SMARTPHONE REAL TIME APPLICATION MODELS IN CLOUD COMPUTING

Nayan Kuruppa

ABSTRACT

Mobile user a becoming large and large. Worldwide user using Smartphone to access their information anywhere and anytime. Smartphone's are similar to carrying a mini world in palm .many different application can be used according to user –centric ability. Smart phone are now capable of supporting a Wide range of applications, many of which demand an ever Increasing computational power. This poses a challenge because Smartphone are resource-constrained devices with limited computation Power, memory, storage, and energy. Fortunately, the Cloud computing technology offers virtually unlimited dynamic Resources for computation, storage, and service provision. Therefore, Researchers envision extending cloud computing services To mobile devices to overcome the smart phones constraints. The challenge in doing so is that the traditional Smartphone Application models do not support the development of applications to proposed the transmission between Smartphone and cloud, then we proposed to secure the data malware to prevent the data storage etc. there may be some of the transmission to smart phone to cloud ,in that what type of security can incorporate cloud computing features and Requires specialized mobile cloud application models. This project presents mobile cloud architecture, offloading decision affecting Entities, application models classification, the latest mobile cloud Application models.

Index terms- Smartphone, Cloud Computing, Computational Offloading, Mobile Cloud Application, Cloud Survey, Change over Methods, Application Models.

1. INTRODUCTION

The client proxy deals with the method offloading and data transfer. Similarly, the server side consists of profiler, server proxy, solver and controller. However, the working of a profiler and server proxy is similar to the Smartphone. The solver is the main decision engine of the MAUI that holds the call graph of the applications and the scheduled methods. Lastly, the controller is responsible for the authentication and resource allocation for incoming requests. Considering the advantages, MAUI provides a programming environment where independent methods can be marked for remote execution. It uses dynamic partitioning of the applications to reduce burden on the programmers. Moreover, MAUI does not only focus on memory constrains of the Smartphone but also considers the energy consumption involved in the offloading procedure. Furthermore, MAUI supports fine grained method level offloading that can offload even single methods instead of offloading the whole software blocks. However, single method offloading is less beneficial compared to combined methods (multiple methods) offloading. Another weakness of MAUI is that if the programmer forgets to mark methods (for remote execution), MAUI will not be able to offload those methods. Also, MAUI saves information about the offloaded methods (for future decisions) and uses online profiling to create an energy consumption model. When new offloading requests are received, MAUI uses history data to predict the execution time of the task. However, the execution time of the task is input size dependant that is not considered by the MAUI. Therefore, the predictions of MAUI might be wrong, resulting in wrong offloading decisions. Nevertheless, the MAUI profilers consume processing power, memory and energy, which is an overhead on the smart phones.

Computation offloading is a procedure that migrates resource-intensive computations from a mobile device to their source-rich cloud, or server (called nearby infrastructure).Cloud based Computation offloading enhances the applications performance, reduces battery power consumption, and execute applications that are unable to execute due to insufficient Smartphone resources. Moreover, cloud offers storage services [7] that can be used to overcome the storage constraints of the smart phones. Currently, many applications exist with cloud support for multiple domains, such as commerce [8], healthcare [9], [10], education social networks [13], gaming [14], file sharing and searching among others.

Open Research Issues Architectural issues: Reference architecture for heterogeneous MCC environment is a crucial requirement for unleashing the power of mobile computing towards unrestricted ubiquitous computing.

Energy-efficient transmission: MCC requires frequent transmissions between cloud platform and mobile devices, due to the stochastic nature of wireless networks, the transmission protocol should be carefully designed.

Context-awareness issues: Context-aware and socially-aware computing are inseparable traits of contemporary handheld computers. To achieve the vision of mobile computing among heterogeneous converged networks and computing devices, designing resource-efficient environment-aware applications is an essential need.

Live VM migration issues: Executing resource-intensive mobile application via Virtual Machine (VM) migration-based application offloading involves encapsulation of application in VM instance and migrating it to the cloud, which is a challenging task due to additional overhead of deploying and managing VM on mobile devices.

