Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 7 No. 3, September, 2016 - www.cisdijournal.net

Security Issues in Mobile Cloud Computing

Elusoji, A.A. (Ph.D)
Department of Computer Technology
Yaba College of Technology
Yaba – Lagos, Nigeria
elusoji872@yahoo.com

Akeredolu, G.R
Department of Computer Science
Federal Polytechnic
Idah – Nigeria
akmasgbenga3@gmail.com

Aiyegbusi A.E
Department of Computer Science
Micheal Otedola College of Primary Education
Epe-Lagos, Nigeria
aiyegbusied@yahoo.com

ABSTRACT

Mobile Cloud Computing (MCC) has revolutionized the way in which mobile subscribers across the globe leverage services on the go. As MCC is still at the early stage of development, it is necessary to grasp a thorough understanding of the technology in order to point out the direction of future research. Mobile Cloud Computing (MCC) is a combination of three main parts; they are mobile device, cloud computing and mobile internet. With the help of MCC, a mobile user gets a rich application delivered over the Internet and powered by cloud-backed infrastructure. The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. Now a day's the major concern for mobile user is security and protection in mobile cloud computing. MCC refers to the availability of cloud computing services in a mobile environment. There are number of loopholes and challenges exist in the security policies of MCC. This paper present a review of MCC, cloud computing service models, and deployment models, mobile cloud computing architecture, mobile cloud computing services and the various security challenges and solutions.

Keywords: Mobile phones, Mobile Cloud Computing (MCC), Security, Privacy.

CISDI Journal Reference Format
Elusoji, A.A., Akeredolu, G.R & Aiyegbusi A.E (2016): Security Issues In Mobile Cloud Computing.
Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 7 No 3. Pp 39-46
Available online at www.cisdijournal.net

1. INTRODUCTION

Mobile devices are increasingly becoming an essential part of human life as the most effective and convenient communication tools not bounded by time and place. The rapid progress of mobile computing (MC) becomes a powerful trend in the development of wireless communications technology as well as commerce and industry fields. MCC is the combination of mobile computing and cloud computing, this provides full access to all technology resources through the cloud "Anytime, Anywhere, Anyhow".

Cloud computing is a paradigm for enabling a convenient way, on-demand easy network access to a shared pool of configurable computing resources like networks, servers, storage, applications and services and also provides a high level abstraction of computation and storage with a very less management effort with the help of service models and the deployment models.
Mobile cloud computing is a model for transparent elastic augmentation of mobile device capabilities via 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 devices [1]. Recently, the MCC is becoming a new hot technology. And the security solution for it has become a research focus. With the development of the mobile cloud computing, new security issues are there, which needs more security approaches.

2. SERVICE MODELS

Cloud computing can be divided into three service models:

Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). An agency may procure any combination of these service models depending on their particular needs [3].

2.0.1 Software as a Service (SaaS)

Software as a Service is a delivery model where the software and the associated data is hosted in a cloud environment by a third party such as a cloud service provider (CSP). Typically the user, such as a staff member in an agency, accesses the software on demand using a browser on a computer or mobile device. The agency does not buy the software. Instead the CSP licenses the SaaS to the agency, which then enables multiple users to access the software [3].

2.0.2 Platform as a Service (PaaS)

Platform as a Service is a delivery model where a CSP provides an online software development platform for an organization such as an agency. The agency's developers use the CSP's computing environments, tools, and libraries to create, test, manage, and host software applications. By moving the entire development platform to the CSP, agencies can lessen the cost and management burden of application development [3].

2.0.3 Infrastructure as a Service (IaaS)

Infrastructure as a Service is a delivery model where CSPs provide the necessary hardware and software upon which a customer can build a customized computing environment. The CSP typically provides an unmanaged environment that enables the customer, such as an agency, to have any "guest" resources it needs installed: operating systems, software bundles, storage capabilities, etc. The agency retains full control of the computing environment and is responsible for configuring and maintaining the guest operating systems and associated applications and resources. The CSP, however, is responsible for maintaining all.

