***An Over View of Mobile Cloud Computing***

***Definitions, Advantages, Challenges and Open Issues***

*Amjad Rttrout[[1]](#footnote-1),[[2]](#footnote-2), Hasan Badir[[3]](#footnote-3) , Nizar Shehab[[4]](#footnote-4)*

**Abstract**

Cloud computing virtualize resources as a service through the internet technology, so the resources should be managed and effectively distributed and allocated according to user request.

Mobile cloud computing is the evolution of rapidly developing mobile technology, that benefits from both mobile computing technology and cloud computing technology. Although many researches have been conducted in mobile computing, the field of mobile cloud computing was widely unexplored. In this article we introduce the concept of mobile computing, cloud computing and the integration between both technologies by exploring the advantages and the challenges.

**Introduction**

Smart phones, notebooks, tablets PC’s, etc… are becoming an important products in our life. Mobile computing is improved rapidly in both directions the hardware and software. The rapid progress of improving mobile computing affected the market of mobile, the demand on mobile computing is increased even mobile computing faces many challenges and problems such as battery life, storage, bandwidth and security.

Cloud computing is the next generation of computing in the upcoming years, which produces some advantages for users in different levels. It produces infrastructure as a service (IaaS) that enables the user to use networks, servers and storage. Cloud computing allows the user to use the platform as a service (PaaS) such as middleware services and operating systems. It also allows users to use software as a service (SaaS) such as application programs.

Since cloud computing enables users to use resources as on demand style, and mobile application is rapidly explosion, mobile cloud computing is introduced as the integration of cloud computing into mobile environment [1]. It brings new types of services and facilities for the users of mobile to take full advantages of cloud computing.

Mobile cloud computing is the developed generation of mobile applications that moves data storage and computing to the cloud in order to reduce mobile device limitations [2].

This article is designed as follows: in the next section the difficulties in mobile computing and how these difficulties are overcome using mobile cloud computing. Then the mobile cloud computing was explored. In the next section issues in mobile cloud computing are discussed. In the last section an opened issues, future work and conclusion are explored.

**Mobile computing difficulties:**

Mobile computing has many difficulties, in this context we should discuss these difficulties and how the mobile cloud computing overcome these difficulties.

1. Battery life time: Power consumption is one of the most important issues in mobile, many solutions are proposed for this problem, one of these solutions is to enhance and improve the CPU performance by applying changes in the hardware [3], [4], and in this case the cost of mobile device will be increased.

Another solution is to shift the complex computation from the mobile device to the cloud devices such as cloud servers. This technique is called computation offloading technique. It avoids long execution time in the mobile device which leads in large amount of power consumption.

2. Enhance data storage capacity: Instead of storing large data on mobile device, mobile cloud computing save storage space in mobile devices and store and access such data on the cloud via wireless network. Such as store/access images and large files [5]. Sharing images and files as done in the face book is one of typical examples of using cloud.

3. Improving reliability: The data stored and distributed in many number of computers in the cloud, which reduces the chance of lost data. Mobile cloud computing can be designed to improve the security for both the service providers and users, such as copyright protection, virus scanning, warm and malicious detection, authorization and authentication [9].

4. Dynamic on-demand provisioning resources: It enables the service providers and users to run their applications without advance reservation of resources.

5. Scalability: Service providers can easily add and deploy an application with minimum constraints in resources.

6. Integration: Service providers in the mobile cloud computing can introduce multiple services that can be integrated easily with each other to meet the user demands and his requirements.

**Applications of mobile cloud computing**

Mobile cloud computing takes advantages of cloud computing, there are many applications could be used in a wide range. These applications can be categorized in different areas. It tackles the main core of human life. Such as business, health, learning and education, entertainment, social networks, search huge number of data and information, etc…

The wide range of such applications take in account the challenges issues for mobile computing such as low bandwidth, high complexity of mobile devices, security and privacy, low storage devices of mobile.

**Issues in mobile cloud computing**

As discussed before, mobile cloud computing can migrate the advantage of mobile computing with cloud computing, in the same time it should be faced many challenges and issues. These issues are strongly related to mobile communication and cloud computing. In this context we should discuss these issues and the available solutions for them.

**-Low bandwidth**

In mobile communication, bandwidth is one of the big issues, this challenge is extended to mobile cloud computing. If we compare the bandwidth of wireless radio resources and the wired network, then the wired network will be the winner.

