mobile devices, wireless communication networks, mobile web and location-based services has laid the foundation for the modern computing model now called mobile cloud computing

The rest of the paper is structured as follow: Section 2 gives a vivid review on the recent related works on cloud architecture and various consolidated Mobile Cloud Architectures applications. This section also reviews various challenges encounter in Mobile Cloud Computing environment, Section 3 discusses the security challenges in Mobile cloud computing which involves security threats of mobile cloud computing that could be divided into three; security threats to mobile devices, security threats to cloud platform and application containers and security threats to communication channels. Section 4 deals with the Secrecy issues as related to communication on the Mobile Computing and also envisioned the future trend of Mobile computing while section 5 gives the conclusion of the paper.

2. Related Works

This paper provides several representatives to mobile cloud approaches in recent time, much other work exist but the purpose of this paper is to provide an overview of the wide spectrum of mobile cloud computing possibilities, architecture, benefits and challenges. Cloud computing is emerging as one of the most prominent means for providing seamless services and applications on mobile devices [7]. There are basically two extreme approaches to mobile applications; offline and online applications but none of these two extreme approaches meet completely meet the requirements of mobile cloud computing.

The offline approach uses the capabilities of mobile devices, but integrates poorly with the cloud system. On the other hand, the online approach makes less use of the mobile devices and their accompanying computing resources and sensors while suffering from interactivity issue [1]. Therefore we belived that to tap into the full benefits and potentials of mobile cloud applications there is the need to investiagate and bring to some point of harmony the gains of both the offline and online approaches. This harmonization leads to the issue of partitioning and offloading and to simplify the development, a convenient but effective programming abstraction is required.

Scenarios of ‘cloud computing’ provides the opportunity to execute applications on servers instead of running them locally and enable mobile devices overcome limitation of limited resources to a great extent [7]. Also, it eliminates the needs for mobile application developers to create multiple versions of the same application. Mobile devices (e.g., Smart phones, tablet PCs, PDAs etc.) are becoming an integral part of human life as the most effective and convenient means of communication unlimited by time and space. This is in conformity with the vision of Weiser [8] known as ubiquitous computing. In this vision, Weiser described that “*Classical computers will be replaced by small intelligent, distributed, and networked devices that will be integrated into everyday objects and activities*.”

Considering cloud computing in mobile context, we then define: “Mobile cloud computing as a model for transparent elastic augumentation of mobile devices capabilities through ubiquitous wireless access to cloud storage and computing resources, with context-aware dynamic adjusting of offloading in respect to change in operating conditions while preserving available sensing and interactivity capabilities of mobile device” [1].

a. Mobile Cloud Computing Architecture

Cloud computing exists when tasks and data are kept on the Internet rather than on individual devices, providing on-demand access. Applications are run on a remote server and then sent to the user [9] (Soeung-Kon, Jung-Hoon & Sung, 2012). Figure 1 shows an overview of the mobile cloud computing architecture. The details of cloud architecture could be different in different contexts; but from the concept of cloud computing, the general architecture of mobile cloud computing can be shown in Figure 1; mobile devices are connected to the mobile networks via base stations such as base transceiver stations, access points or satellites that establish and control the connections and functional interfaces between the networks and mobile devices. Mobile user’s requests information (e.g., ID and location) that are transmitted to the central processors that are connected to servers providing mobile network services. Here, mobile network operators can provide services to mobile users as authentication, authorization, and availibity based on the home agent and subscriber’s data stored in databases. After that, the subscriber’s requests are delivered to a cloud through the Internet.

In the cloud, cloud controllers process the requests to provide mobile users with the corresponding cloud services. These services are developed with the concepts of utility computing, virtualization, and services-oriented architecture (e.g., web, application, and database servers).

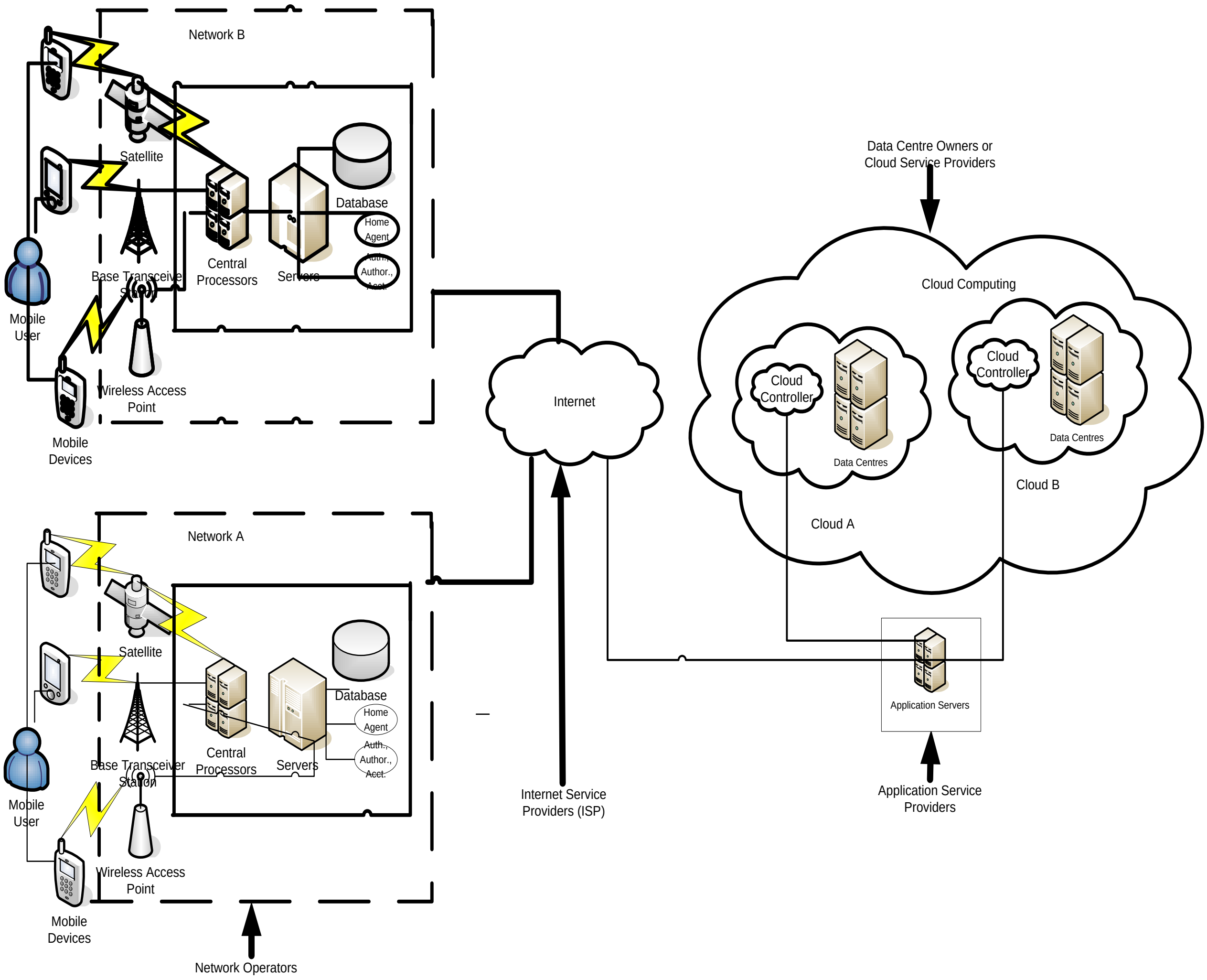

Figure 2. 1: Architecture of Mobile Cloud Computing [10].