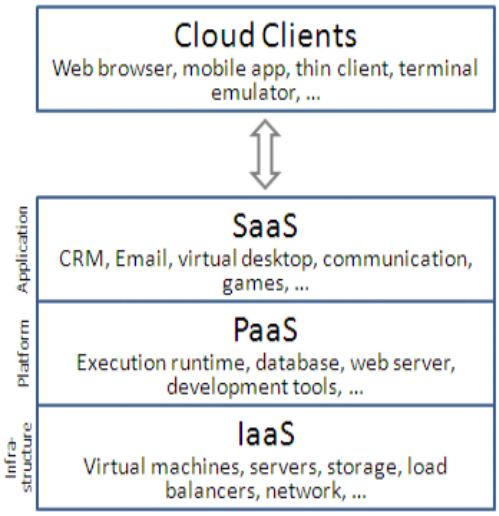

Figure 2.0: Service Model.

2.1 Deployment Models

Businesses can choose to deploy applications on Public, Private, Hybrid clouds or the newer Community Cloud. Here are some fundamentals of each to help with the decision-making process [4].

2.1.1 Public Cloud

A service provider who hosts the cloud infrastructure makes public clouds available to the general public. Generally, public cloud providers like Amazon AWS, Microsoft and Google own and operate the infrastructure and offer access over the Internet. With this model, customers have no visibility or control over where the infrastructure is located. It is important to note that all customers on public clouds share the same infrastructure pool with limited configuration, security protections and availability variances [4].

2.1.2 Private Cloud

Private cloud is cloud infrastructure dedicated to a particular organization. Private clouds allow businesses to host applications in the cloud, while addressing concerns regarding data security and control, which is often lacking in a public cloud environment. It is not shared with other organizations, whether managed internally or by a third-party, and it can be hosted internally or externally [4].

2.1.3 Hybrid Cloud

Hybrid Clouds are a composition of two or more clouds (private, community or public) that remain unique entities but are bound together offering the advantages of multiple deployment models. In a hybrid cloud, you can leverage third party cloud providers in either a full or partial manner; increasing the flexibility of computing. Augmenting a traditional private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload [4].

2.1.4 Community Cloud

A community cloud is a is a multi-tenant cloud service model that is shared among several or organizations and that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider. Community clouds are a hybrid form of private clouds built and operated specifically for a targeted group. These communities have similar cloud requirements and their ultimate goal is to work together to achieve their business objectives [4].