One of the solutions [11] is to share the bandwidth of all mobiles located in the same area. This can be done by forming cloudlet i.e. local cloud. This is possible if the users in the same area are interested in the same content, in this paradigm the distribution policy (how much the participant should receive and which part of the content, and who will take this part and why the other takes another part) lack fairness, in this paradigm the security and privacy issue will float to the surface.

To ensure security, the providers introduce the security as service, so you are not worry about security since it introduced from the vendors.

**-Availability**

It is one of important issues in mobile cloud computing since it depends on wireless network connection which is may be frequently disconnected due to traffic congestion and out of signal, while it is rarely happened in cloud computing with wired network connection.

There are many solutions for this problem such as [12] building a discovery mechanism to discover the unavailable nodes in the cloudlet, each node periodically broadcast control messages to inform other nodes of its status, according to the messages a role level of the other odes is estimated based on bandwidth, disk space and power supply, then the node that has the shortest hop length and the highest role level is selected as the intermediate node to receive the content. In this paradigm the security is treatment by using an account key to authenticate and encrypt the private contents; there are many levels of encryption keys (secure the channels between two nodes and protect the content).

**-Heterogeneity**

Mobile interfaces access the cloud through different radio access technologies such as GPRS, WIMAX, WLAN, CDMA2000 and WCDMA.

This leads to how mobile cloud computing deals with wireless connectivity without affecting scalability and energy efficiency of mobile devices.

An Intelligent Radio Network Access (IRNA [13]) model is used to deal with the dynamics and heterogeneity of available access networks.

**Computing offloading (static and dynamic environment)**

It is one of the main features in mobile cloud computing to improve the battery lifetime. Computing offloading is not always save battery lifetime; sometimes it may consume more energy especially when the code size is small. In addition the technology of wireless access network consumes different amount of energy (communication energy).

So we need a decision to offload the code or not. The decision should be based on the estimation of energy consumption before code execution. This may happened by partitioning the program [7]. We can estimate the communication energy by knowing the size of the code to be transmitted to the cloud and the bandwidth of the wireless network, while the computation energy depends on the computational time of the program. Since this procedure must be done in the runtime, it should be computed dynamically. The suggested paradigm can be applied for the procedure call [10]. Many problems should be arising if the bandwidth is dynamically changed or the disconnection is happened.

Some methods use the abstraction of the program [14] rather than the procedure call. The abstraction is divided into clusters by clustering analysis. To find the optimal partition a heuristic algorithm is applied to minimize the execution time of the program.

Those approaches depend on the execution time and the data size to find the suitable program partition to offload. Since the time is varies through the computation process, it is difficult to achieve an accurate execution time which leads to inefficient offloading performance.

So, another approach [15] of offloading doesn’t depend on the execution time. This approach depends on the time out, if the computation is not completed after the optimal time out, then the computation is offloaded to the cloud.

In dynamic environment i.e. the connectivity is decay periodically or bandwidth is frequently changed there are a few of approaches to tackle this environment. One of these approaches [16] checks the connection status periodically, it calculate and maintain the execution running time of a particular task that is offloading now, if the disconnection is occurred and it can be recovered, then the server send the task information to the client, but if the server cannot re-establish the connection with the client, the server wait for a pre-defined time interval, if it is still disconnected the serve will delete the task and it is considered as unaccomplished task.

Another approach [17] depends on the partitioning code in the dynamic environment by permitting the server on the cloud and the mobile client device to have all the application parts. In this module the application should decide which parts to run on the cloud and which should be run on the mobile client dynamically at the runtime. After that, the partition of minimized energy consumption is adopted. In the mentioned approach, the modules that contain sensitive and private information should be addressed to run locally to ensure the security and privacy.

One of the architectures [6] that partition the application in the dynamic environment depends on marking which methods to run “remote-able”. The remote-able methods can be used to extract the program state and send it to the cloud. There are many indications to decide that the method is not remote-able method, such as, a code that used to implement the client interface, a code that communicate and interact with input and output devices (I/O) or any external component. The serialization is used to determine communication cost. The linear programming formulation is constructed at the runtime that can be used to make the optimal decision of partitioning code.

**Security:**

The security in mobile cloud computing is divided into two parts; the security for mobile users and the security for data. The former related to malicious codes such as viruses and worms while the later related to data/application integrity, authentication and digital rights.