b. Mobile Cloud Computing Applications

Mobile cloud computing is one of the mobile technology trends in the future as it combines the advantages of the integration of both mobile computing and cloud computing, thereby providing optimal services for mobile users [11]. In recent years, applications targeted at mobile devices have started becoming abundant with applications in various categories such as entertainment, health, games, business, social networking, travels and news [12]. The increasing usage of mobile computing is evident in the study by Juniper Research, which states that the consumer and enterprise market for cloud-based mobile applications is expected to rise to $9.5 billion by 2014 [13], [12]. The popularity of these is evident by browsing through mobile app download centres such as Apple’s iPhone apps, Nokia’s Ovi suite or Google apps etc. The applications supported by mobile cloud computing are discussed as follows [11]:

a. Mobile Commerce (m-Commerce)

Mobile commerce (m-commerce) is a business model for commerce using mobile devices [10]. The m-commerce applications generally fulfil some tasks that require mobility (e.g., mobile transactions and payments, mobile messaging, and mobile ticketing). The m-commerce applications have to face various challenges (e.g., low network bandwidth, high complexity of mobile device configurations, and security). Therefore, m-commerce applications are integrated into cloud computing environment to address these issues. [14] Proposes a 3G e-Commerce platform based on cloud computing. This paradigm combines the advantages of both third generations (3G) networks and cloud computing to increase data processing speed and security level based on public key infrastructure (PKI) [15].

b. Mobile Learning (m-Learning)

Mobile learning (m-learning) is designed based on electronic learning (e-learning) and mobility [10]. However, traditional m-learning applications have limitations in terms of high cost of devices and network, low network transmission rate, and limited educational resources [16]–[18]. Cloud based m-learning applications are introduced to solve these limitations, for instance, utilizing a cloud with the large storage capacity and powerful processing ability, the applications provide learners with much richer services in terms of data (information) size, faster processing speed, and longer battery life.

Another example of mobile cloud computing application in learning is ‘Cornucopia’ implemented for researches of undergraduate genetics students and ‘plantations pathfinder’ designed to supply information and provide a collaboration space for visitors when they visit the gardens [19]. The purpose of the deployment of these applications is to help the students enhance their understanding about appropriate design of mobile cloud computing in supporting field experiences. In [20], an educational tool is developed based on cloud computing to create a course about image/video processing. Through mobile phones, learners can understand and compare different algorithms used in mobile applications (e.g., face detection, denoising, image enhancement etc.)

c. Mobile Healthcare (m-Healthcare)

The purpose of applying mobile cloud computing in medical applications is to minimize the limitations of traditional medical treatments (e.g., small physical storage, security and privacy, and medical errors [21]). Mobile healthcare (m-healthcare) provides mobile users with convenient helps to access resources (e.g., patient health records) easily and quickly. Besides, m-healthcare offers hospitals and healthcare organizations a variety of on-demand services on clouds rather than owning standalone applications on local servers.

There are few schemes of mobile cloud computing applications in healthcare. For instance, [22] presents five main mobile healthcare applications in the pervasive environment.

i. Intelligent emergency management system can manage and coordinate the fleet of emergency vehicles effectively and in time when receiving calls from accidents or incidents.
ii. Comprehensive health monitoring services enable patients to be monitored at anytime and anywhere through broadband wireless communications.
iii. Pervasive access to healthcare information allows patients or healthcare providers to access the current and past medical records.
iv. Health-aware mobile devices detect pulse rate, blood pressure, and level of alcohol to alert healthcare emergency system.
v. Pervasive lifestyle incentives management can be used to pay healthcare expenses and manage other related charges automatically.

Similarly, [23] proposes @HealthCloud, a prototype implementation of m-health information management system based on cloud computing and mobile client running Android operating system. This prototype presents three services utilizing the Amazon’s S3 Cloud Storage Service to manage patient health records and medical images.

i. Seamless connection to cloud storage allows users to retrieve, modify, and upload medical contents (e.g., medical images, patient health records, and biosignals) utilizing web services and a set of available APIs called Repretational State Transfer.
ii. Patient health record management system displays the information regarding patient’s status, related biosignals, and image content through application’s interface.
iii. Image viewing support allows the mobile users to decode the large image files at different resolution levels given different network availability and quality.

For practical system, a telemedicine homecare management [24] system is implemented in Taiwan to monitor participants, especially for patients with hypertension and diabetics. The system monitored 300 patients and stores more than 4736 records of blood pressure and sugar measurement data on the cloud. When a participant performs blood glucose/pressure measurement via specialized equipment, the equipment can send the measured parameters to the system automatically. Also, the participant can send parameters by SMS via their mobile devices. After that, the cloud will gather and analyze the information about the participant and return the results [10].

d. Mobile Banking (m-Banking)
Mobile banking (also known as m-Banking, SMS Banking, etc.) is a term used for performing balance checks, account transactions, payments etc., via a mobile device such as a mobile phone or Personal Digital Assistant (PDA). Mobile banking today is most often performed via SMS or the mobile Internet but can also use special programs, called clients, downloaded to the mobile device.

e. Mobile Gaming (m-Gaming)
Mobile game (m-game) is a potential market generating revenues for service providers. M-game can completely offload game engine requiring large computing resource (e.g., graphic rendering) to the server in the cloud, and gamers only interact with the screen interface on their devices. [25] Demonstrates that offloading (multimedia code) can save energy for mobile devices, thereby increasing game playing time on mobile devices. [26] Proposes MAUI, a system that enables fine-grained energy-aware offloading of mobile codes to a cloud. [27] Presents a new cloud-based m-game using a rendering adaptation technique to dynamically adjust the game rendering parameters according to communication constraints and gamers' demand.