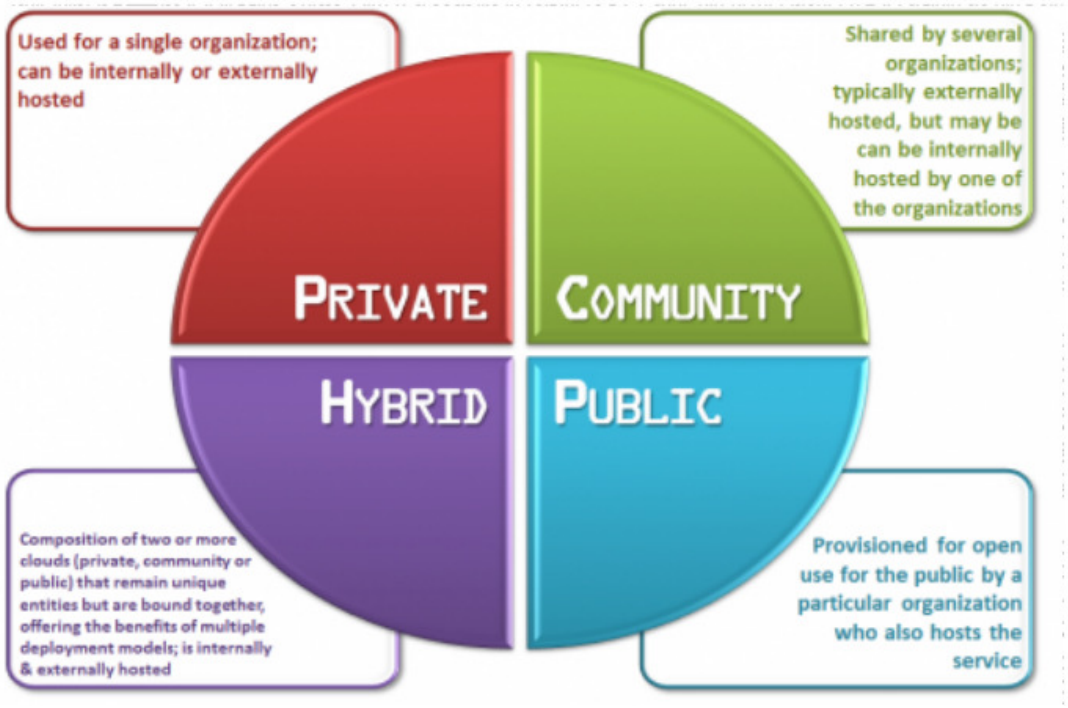

Figure 2.1: Deployment Models

3. MOBILE CLOUD COMPUTING ARCHITECTURE

In Mobile Cloud Computing (MCC) architecture Mobile devices are connected to the mobile networks via base stations that establish and control the connections and functional interfaces between the networks and mobile devices. Mobile users' requests and information are transmitted to the central processors that are connected to servers providing mobile network services. The subscribers' 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 [2]

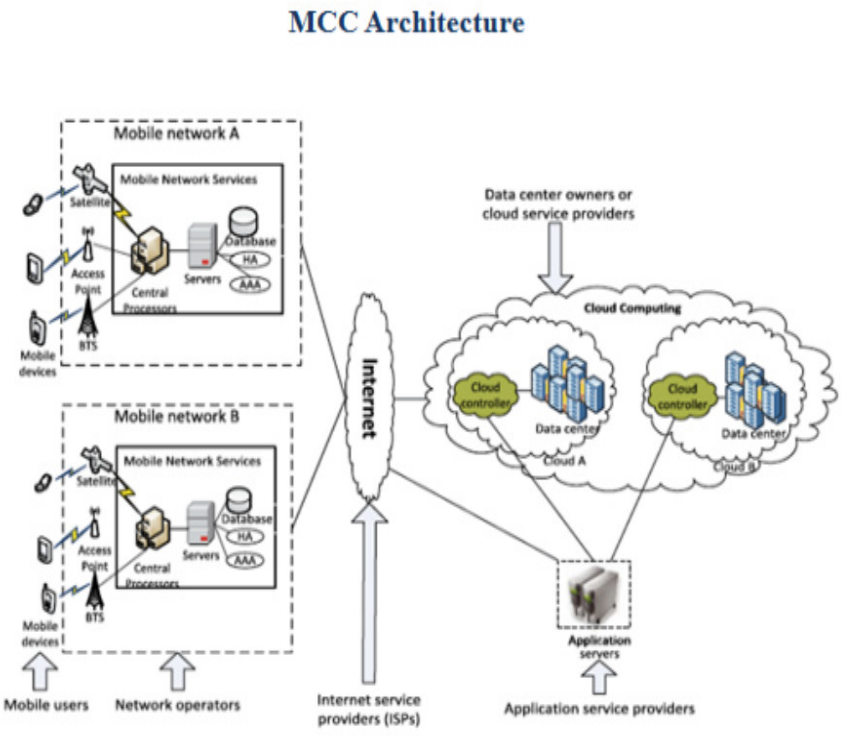

Figure 3: MCC Architecture

4. MOBILE CLOUD COMPUTING SERVICES

A virtualized environment as a service is been created by using Mobile Cloud Computing (MCC). The virtualized environment allows the user to use the different services in different clouds using cloud controller, the service provider enables the user to get connected to the cloud with help of internet .The mobile device just an interface to access mobile apps, contacts and data from the cloud. The mobile cloud is most often viewed as a SaaS cloud, meaning that computation and data handling are usually performed in the cloud [8].