According to security for mobile devices, it is unreasonable to run the anti-spams or anti-viruses on the mobile devices. One of the used approaches used a cloud AV platform [18] consists of host agent and in-cloud network service components. The host agent is a lightweight application runs on mobile devices. The files are analyzed and some of them marked to be part of the host agent and moved to a cache. If the running file is not available in the cache it is sent to the in-cloud network service for verification. The network service determines the file is malicious or not. One of the advantages of this approach is using multiple ant threats engines in parallel using the virtualized container described by this approach.

**Privacy:**

Mobile users using the Location Based Services (LBS) to determine their current locations using GPS positioning devices. This is one of private issues that should be faced and solved. Location Trusted Server (LTS) [19] is one of solutions to solve this issue. LTS gathers the location information and conceal them in cloaked region. The cloaked region is send to LBS. In this situation LBS knows general information about the users but can’t identify them. But LTS can extract and reveal the user information, so the cloaked region proposed to be on both LTS and mobile device as shown in fig. When running the program in sender’s mobile, the program coordinates with the cloud to send information about surrounding users. Then the sender client will generate cloaked region and send it to the LBS. in this approach the both LTS and LBS can’t know the sender information.



Fig. Cloaked Region Architecture

**Data security on the cloud:**

When we talk about data security, it is coming to the mind the integrity of data/applications, authentication and digital rights which are the data related issues in mobile cloud computing.

**Integrity:**

Mobile users mostly concern about their data integrity on the cloud. Some solutions [29, 30] are proposed to address this issue without taking energy consumption in account. Another solution [31] considers energy consumption. In this approach a trusted third party is used in addition to mobile client and the cloud service. Three phases are used; initialized, modify and verification. In the first phase the files that will be sent to the cloud are assigned with message authentication code (MAC). The MAC is stored locally on the mobile client. While the files will be sent to the cloud. When the user want to update the file, the cloud sends the requirements to the trusted crypto coprocessor to generate new MAC related to the MAC that generated in initialized phase. Then the file and the related MAC are sent to the mobile client who compares them with its MAC, if it is authenticated the user can update the file. The comparison is known as verification process. It can be done for one file or collection of files even the whole files stored on the cloud. As we noticed in the verification stage the mobile client only compare between the MAC received from the trusted crypto coprocessor and the MAC that stored on it. So much of work done on the cloud while a little only done on the mobile client who saves energy and bandwidth.

Authentication:

There are many approaches used to authenticate the mobile clients, such as an implicit authentication [22, 23] and TrustCube [21]. Another approach [20] combines the two approaches mentioned before. In the combined approach, the long complex password is avoided. So in this method a short and simple password or PIN’s is used. The web server receives a request from mobile client; this request is redirected to the Integrated Authenticated (IA) service. IA service extracts the needed information and sends an inquiry to IA server through trusted network connect protocol which generate a report and resend it back to the IA service. The IA service determines the authentication result depends on the policy. The authentication result is sent back to the web server. The web server can proceed with the service or denied it depends on the authentication result that receives from IA service.

**Digital rights:**

Some of digital contents (audio, image, video, e-book) sometimes exposed to illegal distribution or even stolen. So protecting the contents from illegal access is one of important issues in mobile cloud computing. One of approaches used to solve this problem is Phosphor proposed in [8]. It depends on a SIM card placed on mobile user that contains a License State Word (LSW) based on application protocol data unit (APDU). So when the mobile user receives the encrypted content from the server, the mobile user uses the decryption key from the SIM card to decode it. If the decoding is succeeded the mobile user can be preceded with the content access. This approach is dedicated for mobiles only, so it can’t be applied to laptops using Wi-Fi access.

Efficiency of data access:

Cloud services are increased; as a result accessing data on the cloud are increased. Storing, managing and accessing data on the cloud through mobile clients faced big challenges since dealing with data resources on the cloud limited by mobile bandwidth, mobility and the device capacity.

So, [24] introduce an E-Recall framework to address the data access issue based on coordination of mobile searching, cloud computing and multimedia integration.

In this approach query formulated block is designed taking in account the optimal representation for user information and search content. While the cloud indexing structure block helps mobile users share and publish media resources in fast way through providing a database access method.