2.3 Challenges with Mobile Cloud Computing

Resource deficiency of mobile devices is the major motivating factor for the adoption of mobile cloud computing [7]. The solution to resource deficiency of mobile devices provided by mobile cloud computing is achieved by adding the deficient resources in mobile devices to the cloud so that these resource deficient mobile devices can access. This arrangement has introduced several challenges to mobile cloud computing. As a result of the integration of different fields, that is, cloud computing and mobile networks, mobile cloud computing has to face many technical challenges [10]. In other to get pervasive and ubiquitous environment for cloud computing in mobile applications, we need to get across various stages of mobile infrastructure, which are responsible for added network latency and transmission delay [7]. Efficiency of delivering services/apps is needed to be increased in order to achieve goal of access anywhere and with whatever device.

According to [7], using cloud computing concept in mobile world is all about supplying mobile applications and services in the cloud, enabled through cloud service providers and then deliver it to end-user's mobile devices over the Internet when required. So in making remote applications available to mobile devices by the use of cloud computing, main components of this arrangement will include:

1. Mobile device (accessing the mobile networks)
2. Mobile Networks (through which mobile devices are accessing cloud)
3. Mobile applications (available in the cloud as software as a Service (SaaS))
4. Security

These entities form the elements of mobile cloud computing and all of these elements have some extent of challenges which form the challenges of mobile cloud computing.

3. Challenges with Mobile Devices

i. **Limited Energy Source of Mobile Devices**: power capacity of mobile devices is based on their batteries whose capacity is limited so it is very important to maximize the battery life [7]. More and more application execution in the cloud means more battery saving but in general it is not possible to completely transfer the whole application execution to the cloud. For example basic functions like opening of an application, inputting data and displaying result of processing obviously need to run on device. Application function can be partitioned to determine which is to be offloaded to the cloud and which is to be carried out on the device itself. Display application need to run on device while non-display and sophisticated applications need to be offloaded to the cloud [7]. Display and sophisticated applications need larger battery packs as they have to run larger display while non-display applications generally have very little display usage. In case of the mobile devices, energy is basically used for displaying different elements and for internet connectivity [28].

ii. **Resource Poverty of Mobile Devices**: Comparison of desktop PC with any mobile device shows that on what cost this feature of mobility is being achieved. As compared to a fixed device, mobile devices in general have [7]:

a. Three times less processing power
b. Eight times less memory
c. Five times less storage capacity
d. Ten times less network bandwidth.

So in general we can say that this resource deficiency is one of the major reasons for the adoption of mobile cloud computing. In order to overcome these limitations of mobile devices, resources are added to the cloud infrastructure and can be used anytime on requirement, providing a seamless user experience for advanced applications. Even after continuous improvements in mobile device performances', the disparity between the resource constraints of mobile and fixed devices will remain and must be accounted for in the types of application selected for mobile cloud computing [7].

3.1 Challenges with Mobile Networks

i. **Inherent challenges of Wireless Network**: wireless network is the base for carrying out cloud computing and it has its own intrinsic nature and constraints. These challenges complicates its design for mobile devices even more in comparison to the fixed cloud computing. Fixed broadband is supported by consistent network bandwidth wile wireless connectivity is characterised by variable data rates, less throughput, longer latency and intermitted connectivity due to gaps in coverage. Subscriber mobility and uncontrollable factors like weather are also responsible for varying bandwidth capacity and coverage [31].

ii. **Various Network Access Schemes**: in order to implement cloud computing to mobile devices, a basic requirement is to have an access to network. In mobile world there are heterogeneous access schemes with different access technologies like GPRS, 3G, WLAN, WiMAX and so on, each one with their own schemes, policies, offerings and restrictions. Due to the existence of different access schemes we need seamless connection handover schemes (to avoid connection failure and connection reestablishment) when moving from one network access point to another network access point [7].

iii. **Reducing Network Latency**: Factors responsible for overall delay response of applications are [7]:

a. Processing time at the data centres
b. Processing time on the device
c. Network latency and
d. Data transport time.

The processing time is based on applications. While nothing much can be done to application processing time, measures can be taken to improve the network latency by keeping applications as close as possible to the users as latency is significantly affected by distance. Heavy data like video and podcasts if kept closer to the device will save bandwidth and cut transmission delay. Similar kinds of applications are highly immersive applications such as real-time translations. Latency can be positively improved by allowing service providers to re-route internet traffic logically based on the location cache capabilities, this can save bandwidth effectively [7].

iv. **Lack of Speedy Mobile Internet Access Everywhere**: in order to get speedy mobile internet access new technologies like HTML5 are being developed [7]. They provide facilities for local caching. Researchers are working to get a better way of accessing mobile web other than browsers. Technologies like OMA's Smartcard Web Servers and TokTok are being introduced just to provide a better access to mobile web. OMA's Smartcard Web Servers, which is basically a souped-up SIM card that connects directly with the carrier to provide applications to mobile phones. TokTok allows voice enabled access to web services like Gmail and Google Calendar. Through these voice-enabled searches, mobile applications talk directly to the service itself sitting on the edge of the network, avoiding the requirement to lunch a web browser and navigate through the mobile web [7].

In order to resolve this connectivity challenge existing with mobile devices, most of the providers are offering 4G/Long Term Evolution (LTE) services. These services provides advantages of data storage capacity, plug and play features, low latency and they support both FDD and TDD using the same platform. According to the requirement, sometime LTE is also loaded on speed as it is capable of providing download peak rates of 100Mbps and upload of 50Mbps [32].

v. **Seamless Connection Handover**: in order to provide data communication using cellular network, mobile operators are trying to set Wi-Fi Aps on street so that offload traffic of Wi-Fi systems can be reduced, resulting in reduced cellular traffic congestion. But in this arrangement basic requirement is to provide seamless connection handover between access networks. Currently executing application is terminated or returns error when moved from one access point of network to another access point of network or when moved from Wi-Fi network to 3G-based cellular network due to occurrence of communication failure and connection reestablishment situations [7].

The problem of communication failure is described as broken-pipe problem and it can be resolved by having communication channel with flushing zero window notification. Similarly, the problem of connection reestablishment is defined by bind error, and can be resolved by implementing TCP port inheritance during socket reconstruction [7]. No additional messages for channel clearing are introduced and no modifications are imposed on TCP protocol stack during TCP port inheritance. The approach of TCP inheritance is independent of the internal architecture of current 3G cellular networks as it is purely based on end-to-end architecture. By imposing zero window advertising and TCP port inheritance, an open network connections and server sockets can be preserved [33].

vi. **Bandwidth**: nowadays, accessing social media sites (e.g., YouTube, Facebook, Twitter etc) through mobile devices is becoming very popular. These sites generally require more bandwidth in comparison to the traditional sites. If number of clients using social media of any organization increases the demand for modified network infrastructure capable of supporting wide-scale use of external and resource intensive web sites also increases. It is therefore the organization’s responsibility to plan and ensure that adequate bandwidth is available for widespread Internet use. Additional bandwidth can be achieved from hosting environment to cover surges in Internet or network activity. In case of rich internet and immersive applications, (e.g., online gaming etc) that requires high-processing capacity and minimum network latency, cloud computing faces challenges due to low bandwidth of mobile network. In this case, an improved network bandwidth is required so that data transfer within the cloud and other services can be improved [7].