Mobile communication congestion issues: Mobile data traffic is tremendously hiking by ever increasing mobile user demands for exploiting cloud resources which impact on mobile network operators and demand future efforts to enable smooth communication between mobile and cloud endpoints.

Trust, security, and privacy issues: Trust is an essential factor for the success of the burgeoning MCC paradigm.

2. EMERGING ISSUES: CLOUD COMPUTING

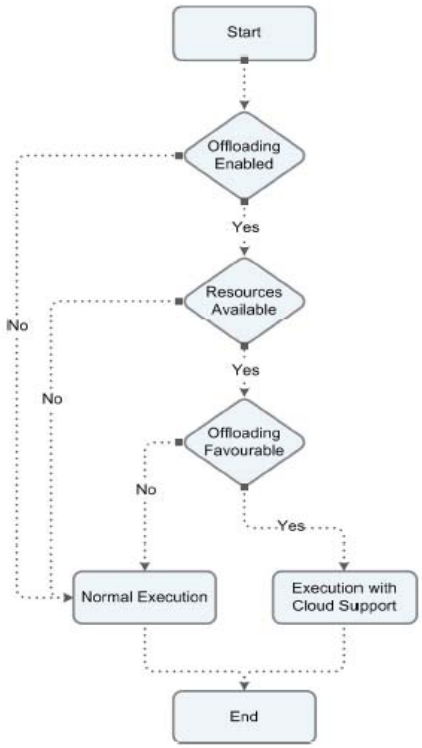
Mobile Cloud computing presents specific challenges to privacy and security. When using cloud-based services, one is entrusting their data to a third-party for storage and security. Can one assume that a cloud-based company will protect and secure ones data (back it up, check for data errors, defend against security breaches) if one is using their services at a very low cost? Or often for free? Once data is entrusted to a cloud-based service, which third-parties do they share the information with? Cloud-sourcing involves the use of many services, and many cloud based services provide services to each other, and thus cloud-based products may have to share your information with third parties if they are involved in processing or transferring of your information. They may share your information with advertisers as well, as many do to help cover the costs. Of course each cloud-based service has its own terms and conditions, or service level agreement, that the user agrees to (often without reading), and is often updated. Privacy and security issues around cloud computing can also be addressed as an education and awareness issue.

People need to be aware of terms and conditions as well as to keep up with updates. In the same plenary it was also pointed out cloud computing is expected to enable small and medium businesses to enter the market with lower up-front costs to operate without

a large IT department. Cloud computing offers ngos, government, universities, hospitals and others the opportunities of reduction in IT costs and the rationalization of certain services through economies of scale. Cloud computing offers a chance for reliable online digital storage of files, often quite helpful for users accessing the internet from mobile phones or internet cafés, and without large storage devices. Cloud computing transfers much of the processing required to use web applications away From the browser as processing is done "in the cloud" in the distributed infrastructure (e.g. Servers) of the cloud computing service. Cloud computing is thus in theory quite friendly to cheaper devices with low processing power, and lower storage capacities "the delivery of computing as a service rather than a product, whereby shared resources, software and information are provided to computers and other devices... Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services

3. ARCHITECHTURE AND OFFLOADING MODEL

The process offloading means that in the absences of authorized model the efficient usage occurs this said to free computational processing



Here while starting the concept of offloading we know that offloading is a type of authorization model .when offloading is enabled our resources is ready for our usage once the concept is favourable for our method allocation we can simple execute like view and know or else we make some changes in our system or allocation one we delete or files or else we include new concept file.

3.1 Issues and services

Security

Security is one of the most prominent bottlenecks in the adoption of cloud computing .Cloud computing endure a number of security issues, for instance, data access control , data distribution over a distributed infrastructure, data integrity, service availability, and secure communication.

In mobile cloud computing, security needs to be analyzed from two

perspectives i.e., the Smartphone and the cloud. The smart phones must be clean from the malicious codes, such as viruses, Trojan horses, and worms. The malicious codes are security threats and can change an application's behaviour, which may cause privacy leakage or data corruption. Therefore, to keep the smart phones clean from the malicious codes, security applications must be used regularly.