To utilize the memory capacity of mobile devices a local storage cache is proposed in [25]. In this solution a pocket cloudlet based on mobile memory to store the specific parts of cloud services. So much of work done on the mobile cache which increases the access speed, but to minimize consuming energy not all data are stored on the mobile cache. The authors proposed architecture to determine the amount of data to be stored on the cloudlet cache. So, to manage data between the cloud and the mobile devices sync mechanism is proposed to deal with data modification in both sides.

But this approach needs an expensive cache memory to store data from the cloud, and it should determine which data services to be cached. So with different and varied services this approach becomes inflexible.

Another approach [26] is proposed to address three main issues; the connection between the mobile users and the cloud, cache consistency and supporting data privacy. In this approach wireless-friendly network file system for mobile devices and the cloud (RFS) is used. RFS client on mobile devices and RFS server located on the cloud.

The client side has four components: encrypt sync, metadata and local cache heap. Sync component is connected to the Comm component on the RFS server via HTTP protocol to sync data between client and the cloud.

Encrypt component is used to control the data encryption and decryption. Metadata and the local cache heap used to manage all files cached on the mobile client.

When the cloud receives a request from a client, it records file’s block access patterns. Hence, the cloud can predict a new user’s access pattern and apply a server pre-push optimization to increase the speed of file delivery.

Finally, the cloud adapter is used to enable all RFS services to be performed on the diverse cloud storage systems, since cloud storage systems have their own API. This approach can be considered as a suitable solution for accessing data on the cloud from mobile users since it addresses several issues, i.e., device-aware cache management, data privacy, and wireless connectivity.

In the future, it is expected to improve RFS by posing policies to manage users (i.e., what and when to encrypt). Alternatively, some other approaches (e.g., Moxie [27]) can be applied to hash the contents of files, thereby optimizing the use of bandwidth [1].



Fig. RFS Architecture

**Context-aware mobile cloud services:**

Mobile user should be feel satisfaction if his preferences are taken in account, so the service provider tries to utilize the data types, network status, device environment and user preferences to improve the quality of service (QoS).

One of the models is Mobile Service Clouds (MSCs). In this model the user request pass through a gateway which choose the proper proxy that meets the user requirements. The result then sends to the user. If a disconnection is happened then MSCs will establish a special proxy for mobile to monitor the service path and support dynamic reconfiguration with minimum interruption.

So this model can treatment the disconnection and provide the QoS at acceptable level.

VOLARE [28] is a middle ware embedded on mobile device. It is maintain and monitor the resources and context of mobile device dynamically. When a service is request from the cloud, the mobile operating system sends context data to context monitoring module and QoS monitoring data to QoS monitoring module. The adaptation module will process the request taking in account the alerts receives from the context monitoring module.

If the QoS levels of service provided by service providers are lower than an accepted level of the request, Service Request Module will be notified to launch a new request that satisfies the new requirements. The advantage of this model is that the model can automatically recognize changes in the contexts on mobile device by providing an effective service request for mobile users at runtime. [1]

**Open issues and future work**

We discuss many issues in mobile cloud computing, there are still many issues that contributes in developing mobile cloud computing. In this section we should discuss the possible directions in mobile cloud computing development.

1. **Low Bandwidth:**

Although there are many efficient and optimal solutions, it is still to tackle this issue since the number of mobile and cloud users are dramatically increased which affect the limited bandwidth.

The 4G network and the Femtocell considered the upcoming technology that solves the limitation of bandwidth and makes the revolution in this field.

The bandwidth is increased from 14.4Mbit/s in 3G to 128Mbit/s. Even this leaping there are many issues to be taking in account such as network architecture, quality of service (QoS) and access protocol.

In [32] Femtocell is a small cellular base station used in a small area, one approach [33] develop a service that combines the Femtocell and cloud computing which can deliver mobile services over the Femtocell network. If the demand increased an additional resources are automatically taken in account and increased while if the demand is scaled down the excess resources are automatically removed. So in this paradigm the only necessary and needed resources are being used. This approach is seemly useful when used with cloud, but it needs to investigate and to know the impact when it applied with mobile cloud computing.

1. **Management of network access:**

It improves and optimize the usage of bandwidth spectrum. Cognitive radio increases the efficiency of the spectrum utilization. It allows the unlicensed users to access the spectrum that allocated for licensed users. So the lack of spectrum in mobile cloud computing can be solved by integrating this technique. So mobile users in mobile cloud computing must be able to detect the availability of radio resource and to ensure the service is not interfered.