3. 2 Challenges with Mobile Applications

Offloading workloads to the cloud introduces many other issues such as the need for establishing a connection to the cloud which deplete the battery life during the process of establishment of connectivity to cloud and secondly, it introduces security challenge of man-in-the middle attacks and other similar issues. Similarly, offloading is one of the main features of mobile cloud computing to improve the battery lifetime for the mobile devices and to increase the performance of applications [10]. However, there are many related issues including efficient and dynamic offloading under environment changes.

a. Offloading in the Static Environment:

Experiment in [29] shows that offloading is not always the effective way to save energy. For code compilation, offloading might consume more energy than that of local processing when the size of codes is small. For example, when the size of altered codes after compilation is 500 KB, offloading consumes about 5% of a device’s battery for its communication, whereas the local processing consumes about 10% of the battery for its computation. In this case, the offloading can save the battery up to 50%. However, when the size of altered codes is 250 KB, the efficiency reduces to 30%. When the size of altered codes is small, the offloading consumes more battery than that of local processing. [29] Shows another example of a Gaussian application (to solve a system of linear algebraic equations) which offloads the entire matrix into the remote server. In terms of the energy efficiency, the cost of offloading is higher for a small matrices (e.g., smaller than 500 x 500 in size), whereas the cost saving can be up to 45% for large matrices. Therefore, it is a critical problem for mobile devices to determine whether to offload and which portions of the application’s codes need to be offloaded to improve the energy efficiency. In addition, different wireless access technologies consume different amount of energy and support different data transfer rates. For example, for smart phones, Wi-Fi presents the less costly path (with 23% less energy consumption) in comparison to GPRS in a web browsing scenario [7]. If we ignore the maintenance of GPRS connection (for example, for non-phone devices like tablets) then the power consumption of GPRS verses Wi-Fi is even starker, with Wi-Fi using just one third of the energy of GPRS. These factors have to be considered.

b. Offloading in the dynamic environment:
The environment changes can cause additional problems [10]. For instance, the transmitted data may not reach the destination, or the data executed on the server will be lost when it has to be returned to the sender. [30] Analyzed the performance of offloading systems operating in wireless environments. In this work, the authors take into account three circumstances of executing an application, thereby estimating the efficiency of offloading. They are the cases when the application is performed locally (without offloading), performed in ideal offloading (without failures), and performed with the presence of offloading and failure recoveries. In the last case, when failure occurs, the application will be re-offloaded. This approach only re-offloads the failed tasks, thereby improving the execution time. However, this solution has some limitations. That is, the mobile environment is considered as a wireless ad hoc local area network (i.e., broadband connectivity is not supported). Also, during offloading execution, a disconnection of a mobile device is treated as a failure.

c. Interoperability: Bring-Your-Own-Device (BYOD) policy creates interoperable challenges [34]. It's possible that there is an assorted mix of mobile devices including Android, iPhone, BlackBerry and others being used by employees in an organization or a group of people sharing a network. In this kind of situation according to the nature of cloud applications being used and operating system of mobile device interoperability issue can prove to be a major challenge in pulling/pushing data across multiple devices [35]. BOYD policy acceptance forces developers to think of a wide range of new security and management features that have to be built into application, providing safe access to company data [7]. By using context and location information mobile access can be optimized. Context aware services exploit data collected from terminal sensors or network sensors measuring network status and load. Network services and consumer application both uses these information.

d. Cloud Application Flexibility: an application is going to be supported by certain mobile cloud Infrastructure or not, can easily be judged on the basis of its requirements against the cloud infrastructure characteristics along the device, network bandwidth and latency vectors. Different applications' needs are different for its respective cloud infrastructure attributes (computation intensity, network bandwidth, and network latency). In high-demand applications transmission and latency delay can be minimized by considering 'near bye' data centres. And for a highly immersive application mobile cloud infrastructure can go for Wi-Fi offload that reduce latency further which is generally required by such applications [31]

e. Mobile Cloud Convergence: in order to achieve advantage of mobility by integrating cloud computing to mobile world, Data distribution is the key issue [7]. Limitation of mobile devices for their computing power makes task distribution very important as the computing power of mobile devices is not powerful enough for making these devices to be the main computing platform. Mobile cloud convergence provides performance improvement, longer battery life and a solution to the computation power problem. Basic approach of mobile cloud convergence is to partition application such that parts that need more computation run on the cloud and the remaining parts associated with the user interface run on the mobile device [7]. As a single process is being partitioned here so inter-process communication (IPC) is very important to realize this convergence. An improved and optimal PI calculation algorithm can be achieved by optimizing mobile cloud convergence. Wireless technologies, advanced electronics and internet are overlapped and integrated to achieve pervasive and ubiquitous computing [33].

3.3 Security Challenges

Trust, Security and privacy are never ending issues in mobile cloud computing. These issues are inherited from the various domains from which mobile cloud computing is derived [9]. Moreover, since mobile cloud computing is a combination of mobile networks and cloud computing [36], [9], security threats of mobile cloud computing could be divided into three; security threats to mobile devices, security threats to cloud platform and application containers and security threats to communication channels [12], [9]. Hence, security whether of cloud or of mobile devices is explained through listing prevalent threats and corresponding security measures to them [37].

The protection of user's privacy and data/information secrecy from adversary is a key to establish and maintain consumer's trust in the mobile platform, especially in mobile cloud computing [10]. In the following, the security related issues in mobile cloud computing is introduced in two categories: the security for mobile users and the security for data. Also, some solutions to address these issues are reviewed.