4.1 Mobile phone without SIM (Subscriber Identity Module) Card

In general the mobile phones have the SIM card to store contacts but what happens when the mobile phone is lost, all the contacts are lost and the misuse of SIM can also happen unless and until the SIM is deactivated. Mobile Cloud Computing (MCC) enables the user to use mobile phone without a SIM card. The user must have the username and password must be there to access the contacts. The 4G Technology is helping out to have mobile phone without a SIM card, example Samsung introduced the Yes Buzz 4G cloud phone in Malaysia in January 2011. It has no SIM card and allows contacts to be saved and synchronized on the Internet [5].

4.2 Mobile apps the state of art of Mobile Cloud Computing (MCC)

Cloud apps have the power of a server-based computing infrastructure accessible through an app's mobile interface. Like an ipod touch which run all online apps from play store. The mobile will run all online apps from and on cloud [9]. The mobile apps will be available on cloud, the mobile user generally download the apps from the App store, every mobile phone provider have their own cloud, the user access to that cloud and downloads the apps into their mobile like APPLE has icloud, Apple cloud were APPLE apps are available, it is called as APPLE store. Soon the downloading concept of apps on to mobile will perish, the mobile user can use the cloud controller and run the mobile apps on mobile cloud itself. The apps will be available on the mobile phone just like desktop shortcuts.

4.3 Huge amount of data is stored in Cloud
The huge amount of data can be stored on private clouds which are cheaply available which enables huge amount of data to be stored in cloud. Even the mobile is lost the data is safe in cloud and even the contacts. You have an ID to access the cloud you can access it from new mobile device too but the Authenticity, Authorization and Accountability is checked before accessing to the data. The data storage is made easier. There are more chances of mini phones in future, Mobile Cloud Computing allows to store data and retrieve the huge amount of data stored in cloud, the mobile device is merely an interface to access the data and making it a powerful device [7].

Resource Management of Mobile Cloud vComputing (MCC)
Mobile Cloud Computing manages the resources and creates the virtualized environment to use all the services in different clouds as if available in the mobile device itself. The resources available on the cloud are just used on mobile devices just like desktop shortcuts in computer systems. All these are well managed by mobile cloud computing [12].

HTML, CSS and Hypervisor
HTML5 enables to watch a video without a plug-in like Adobe Flash or Microsoft Silverlight, to store and access data such as e-mail messages and calendars, which helps make web applications more useful. CSS3 works with HTML5 to specify how elements of a page should be rendered. An HTML specification tells a web browser what to display, and a CSS specification tells the web browser how to display it. Hypervisor Another enabler for cross-platform applications is an embedded hypervisor, which allows a web application to run on any smart phone without being aware of the underlying architecture (mobile). The hypervisor allows other software to run in a virtualized environment [2]. Mobile platforms require the hypervisor to be built in.

5. CHALLENGES AND SOLUTIONS
Since mobile cloud computing is a combination of mobile networks and cloud computing, the security issues can be divided into.

5.1 Mobile network user's security

5.1.1 Security for mobile applications:
The simplest ways to detect security threats will be installing and running security software and antivirus programs on mobile devices. But since mobile devices are constrained with processing and power limitations, protecting them from these threats could be more difficult compared to regular computers. Instead of running anti-virus software or threat detection programs locally, mobile devices only performs lightweight activities such as execution traces transmitted to cloud security servers.

5.1.2 Privacy:
Providing private information such as indicating your current location and user's important information creates scenarios for privacy issues. For example, the use of location based services (LBS) provided by global positioning system (GPS) devices [13]. Threats for exposing private information could be minimized through selecting and analyzing the enterprise needs and require only specified services to be acquired and moved to the cloud.

5.2 Security Issues in Cloud:
There are nine major threats to security in clouds known as the notorious nine.

- Data Breaches
- Data Loss
- Account or Service traffic hijacking
- Insecure interfaces and APIs
- Denial of Service Ranks
- Malicious insiders
- Cloud Abuse
- Insufficient Due delligence
- Shared technology vulnerabilities.