1. **Quality of service (QoS):**

When mobile user access the servers in the cloud he may face many obstacles such as limited bandwidth which pour in congestion, signal attenuation caused by mobile mobility. The mentioned difficulties increase the network delay which affects the QoS.

So to treat the drop in service quality two new research directions are coming to the surface, clone cloud and cloudlets.

1. **Pricing:**

Mobile cloud computing involves mobile service provider (MSP) and cloud service provider (CSP). Both types have different services management, customer management, methods of paying and prices.

Since the customer should pay for the service, it is important to divide the price over the entities used by this service in a manner that satisfies the entities providers. So a new business model for mobile cloud computing should be developed taken in account pricing issues.

1. **Standard interface:**

Nowadays the interface between the mobile users and the cloud is based on the web interface. The web interface may have overhead since it is not designed originally for mobile, so interoperability and compatibility among mobile devices for web interface become an issue.

HTML5 is expected to be the promising solution, but it would be investigated carefully and its performance should be evaluated to ensure it will work efficiently in mobile cloud computing [1].

1. **Service convergence:**

Intensive competition of cloud service providers can pour in dividing the services among multiple clouds, in this case a single cloud may not enough to meet the user demands. In this case a new schema is needed to use multiple clouds which be interacts as a unified cloud. This new fashion is called sky computing which is considered the next generation of cloud computing. In the same context mobile sky computing enables providers to build cross-cloud communication in a unified way. The integration, convergence of such services must be explored and investigated deeply.

**Conclusion**

Mobile cloud computing is one of mobile technology trends in the future. It combines between mobile computing and cloud computing. The studies show that the demand on mobile cloud computing is increasing dramatically. With this importance, this article provided an overview of mobile cloud computing, its definition, the architecture, and the advantages.

The applications of mobile cloud computing are discussed such as mobile commerce, mobile learning, and mobile healthcare. The issues and related approaches for mobile cloud computing have been discussed. Finally, the future research directions have been proposed.

**References**

[1] Hoang T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang. “A survey of mobile cloud computing: architecture, applications, and approaches” Wireless Communications and Mobile Computing [Volume 13, Issue 18,](http://onlinelibrary.wiley.com/doi/10.1002/wcm.v13.18/issuetoc)pages 1587–1611, 25 December 2013

[2] Chetan S., Gautam Kumar, K. Dinesh, Mathew K. and Abhimanyu M.A. "Cloud Computing for Mobile World" January 2013.

[3] R. Kakerow, “Low power design methodologies for mobile communication,” in Proceedings of IEEE International Conference on Computer Design: VLSI in Computers and Processors, pp. 8, January 2003.

[4] L. D. Paulson, “Low-Power Chips for High-Powered Handhelds,” IEEE Computer Society Magazine, vol. 36, no.1, pp. 21, January 2003.

[5] E. Vartiainen, and K. V. -V. Mattila, “User experience of mobile photo sharing in the cloud,” in Proceedings of the 9th International Conference on Mobile and Ubiquitous Multimedia (MUM), December 2010.

[6] E. Cuervo, A. Balasubramanian, Dae-ki Cho, A. Wolman, S. Saroiu, R. Chandra, and P. Bahl, “MAUI: Making Smartphones Last Longer with Code offload,” in Proceedings of the 8th International Conference on Mobile systems, applications, and services, pp. 49-62, June 2010.

[7] K. Kumar and Y. Lu,“Cloud Computing for Mobile Users: Can Offloading Computation Save Energy,” IEEE Computer Society, vol.43, no. 4, April 2010.

[8] P. Zou, C. Wang, Z. Liu, and D. Bao, “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.

[9] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian. “Virtualized in-cloud security services for mobile devices,” in Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt), pp. 31-35, June 2008.

[10] Z. Li, C. Wang, and R. Xu, “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.

[11] X. Jin and Y. K. Kwok, “Cloud Assisted P2P Media Streaming for Bandwidth Constrained Mobile Subscribers,” in Proceedings of the 16th IEEE International Conference on Parallel and Distributed Systems (ICPADS), pp. 800, January 2011.