4.0 Security Issues Relating to Mobile Devices

As far as mobile devices are concerned, security remains a key concern. As if a device gets stolen or misplaced, crucial data may be compromised. Data misuse from stolen/misplaced devices can be avoided by wiping of mobile devices remotely. This feature is generally provided by most of the mobile manufacturers and wireless carriers [35]. Mobile devices such as PDAs, cellular phones, smart phones etc. are vulnerable to numerous security threats like malicious codes (e.g., viruses, worms, and Trojan horses). Global Positioning System (GPS) of mobile devices could also raise privacy issues for subscribers. The following security issues relating mobile devices are identified.

i. **Privacy and Confidentiality**: Providing private information such as indicating your current location and users' important information creates scenarios for privacy issues. With the advantages of GPS positioning devices, the number of mobile users using location based services (LBS) increases. However, the LBS face a privacy issue when mobile users provide private information such as their current location [10]. This problem becomes even worse if an adversary knows the users' important information. Location Trusted Servers (LTS) [38] is presented to address this issue. As shown in figure 2, after receiving the mobile user's request, LTS gathers their location information in a certain area and cloaks the information called 'cloak region' based on k-anonymity concept [39], [10] to conceal the user's information. The 'cloaked region' is sent to LBS, so LBS know general information about the users but cannot identify them. [40] points out the problem that if LTS reveals the users' information, or if LTS colludes with LBS, the user's information will be in danger. The authors propose to generate the 'cloaked region' on mobile devices based on Casper Cloaking Algorithm [41]. Meanwhile, gathering the information of other users around the sender will be done on the cloud to reduce cost and improve speed and scalability. When launching the program on the sender's mobile devices, the program will require the cloud to provide information about surrounding users. After that, the mobile client will generate the 'cloaked region' to the LBS. In this way, both LTS and LBS cannot know the sender's information [10].

There are various policies and schemes such as Fair Information Practice Principles (FIPP) being proposed which require rigorous controls and procedures to protect the privacy of individuals [7]. Risk of privacy exposure, identity theft, and fraud can be reduced by implementing enhanced protection measures for sharing data in interconnected systems, implementing monitoring capabilities and protocols, and educating users about proper social media safe surfing [7]. By establishing policies regarding use of social media and implementing processes to protect their infrastructures from unauthorized use of social media an organization can protect themselves from serious legal and security-related problems. Otherwise their information infrastructure and reputation both will be irreparably damaged.

Encryption provides most effective way to maintain integrity and confidentiality of information. Encryption favours data storage and transport but it fundamentally prevents data processing. Therefore, initially it was quite useless to send encrypted data to cloud providers for processing. But this challenge has been met by homomorphic cryptography (HC) which ensures that operations performed on an encrypted text results in an encrypted version of the processed text [42].

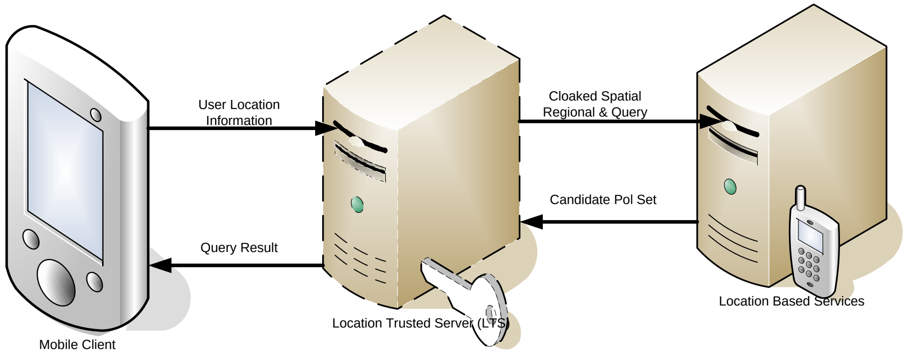
User Location Information
Cloaked Spatial Regional & Query
Candidate PoI Set
Query Result
Mobile Client
Location Trusted Server (LTS)
Location Based Services

Figure 4.1: Overall Architecture of Spatial Cloaking [10].

ii. **Security for Mobile Applications:** The simplest way to detect security threats of any mobile device is by installing and running security software (like Kaspersky, McAfee, and AVG antivirus programs etc.). However, since mobile devices have limited processing power and energy supply, protecting them from the threats is more difficult than that of resourceful device like the PC [7]. Several approaches have been developed for example; since it is impossible to keep running antivirus programs on mobile device as it reduces the battery lifetime, [43], propose that we can move the threat detection capabilities to clouds. Before mobile users could use a certain application, it should go through some level of threat evaluation. All file activities to be sent to mobile devices will be verified if it malicious or not. This paradigm is an extension of the existing Cloud Anti-virus platform that provides an in-cloud service for malware detection. The advantage of in-cloud detection of malware enables the use of multiple antivirus engines in parallel by hosting them in virtualized containers [44], [10].

However, to apply CloudAV platform for the mobile environment, a mobile agent should be improved and customized to fit in the mobile devices. [43] Builds a mobile agent to interact with the CloudAV network service for the Linux-based Maemo platform implemented on a Nokia N800 mobile device. The mobile agent is deployed in Python and uses the [45] framework to interpose on the system events. [46] Demonstrates the efficiency of using cloud computing for detecting malicious software on mobile devices. They presented a paradigm in which attack detection for smart phone is performed on a remote server in the cloud. Similarly, instead of running an antivirus program locally, the smart phone records only a minimal execution trace and transmits it to the security server in the cloud. This approach therefore enhances the efficiency of detecting malware and also improve battery lifetime up to 30%. Although storing a large amount of data/applications on a cloud has its own benefits but integrity, authentication and digital rights of data/applications should be taken into consideration [10].

4.1 Security Issues Relating to Cloud Platform and Application Containers

Although both mobile users and application developers benefit from storing a large amount of data/applications on a cloud, they should be careful of dealing with the data/applications in terms of their integrity, authentication, and digital rights. The data related issues in mobile cloud computing is as follows:

i. **Integrity**: Mobile users are often concerned about their data integrity on the cloud. Several solutions are proposed to address this issue [47], [48]. However, such solutions do not take into consideration the energy consumption of mobile users. [48] Considers the energy consumption issue. This scheme consists of three main components: a mobile client, a cloud storage service, and a trusted third party. The scheme performs three phases: the initialization, update and verification. In the first phase, files (F_x) that needs to be sent to the cloud will be assigned with a message authentication code ($MACF_x$). These $MACF_x$ will be stored locally, while the files will be sent and stored on the cloud. In the update phase, a case where the user wants to insert the data into file ($F_{x)}$ is considered. The cloud then sends the file (F_x) to this user. At the same time, the cloud also sends a requirement to the Trusted Crypto Coprocessor (TCC) to generate $MAC'F_{x.}$ Trusted Crypto Coprocessor then sends $MAC'F_x$ to the client to verify F_x by comparing it with $MACF_x$. If everything is properly authenticated, the user can insert/delete data. Finally, the mobile client can request the integrity verification of a file, collection of files, or the whole file system stored in the cloud. This phase starts when the user sends a requirement to verify integrity of files to TCC. The TCC then retrieves files that need to be checked from the cloud and generates $MAC'F_x$ to send to the client. The client only compares the retrieved $MAC'F_x$ and $MACF_x$ that are stored on its device to verify the integrity of such files. This technique saves both energy for the mobile device and bandwidth for the communication network [10].