Since the security issues fall in two categories, the security measure is also described as:

A. Mobile network user's security:

- Don't leave your mobile device unattended;
- Protect Your Device with Passwords: Enable your device's power-on login, system login authentication, and password-protected screen saver.
- Disable Wireless Connection When It Is Not In Use: WiFi, infrared, and Bluetooth devices are constantly announcing their presence if they are enabled.
- Protect your device with anti-virus software using the latest virus definitions.
- Remove Your Preferred Network List when using Public Wireless Service.
- Encrypt Your Wireless Traffic Using a Virtual Private Network (VPN).
- Turn off Ad-Hoc Mode Networking.
- Turn off Resource Sharing Protocols for Your Wireless Interface Card

B. Measures for cloud Security:

The data can be encrypted to reduce the impact of a breach, but if the encryption key is lost, the data is also lost. However, if offline backups of the data are kept to reduce data loss, the exposure to data breaches increases. A malicious hacker might delete a target's data out of spite but then, the data could be lost to a careless cloud service provider or a disaster, such as a fire, flood, or earthquake [10].

Compounding the challenge, encrypting the data to ward off theft can backfire if the encryption key is lost. The key to defending against this threat is to protect credentials from being stolen. Organizations should look to prohibit the sharing of account credentials between users and services, and they should leverage strong two-factor authentication techniques where possible. IT admins rely on interfaces for cloud provisioning, management, orchestration, and monitoring. APIs are integral to security and availability of general cloud services [14]. From there, organizations and third parties are known to build on these interfaces, injecting add-on services. "This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency". DoS outages can cost service providers customers and prove pricey to customers who are billed based on compute cycles and disk space consumed. While an attacker may not succeed in knocking out a service entirely, he or she "may still cause it to consume so much processing time that it becomes too expensive for you to run and you'll be forced to take it down yourself" [11].

From IaaS to PaaS to SaaS, the malicious insider has increasing levels of access to more critical systems and eventually to data. In situations where a cloud service provider is solely responsible for security, the risk is great. "Even if encryption is implemented, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack, " according to CSA. Organizations embrace the cloud without fully understanding the cloud environment and associated risks. For example, entering the cloud can generate contractual issues with providers over liability and transparency. What's more, operational and architectural issues can arise if a company's development team isn't sufficiently familiar with cloud technologies as it pushes an app to the cloud. CSA's basic advice is for organizations to make sure they have sufficient resources and to perform extensive due diligence before jumping into the cloud. "Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multicustomer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models, "according to the report.

The information on cloud can thus be secured by-

- Authentication - The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
- Authorization - Authorization is the process of giving someone permission to do or have something. In multiuser computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth) [6].
- Encryption - The translation of data into a secret code. Encryption is the most effective way to achieve data security.
- Integrity- Every mobile cloud user must ensure the integrity of their information stored on the cloud. Every access they make must me authenticated and verified. Different approaches in preserving integrity for one's information that is stored on the cloud is being proposed. For example, every information stored by each individual or enterprise in the cloud is tagged or initialized to them wherein they are the only one to have access (move, update or delete) such information. Every access they make must be authenticated assuring that it is their own information and thus verifying its integrity.

- Legal Provision- Distribution and piracy of digital contents such as video, image, audio, and e-book, programs should be criticized. The solutions to protect these contents from illegal access are applied such as encryption and decryption keys to access these contents.

6. CONCLUSION AND FUTURE WORKS

Cloud computing is clearly one of the most enticing technology areas of the current times due, at least in part to its cost-efficiency and flexibility. Security and privacy are one of the most challenging issues in MCC. The security threats have become obstacles in the rapid adaptability of the MCC paradigm. The lack of an in-depth study of the security and privacy in MCC was detected in current available literature. Therefore, this paper has attempted to provide more insight to this field of research by studying and theoretical comparison of different approaches proposed by the researchers to provide security and privacy in MCC. The limited processing power and memory of a mobile device dependent on inherently unreliable wireless channel for communication and battery for power leaves little scope for a reliable security layer.