[12] G. Huerta-Canepa and D. Lee, “A virtual cloud computing provider for mobile devices,” in Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond (MCS), no. 6, 2010.

[13] A. Klein, C. Mannweiler, and H. D. Schotten, “A Framework for Intelligent Radio Network Access Based on Context Models,” in Proceedings of the 22nd WWRF meeting 2009, May 2009.

 [14] C. Wang and Z. Li, “A computation offloading scheme on handheld devices,” Journal of Parallel and Distributed Computing Special issue on middleware, vol. 64, no. 6, pp. 740 - 746. June 2004.

[15] C. Xian, Y. H. Lu, and Z. Li, “Adaptive computation offloading for energy conservation on battery-powered systems,” in International Conference on Parallel and Distributed Systems, vol. 2, pp. 1, December 2009.

[16] M. H. Tang and J. Cao, “A dynamic mechanism for handling mobile computing environmental changes,” in Proceedings of the 1st international conference on Scalable information systems (InfoScale), no. 7, pp. 1-9, May 2006.

[17] B-G. Chun and P. Maniatis, “Dynamically partitioning applications between weak devices and clouds,” in Proceedings of the 1st ACMcWorkshop on Mobile Cloud Computing & Services: Social Networks and Beyond (MCS), no. 7, June 2010.

[18] J. Oberheide, E. Cooke, and F. Jahanian. “Cloudav: N-version antivirus in the network cloud,” in Processing of the 17th USENIX Security Symposium, July 2008.

[19] H. Zhangwei and X. Mingjun, “A Distributed Spatial Cloaking Protocol for Location Privacy,” in Proceedings of the 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), vol. 2, pp. 468, June 2010.

[20] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, “Authentication in the clouds: a framework and its application to mobile users,” in Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW), pp. 1 - 6, 2010.

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

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

[23] E. Shi, Y. Niu, M. Jakobsson, and R. Chow. “Implicit Authentication through Learning User Behavior,” in Proceedings of the implicit authentication Security Conference (ISC), October 2010.

[24] J. Shen, S. Yan, and X-S. Hua, “The e-recall environment for cloud based mobile rich media data management,” in Proceedings of the 2010 ACM multimedia workshop on Mobile cloud media computing, pp. 31-34, October 2010.

[25] E. Koukoumidis, D. Lymberopoulos, K. Strauss, J. Liu, and D. Burger, “Pocket cloudlets,” in Proceedings of the 16th international conference on Architectural support for programming languages and operating systems (ASPLOS), pp. 171-184, March 2011.

[26] Y. Dong, J. Peng, D. Wang, H. Zhu, F. Wang, Sun C. Chan, and Michael P. Mesnier, “RFS: a network file system for mobile devices and the cloud,” ACM SIGOPS Operating Systems Review, vol. 45, no. 1, pp. 101-111, January 2011.

[27] R. P. Eaton, “Improving access to remote storage for weakly connected users”, University of California at Berkeley Berkeley, 2007.

[28] P. Papakos, L. Capra, and D. S. Rosenblum, “VOLARE: context-aware adaptive cloud service discovery for mobile systems,” in Proceedings of the 9th International Workshop on Adaptive and Reflective Middleware (ARM), pp. 32-38, November 2010.

[29] A. Tanenbaum and M. Van Steen, “Distributed Systems: Principles and Paradigms,” Pearson Prentice Hall, 2007.

[30] W. Wang, Z. Li, R. Owens, and B. Bhargava, “Secure and efficient access to outsourced data,” in ACM Cloud Computing Security Workshop (CCSW), pp. 55 - 66, 2009.

[31] W. Itani, A. Kayssi, and A. Chehab, “Energy-efficient incremental integrity for securing storage in mobile cloud computing,” International Conference on Energy Aware Computing (ICEAC), pp. 1, January 2011.

[32] J. Boccuzzi and M. Ruggiero, “Femtocells: design & application,” McGraw-Hill, 2011.

[33] http://www.haysystems.com/

1. Associate Professor, Arab American University – Palestine - Jenin [↑](#footnote-ref-1)
2. Associate Professor, Claude Bernard Lyon1 University, Lyon, France [↑](#footnote-ref-2)
3. Professor at Abdelmalek Assady university – Marroco - Tanja [↑](#footnote-ref-3)
4. Arab American University – Palestine - Jenin [↑](#footnote-ref-4)