ii. **Authentication**: [41] Presents an authentication method using cloud computing to secure the data access suitable for mobile environments. This scheme combines TrustCube [49] and implicit authentication [50], [51] to authenticate the mobile client. TrustCube is a policy-based cloud authentication platform using the open standards, and it supports the integration of various authentication methods [10]. The authors build an implicit authentication system using mobile data (e.g., calling logs, SMS Message, Website access, and location) for existing mobile environment. The system requires input constraints that make it difficult for mobile users to use complex passwords. As a result, this often leads to the use of simple and short passwords or personal identification numbers (PINs). Figure 3, shows the system architecture and how the system secures the user's access. When a web server receives a request from a mobile client, the web server redirects the request to the integrated authenticated (IA) service along with the details of the request. The IA service retrieves the policy for the access request, extracts the information that needs to be collected, and then sends an inquiry to the IA server through the trusted network connect protocol. The IA server receives the inquiry, generates a report and sends it back to the IA service. After that, the IA service applies the authentication rule in the policy and determines the authentication result and sends the authentication result back to the web server. Based on the authentication result, the web server either provides the service or denies the request.

iii. **Digital Rights Management**: The unstructured digital contents (e.g., video, image, audio, and e-book) have often been pirated and illegally distributed. Protecting these contents from illegal access is of crucial importance to the content providers in mobile cloud computing like traditional cloud computing and peer-to-peer networks. [52] Proposed Phosphor, a cloud-based mobile digital rights management (DRM) scheme with a subscriber identity module (SIM) card in mobile phone to improve the flexibility and reduce the vulnerability of its security at a low cost. The Authors design a licence state word (LSW) located in a SIM card and the LSW protocol based on the application protocol data unit (APDU) command. In addition, the cloud-based DRM with an efficient unstructured data management service can meet the performance requirement with high elasticity [10]. Thus, when a mobile user receives the encrypted data (e.g., video stream) from the content server via real-time support protocol, the user then uses the decryption key from a SIM card via APDU command to decode. If the decoding is successful, the mobile user can watch this video on his/her phone. The drawback of this solution is that it is still based on the SIM card of the mobile phone; so, it cannot be applied for other kinds of access; that is, a laptop using Wi-Fi to access these contents [10], [9].

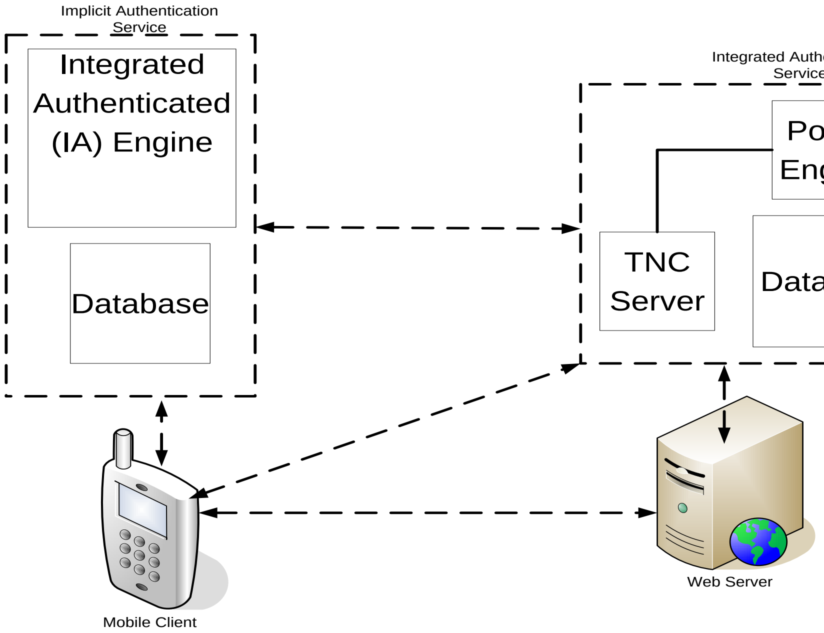
Implicit Authentication Service
Integrated Authenticated (IA) Engine
Database
Integrated Authenticated Service
Policy Engine
TNC Server
Database
Web Server
Mobile Client

Figure 4.2: TrustCube Architecture

4.3 Security Issues Relating to Communication Channels

The security issues may be discussed as follows:

i. Network Monitoring:

In addition to latency and bandwidth problems network performance monitoring is also an important issue which needs proper concern and care [7]. It is critical to have a dynamic cloud performance system that can allow traffic re-routing, access swapping and handover. With all these key challenges given mobile computing is still a viable business and is being preferred by more cloud users.

ii. **Malicious Attacks**: All networks are susceptible to one or more malicious attacks. As more external website are being accessed, malicious actors will have more opportunities to access the network and operational data of users. Implementing security controls across all Web 2.0 servers and verifying these rigorous security controls can reduce the threats to internal networks and operational data. Additionally, separating Web 2.0 servers from other internal servers may further mitigate the threat of unauthorized access to information through social media tools and Websites [7]. Some of the potential attack vectors criminals may attempt include [7]: (i) Man-in-the-middle Cryptographic Attacks: This attack is carried out when an attacker places himself between two users. In this kind of attack, attacker places himself in the communication path and after that, it is up to him to know what to do, he can intercept and modify communication [7]. (ii) Denial of Service DoS Attacks: The cloud is more susceptible to DoS attacks because more than one client can access cloud at the same time, which makes DoS attack much more damaging. Twitter has suffered a devastating DoS attack in 2009 [7]. (iii) Side Channel Attacks: In this kind of attacks a malicious virtual machine is placed in close proximity of a target cloud server to compromise the cloud security and then a side channel attack is launched [7]. (iv) Authentication Attacks: Authentication is one of the weak points in case of hosted and virtual services and is generally been targeted. A user can be authenticated in number of ways and these mechanisms and methods which are used to secure the authentication process are frequently been targeted by the attackers.

4.4 Future of Mobile Cloud Computing

As technology advances and mobile devices with better operating systems become ubiquitous, devices such as PDA cell phones, cell phones working with WLANs and cell phones with MP3 players will integrate each others technology. While wired devices will be phased-out of usage, mobile application development such as Android apps development will ensue.

5 Conclusion

In this paper, we have covered several mobile cloud computing approaches, applications, and challenges. Much other related exist, but the purpose of this paper is to provide an overview of the wide range of mobile cloud computing possibilities and challenges. Mobile cloud computing will continue to be the technology trend both now and the future as in combines the benefits of cloud computing, wireless mobile networks and mobile devices. The integration of these technologies raises issues and challenges such as security, privacy and trust. Although these issues are being addressed by various researchers, they remained a never ending issues associated with mobile cloud computing.

REFERENCES

[1] Rashmi, A. Badjad, Monika Srivastava & Amit Sinha "Survey on Mobile Cloud Computing," International Journal of Engineering Sciences & Emerging Technologies,vol. 1, Issue 2, pp. 8 - 19, February 2012.