However, the scanning processes of the security applications are a computation-intensive task that consumes high energy. Therefore, it is not feasible for the smart phones to execute security applications for extended periods.

In this paper authors propose multiple techniques that perform computation offloading of (malicious code scanning) resource-intensive tasks to achieve security and gain energy efficiency. Alternatively, from the cloud security perspective, the data stored in the cloud can be lost, altered, denied, or leaked. Therefore, the data stored in the cloud must have multiple backups with integrity support to avoid data loss and undesired modifications

Scalability

Scalability is one of the most important features of cloud computing. Therefore, the mobile cloud application models must support the development of applications that can scale in the cloud to meet unpredictable user demands. Moreover, the application models must enhance the supported features to incorporate new types of applications in a timely manner. Nevertheless, the mobile cloud application models must also be scalable in terms of adoption. For instance, an application model that requires nearby computational infrastructure and demands heavy software installations is less scalable compared to the application model that is based on the cloud platform having no hardware setup requirement. However, the scalability is not only dependent on the application model, and to some extent depends on the cloud platform. Google App Engine focuses on the traditional web applications with stateless computation and state full data storage that makes the applications impressively scalable. Therefore, the aforementioned scalability issues must be considered during the development or adoption of the mobile cloud application models. Therefore, to make the application models scalable and capable of utilizing virtually unlimited resources with guaranteed availability; shifting the task of computation from the nearby infrastructure to the real cloud platforms is an appealing choice.

Platform

A platform is the underlying software technology of the smart phones on which the application models are based. Smartphone manufactured by different manufacturers can be grouped together based on the operating systems that run on the devices. The renowned Smartphone operating systems are Android, iOS, Symbian, Mobile operating system and BlackBerry OS .

• *Android* is an open source operating system powered by Google, and its kernel is based on Linux. Android OS supports Java based application.

• *iOS* is a proprietary OS of Apple and is based on MAC OS X. iOS applications are mainly developed in objective C.

• *Symbian* is an open source OS powered by Nokia, while its applications are developed in Java and C++.

• *Mobile OS* is a proprietary of Microsoft and support applications Developed on .Net framework. Nokia has also announced that its newly manufactured smart phones will be running Windows Phone 7 powered by Microsoft.

• *BlackBerry OS* is a proprietary of Research in Motion (RIM) and its applications are mainly developed in Java. a single platform due to the heterogeneity of the underlying technologies, and the variety of supported programming languages. For example, Apple iOS does not support Java based applications, and its applications are purely coded in Objective C. Moreover, some mobile operating systems are not designed for computational offloading, for instance, the Google Android application model has more support for computational offloading compared to Apple iOS.