Thus there is a need for a lightweight secure framework that provides security with minimum communication and processing overhead on mobile devices. There is a need for a secure communication channel between cloud and the mobile device. The secure routing protocols can be used to protect the communication channel between the mobile device and cloud. We also need to address issues pertaining to data security, network security, data integrity, authentication, authorization and access control. To achieve a secure MCC environment, security threats need to be studied and addressed accordingly. In the future, our research work focus on to propose a security model framework to enhance security and privacy in MCC.

Cloud computing offers on-demand network access to a shared pool of computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This paper discusses mobile cloud computing, its architecture, characteristics and the various security issues associated with it. It also deals with the measures to be taken for the prevention of the security problems.
In a way to have an appropriate Futuristic model and architecture for Cloud Computing, we have successfully illustrated the basic idea of what is Cloud Computing, different deployment and service models of Cloud Computing, emergence of cloud computing, Design and Implementation level issues faced during evolution of Cloud.

REFERENCES

[1] P. Theresa Joy and K. Poulose Jacob, "Cooperative Caching Framework for Mobile Cloud Computing", Global Journals Inc.(USA), Version 1.0, Online ISSN: 0975-4172 & Print ISSN: 0975-4350, vol. 13, no. 8, (2013)
[2] AppcoreBlog, http://blog.appcore.com/blog/bid/167543/Typesof-Cloud-Computing-Private-Public-and-Hybrid-Clouds
[3] A. N. Khana, M. L. M. Kiaha, S. U. Khanb and S. A. Madani , "Towards secure mobile cloud computing: A survey", Future Generation Computer Systems, vol. 29, Issue 5, (2013) July.
[4] M. R. Prasad, J. Gyani and P. R. K. Murti, "Mobile Cloud Computing: Implications and Challenges", Journal of Information Engineering and Applications, vol. 2, no. 7, (2012).
[5] Morshed, M. S. Jahan, M. M. Islam, M. K. Huq, M. S. Hossain and M. A. Basher, "Integration of Wireless Hand-Held Devices with the Cloud Architecture: Security and Privacy Issues", International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), (2011) October.
[6] W. Jia, H. Zhu, Z. Cao, L. Wei and X. Lin, "SDSM: A secure data service mechanism in mobile cloud computing", IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), (2011) April 10-15.
[7] D. Popa, M. Cremene, M. Borda and K. Boudaoud, "A security framework for mobile cloud applications", 11th Roedunet International Conference (RoEduNet), (2013) January 17-19.
[8] S. Singh, R. Bagga, D. Singh and T. Jangwal, "Architecture of Mobile application, Security issues and Services involved in Mobile Cloud Computing Environment", International Journal of Computer and electronics Research, vol. 1, Issue 2, (2012) August.
[9] S. S. Qureshi, T. Ahmad, K. Rafique and Shuja-ul-islam, "Mobile cloud computing as future for mobile applications - Implementation methods and challenging issues", IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), (2011) September 15-17.
[10] H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, "Resource Allocation for Security Services in Mobile Cloud Computing", IEEE Infocom 2011 Workshop on M2MCN, (2011).
[11] C. -L. Tsai, U. -C. Lin, A. Y. Chang and C. -J. Chen, "Information security issue of enterprises adopting the application of cloud computing",Sixth International Conference on Networked Computing and Advanced Information Management (NCM), (2010) August 16-18.
[12] D. Huang, X. Zhang, M. Kang and J. Luo, "Mobile Cloud: Building Secure Cloud Framework for Mobile Computing and Communication", Fifth IEEE International Symposium on Service Oriented System Engineering (SOSE), (2010) June 4-5.
[13] Cloud.cio.gov,http://cloud.cio.gov/topics/cloud-computingservice-models
[14] W-T. Tang, C-M. Hu, and C-Y. Hsu, "A mobile phone based homecare management system on the cloud," in Proceedings of the 3rd International Conference