[2] Voas, J., & Zhang, J. "Cloud Computing: New Wine or Just a New Bottle?" *IT Professional*, vol. 11, No. 2, PP. 15-17, April 2009.

[3] Abah Joshua, Francisca N. Ogwueleka "Cloud Computing with Related Enabling Technologies" International Journal of Cloud Computing and Services Science (IJ-CLOSER), vol. 2, No. 1, pp. 40 – 49, February 2013.

[4] Kovachev D., Renzel R. Klamma & Cao Y., "Mobile Community Cloud Computing: Emerges and Evolves," in Proceedings of the IEEE First International Workshop on Mobile Cloud Computing, Kansas MO, USA, 2010.

[5] Niroshinie F., Seng W.L., & Wenny R. "Mobile Cloud Computing: A Survey," Elsevier; Future Generation Computer Systems, vol. 29, pp. 84 - 106, 2013. DOI: 10.1016/j.future.2012.05.023.

[6] Satyanarayanan M., Bahl P., C' aceres R. & Davies N. "The Case for VM-Based Cloudlets in Mobile Computing," IEEE pervasive Computing, vol. 8, No. 4, pp. 14 – 23, October 2009.

[7] Deepti Sahu, Shipra Sharma, Vandana Dubey & Alpika Tripathi, "Cloud Computing in Mobile Applications," International Journal of Scientific and Research Publications, Vol. 2, Issue 8, PP. 1 - 9, August 2012.

[8] Weiser Mark, "The Computer for the 21st Century." Scientific American, 265(3): 94-104, 1991.

[9] Soeung-Kon Victor Ko, Jung-Hoon Lee, Sung Woo Kim, "Mobile Cloud Computing Security Considerations," Journal of Security Engineering, Vol. 9, No. 2, PP. 143-150, 2012.

[10] Hoang T.D., Lee C., Niyato D. & Wang P., "A Survey of Mobile Cloud Computing: Architecture, Applications and Approaches." Wireless Communications and Mobile Computing , John Wiley & Sons Ltd., PP. 1-27, 2011. DOI: 10.1002/wcm.1203.

[11] Rajendra M.P., Jayadev G. & Murti P.R.K., "Mobile Cloud Computing: Implications and Challenges," Journal of Information Engineering and Applications. Vol 2, No.7, PP. 7-15, 2012.

[12] Niroshinie F., Seng W.L., & Wenny R., "Mobile Cloud Computing: A Survey," Elsevier; Future Generation Computer Systems, 29(2013) 84-106, 2013. DOI: 10.1016/j.future.2012.05.023.

[13] Perez S, "Mobile Cloud Computing: $9.5 Billion by 2014," readwrite.com, February 2010 available at http://readwrite.com/2010/02/22/mobile_cloud_computing_95_billion_by_2014#awesm=~otXBY23FkMooue.

[14] Yang X., Pan T. & Shen J., "On 3G Mobile E-commerce Platform Based on Cloud Computing," in Proceedings of the 3rd IEEE International Conference on Ubi-Media Computing (U-Media), PP. 198-201 August 2010.

[15] Dai J. & Zhou Q., "A PKI-based Mechanism for Secure and Efficient Access to Outsourced Data." in Proceedings of the 2nd International Conference on Networking and Digital Society (ICNDS), 640, 2010.

[16] Chen X., Liu J., Han J., & Xu H., "Primary Exploration of Mobile Learning Mode under a Cloud Computing Environment," in Proceedings of the International Conference on E-Health Networking, Digital Ecosystems and Technologies (EDT), Vol. 2, PP. 484 – 487, June 2010.

[17] Gao H. & Zhai Y., "System Design of Cloud Computing Based on Mobile Learning," in Proceedings of the 3rd International Symposium on Knowledge Acquisition and Modelling (KAM), PP. 293 – 242, November 2010.

[18] Jian L., "Study on the Development of Mobile Learning Promoted by Cloud Computing," in Proceedings of the 2nd International Conference on Information Engineering and Computer Science (ICIECS), PP. 1, December 2010.

[19] Rieger R. & Gay G., "Using Mobile Computing to Enhance Field Study." In Proceedings of the 2nd International Conference on Computer Support for Collaborative Learning (CSCL), 218-226, 1997.

[20] Ferzli R. & Khalife I., "Mobile Cloud Computing Educational Tool for Image/Video Processing Algorithms." In Digital Signal Proceedings Workshop and IEEE Signal Processing Education Workshop (DSP/SPE), 529, 2011.

[21] Kopec D., Kabir M.H., Reinharth D., Rothschild O., & Castiglione J.A., "Human Errors in Medical Practice: Systematic Classification and Reduction with Automated Information Systems," Journal of Medical Systems, Vol. 27, No. 4, PP. 297 – 313, 2003.

[22] Varshney U., "Pervasive Healthcare and Wireless Health Monitoring." Journal on Mobile Networks and Applications. 12(2-3); 113-127, 2007.

[23] Doukas C. & Pliakas T. & Maglogiannis I., "Mobile Healthcare Information Management Utilizing Cloud Computing and Android OS." In Annual International Conference of the IEEE on Engineering in Medicine and Biology Society (EMBC), 1037-1040, 2010.

[24] Tang W.T., Hu C.M. & Hsu C.Y., "A Mobile Phone Based Homecare Management System on the Cloud." In Proceedings of 3rd International Conference on Biomedical and Informatics (BMEI), 2442, 2010.

[25] Li Z., Wang C. & Xu R., "Computation Offloading to Save Energy on Handheld Devices: A Partition Scheme," in Proceedings of the 2001 International Conference on Compilers, architecture, and Synthesis for Embedded Systems (CASES), PP. 238 – 246, November 2001.

[26] Cuervo E., Balasubramanian A., . . . & Dae-ki C. et al., "MAUI: Making Smart phones Last Longer with Code Offload." In Proceedings of the International Conference on Mobile Systems, Applications and Services, 49-62, 2010.

[27] Wang S. & Dey S., "Rendering Adaptation to Address Communication and Computation Constraints in Cloud Mobile Gaming." In IEEE Global Telecommunications Conference (GLOBECOM), 1-6, 2011.

[28] Jitendra M., "Extending the Principles of Cloud Computing in Mobile Domain." D.C. Wyld et al. (Eds.): NeCoM/WeST/WiMoN 2011, CCIS 197, PP. 197-203, 2011. ©Springer-Verlag Berlin Heidelberg 2011.

[29] Rudenko A., Reiher P., Popek G.J. & Kuenning G.H., "Saving Portable Computer Battery Power Through Remote Process Execution." Journal of ACM SIGMOBILE on Mobile Computing and Communications Review 2(1), 1998.