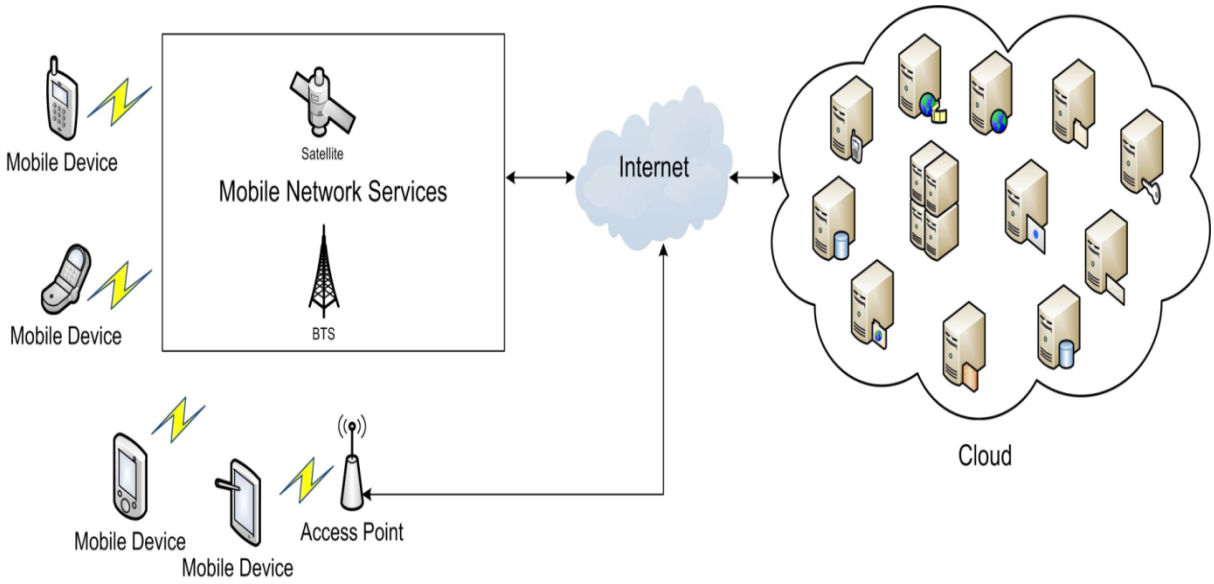


Figure 1: Architecture Of Mobile Cloud Computing

4. MODULES

4.1 Integration

In this module Smartphone is get connected with cloud computing to access the services .integration between Mobile and cloud is done here. Mobile cloud computing as an integration of cloud computing technology with mobile devices to make the mobile devices resource-full in terms of computational power, memory, storage, energy, and

context awareness. Multiple services from different service providers can be integrated easily through the cloud and the Internet to meet the users.

4.2 User Registration

In this module the Smartphone user is get resisted with cloud to access the authenticate usage. Only the authenticate user can access the cloud services. To avoid duplication and to protect user data from malicious programs .authorised user can store and use their data while it not possible for normal users. A user may enable or disable the computation offloading based on network data cost, cloud service cost, importance of data privacy and job turnaround time.

4. 3: Authentication / Authorization

In this module the resisted user access is performed .once the user get enter into the cloud it check for authentication .the user value are get stored in server at the time of registration and the service is installed .once the service is installed the address of the server is passed to the resource manager running on the Smartphone in the form of two dimension barcode. Authorization is given to user to use the licensed application.

4.4: Response / Download

In this module the user can upload their data for later access and download when it need. They can simply access this technique without any duplication with authorized performance. Sharing of application is performed when the user allots it's manage role as public.

4.5: cloud services

In this module services from cloud is done. Cloud provides their user to access application by free cost or payment mode; according to the application it is divided. Example cloud services for travellers some are given, such as guiding their trip, showing maps, recording itinerary, and storing images and video.

5. CONCLUSION

A number of the application models developed applications usually support one execution platform, thus, limiting the offloading of the elements (applications, components, clones) to other platforms. The mobile cloud execution platforms need to be standardized to ease computation offloading to the mobile cloud platforms. Also, new energy consumption models are required to facilitate accurate decision making by considering the main entities involved in the offloading process. Virtualization technology provides good support to achieve aim of cloud computing like higher resource utilization, elasticity, reducing IT cost or capital expenditure to handle temporary loads as well as cloud computing have various flexible service and deployment models which is also one of the main issue of adopting

this computing paradigm. The mobile cloud application models that are based on augmented execution of the Smartphone clone in the cloud require synchronization of the Smartphone and the clone. Therefore, new synchronization policies are required that can perform timely synchronization, taking into account accuracy, execution delay, and bandwidth utilization. Moreover, a Smartphone clone contains its user's data and licensed applications that are vulnerable to security attacks and piracy issues. A security mechanism is required to secure the clones from illegal access and protect the Smartphone users from the malicious VMs executing in the cloud. Nevertheless, if a Smartphone clone falls into the wrong hands, then the adversary may install the clone on a Smartphone of the same model and access the licensed applications illegally. To handle this issue, a new mobile cloud application piracy control framework is required. Some European Union data management laws and cloud computing principals are contrary to each other. Therefore, new policies are required that can confine mobile user access to optimum resources, or timely identify and revoke access of the untrustworthy users. Consequently, there is a need to standardize the mobile cloud computing platforms and refine the data management laws accordingly, so that the mobile cloud computing can flourish and mobile users can truly benefit from the cloud computing technology.

REFERENCES

[1] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[2] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.

[5] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[7] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002, pp. 3–13.

[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[10] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[11] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.