[30] Ou S., Yang K., Liotta A. & Hu L., "Performance Analysis of Offloading Systems in Mobile Wireless Environments." In Proceedings of the IEEE International Conference on Communications (ICC), 1821, 2007.

[31] Kyung M., "Mobile Cloud Computing Challenges". Corporate Technology Strategist, 2010. Available at http://www2.alcatel-lucent.com/blogs/techzines/2010/mobile-cloud-computing-challenges/

[32] Irmee L., "Overcoming Challenges in Mobile Cloud Computing," Cloudtimes, 2011. Available at http://cloudtimes.org/2011/07/11/overcoming-challenges-in-mobile-cloud-computing/

[33] Min C., Jonghyuk P., & Young-Sik J., "Mobile Cloud Computing Framework for a Pervasive and Ubiquitous Environment." Springer Science Business Media, LLC 2011.

[34] Colin S., "BYOD Policy", Techtarget, 2011. Available at http://searchconsumerization.techtarget.com/definition/BYOD-policy.

[35] Roger C. (2011). "Mobile Cloud Adoption Challenges in the Enterprise,"Cloudcomputingtopics, April 16th, 2011. Available at http://cloudcomputingtopics.com/2012/04/mobile-cloud-adoption-challenges-in-the-enterprise/

[36] Eileen B., "Moving from Cloud Computing to Mobile Cloud Computing." Agilis Solutions, All about the Cloud, May 23-26, 2011.

[37] Aubery-Derrick S., "Detection of Smart Phone Malware", Electronic and Information Technology University Berlin Unpublished PhD. Thesis. PP. 1-211, 2011.

[38] Zhangwei H., & Mingjun X. (2010). "Distributed Spatial Cloaking Protocol for Location Privacy," In Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), 468, 2010.

[39] Sweeny L. (2002). "K-anonymity: A Model for Protecting Privacy." International Journal of Uncertainty Fuzziness and Knowledge-Based Systems, 10(5): 557-570, 2002.

[40] Wang S. & Wang X.S., "In-device Spatial Cloaking for Mobile Users Privacy Assisted by the Cloud." In Proceedings of the 11th International Conference on Mobile Data Management (MDM), 381, 2010.

[41] Chow C.Y., Mokbel M.F., & Aref W.G.C, "Query Processing for Location Services without Compromising Privacy," ACM Transaction on Database Systems (TODS), 34(4): 1-48, 2009.

[42] Peter S., "Challenges of Cloud Networking Security," Techreport, pp. 137-210, 2010. Available at http://www.hpl.hp.com/techreports/2010/HP-210-137.pdf

[43] Oberheide J., Veeraraghavan K., Cook E., Flinn J., & Jahanian F., "Virtualized In-cloud Security Services for Mobile Devices," In Proceedings of the 1st Workshop on Virtualization in Mobile Computing (Mobivirt), 31-35, 2008.

[44] Watson M.R., "Malware Detection in the Context of Cloud Computing." PGNet, PP. 1-5, 2012.

[45] Dazuko O.J., "An Open Solution to Facilitate On-access Scanning," In Proceedings of the 13th Virus Bulletin International Conference, 2003.

[46] Portokalidis G., Homburg P., Anagnostakis K., & Bos H. (2010). "Paranoid Android: Versatile Protection for Smart phones," In Proceedings of the 26th Annual Computer Security Application Conference (ACSAC), 347-356, 2010.

[47] Wang W., Li Z., Owens R., & Bhargava B., "Secure and Efficient Access to Outsourced Data," in ACM Cloud Computing Security Workshop (CCSW), PP. 55 – 66, 2009.

[48] Itani W., Kayssi A., & Chehab A., "Energy-efficient incremental integrity for securing storage in mobile cloud computing," International Conference on Energy Aware Computing (ICEAC), PP.1, January 2011.

[49] Song Z., Molina J., Lee S., Kotani S., & Masuoka R., "TrustCube: An Infrastructure that Builds Trust in Client," In Proceedings of the 1st International Conference on Future of Trust in Computing, 2009.

[50] Jakobsson M., Shi E., Golle P., & Chow R., "Implicit Authentication for Mobile Devices," in Processing of the 4th USENIX Workshop on Hot Topics in Security (HotSec), August 2009.

[51] Shi E., Niu Y., Jakobsson M., & Chow R., "Implicit Authentication through Learning User Behaviour," In Proceedings of the Implicit Authentication Security Conference (ISC), October 2010.

[52] Zou P., Wang C., Liu Z., & Bao D., "Phosphor: A Cloud-Based DRM Scheme with Sim Card," in Proceedings of the 12th International Asia-Pacific on Web Conference (APWEB), PP. 459, June 2010.

BIOGRAPHY OF AUTHORS

Victor Onomza Waziri obtained his BSc/Ed (Maths) from Usmanu Danfodiyo University Sokoto (1990), M. Tech (Applied Mathematics) and PhD (Applied Mathematics) based-on Computational Optimization in 1998 and 2004 respectively From the Federal University of Technology, Minna-Nigeria. He did his PostDoctoral Fellowship in Computer Science at the University of Zululand, South Africa in 2007. He is the Current Head of Cyber Security Science, Federal University of Technology, Minna-Nigeria. His research works are in the fields of Computational Optimization, Modern Cryptography, CyberSecurity/ Malware Detection, Mobile Cloud Computing Security, Programming and Network Security. He has published many academic papers at both local and International Scene
Victoor.waziri@futminna.edu.ng/ onomzavictor@gmail.com

Joshua Abah received a B.Tech (Hons) in Computer Science from Abubakar Tafawa Balewa University Bauchi, Nigeria in 2005, and MSc. in Computer Science from Bayero University Kano, Nigeria in 2011. He is at present a Ph.D fellow in Computer Science at the Federal University of Technology Minna, Nigeria. He is currently working in the academia where he has been for the past seven years. His research interests include Mobile Cloud Computing Security, Network Security, Cloud Computing, Virtualization, Scheduling Algorithms, QoS and Computer Education. He has well over eight journals both local and international and has authored five textbooks to his credit.
ehoshua_a@yahoo.com

Prof. Olumide Sunday Adewale, is a Professor of Computer Science. He lectures at the Federal University, Akure-Nigeria. Has published many academic papers at both local and at International Scene. He is a Visiting Professor to the Department of Computer Science, Federal University of Technology, Minna-Nigeria.
adewale@futa.edu.ng

Muhammad Bashir Abdullahi received B.Tech (Honors) in Mathematics/Computer Science from Federal University of Technology, Minna-Nigeria and Ph.D. in Computer Science and Technology from Central South University, Changsha, Hunan, P. R. China. His current research interests include trust, security and privacy issues in wireless sensor and ad hoc networks, Internet of things and information and communication security.
Email: el.bashir02@futminna.edu.ng