An International Journal
JSCDSS
http://www.jscdss.com
Vol.1 No.1 December 2014: 1-11
Article history:
Accepted 11 November 2014
Published online 13 November 2014

Journal of Soft Computing and Decision Support Systems

A Framework for Mobile Maternity Data Management on Cloud Computing

Morteza Zamani Roudbaraki [a,*], Wahidah Husain [b]
[a] Engineering Computer Department, Islamic Azad University, Lahijan Branch, Guilan State, Iran
[b] School of Computer Sciences, Universiti Sains Malaysia, 11800 USM, Pulau Pinang, Malaysia

*** Corresponding author email address:** behrooz.zamani@gmail.com

Abstract

Pregnancy period is a special moment of women's life and maternity healthcare is considered as an important part of society healthcare. There are some problems and limitations with the existing services to support gravid women. The first problem is that there is no electronic system to share maternity data between hospitals and clinics. The existing systems do not exploit web and mobile technology, and there is no pervasive and ubiquities system. Most of health clinics' activities are done with traditional approaches. The second problem is that 20% of pregnant women have to rest at hospital for some days, weeks, or months because of some pregnancy complication such as bleeding, low placenta, and so forth. There is no monitoring service at home to reduce the number of hospitalized pregnant women. The next problem is with rural enceinte women who have higher poverty rates and tend to be in poorer health. Fewer doctors and hospitals, and other health resources will cause more difficulties for them getting to health services. So far, there is no monitoring system for rural enceinte women. Using mobile devices for monitoring pregnant women is a way to overcome those problems. Maternity monitoring by mobile makes an opportunity which by using it we can share maternity data and monitor enceinte women at home instead of being hospitalized. But maternity monitoring via mobile devices can raise other technical problems. The first problem is the quality, availability, accessibility, security and privacy of patients' data. The second problem is mobile device limitation that includes the limitation of memory, battery life span, and processor speed. In this study to solve these problems the literature review has been conducted on maternity data management, pervasive mobile healthcare system, cloud computing, and mobile healthcare system on cloud computing. Then a new architecture is proposed to solve those problems.

Keywords: Cloud computing, Mobile cloud computing, Maternity data management, Mobile healthcare system

1. Introduction

Using cloud computing is a new method for sharing and managing data. It reduces the cost of computing resources. Combining of cloud computing and mobile devices as mobile cloud computing technology make an opportunity which by use it customer can use different computing resources over a network via their mobile. Recently, how to use mobile cloud computing in healthcare area is main goal which researchers try to aim it (Yuan, 2013). By using mobile cloud computing, the healthcare data can be accessed through mobile but there are various problems including security and privacy challenges, mobile's memory and power supply limitation that need to be understood and taken care of (Bhadauria et al., 2011).

The main goal of this paper is to offer a new architecture for managing the maternity data via mobile by using cloud computing. The objectives are:

a) To identify the most suitable maternity data management system on mobile cloud computing to ensure the quality, completeness, availability, accessibility, and security & privacy of patient's data.
b) To identify the limitation of mobile device on cloud computing technology.
c) To propose the most suitable architecture on mobile cloud computing for managing maternity data.

2. Literature Review

2.1 Maternity Data Management

Maternity data management deals with some challenges including the level of its quality, completeness, availability, security & privacy. These issues need to be improved if we want to have a successful National Healthcare System (NHS). Unfortunately, at a national level, maternity data are recorded based on various methods and it is not possible to make a linkage between different local databases and computer systems to make an integrated storage. In pervasive computer system, accessibility to maternity data is difficult (Kenney, 2009).

Those patients who want to use mobile for sending or delivering their maternity data, need to update their data continuously and manage them on the network in real-time because when the location is not stable the system must be reconfigured to response the patient's queries. Here, data accessibility and security & privacy are the main issues at real-time (Imielinski, 2004).

Via mobile, updating process will be done with more difficulties over low-bandwidth wireless links. However, the management process via mobile is improving, for example new technologies in hardware area could change a simple mobile device to a palmtop which means it can work as a hand-held computer. Nevertheless, we are still involved with some limitations of mobile device like memory storage, CPU speed, and small power supply to manage the data (Imielinski, 2004).

Three factors that are very important to manage the maternity data and condition are security & privacy, accessibility and availability of information. Furthermore, these three items are important criteria to prepare an application in IT area (Varshney, 2003; Doukas et al., 2010). In earlier days, the most important issue was to maintain and store maternity data because the patient's information was not being accessible. Data had quality and completeness problem and many problems and errors happened to retrieve the information (Somasundaram, 2011).

One possibility to save data for making a pervasive system is to use distributed environment. The most important problem in data management is the physical management of data in the distributed environment. In this situation, for getting data, two issues may happen that are time-consuming and error-prone to get information (Deelman & Chervenak, 2008).

2.2 Cloud computing

Cloud computing is a technology for sharing resources such as database, storage, services and servers. It can be launched very fast because it does not need a high level of managing (Mell and Grance, 2011). Cloud computing is a new technology that offers hosting and delivery service along with Internet. Business owners have much enthusiasm for using cloud computing because it allows enterprises to start from small quantities and raise their resources gradually if they need new resources (Zhang et al., 2010). When the system is prepared based on cloud computing, users can access to the system by using a web browser regardless of their location. No matter what kind of device they use (e.g. mobile phone) because the system is independent of the device and location (Doukas, 2010).

Cloud computing has five features which includes on-demand service, wide access to the network, pooling resources, elasticity, and measured service. The meaning of on-demand service is that a user can manage and launch computing issues without the need to ask help from service provider. The meaning of wide access to the network is that customers can use various types of devices like laptop, PDAs, and mobile which can be connected to network but a standard mechanism is necessary to exchange information between these devices (Mell and Grance, 2011).

The meaning of pooling resources is that the provider's computing resources can support different customers with different needs and demands without depending on location. When the resource is shared, using a resource by a customer does not cause any constrain for other customers to use it. The meaning of elasticity is that cloud computing providers must allow customers to have great flexibility for upping or downing their requirement by scaling the cost of the system. The meaning of measured services is that the cloud computing must control and monitor the usage of resources and be able to optimize them. The report of resource usage must be sent to customers. Pay-per-use must also be provided for customers (Lupse et al., 2012).

There are three types of architectures for cloud computing whose names are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The meaning of Saas is that the customers are able to use software which has been placed on the cloud infrastructure and previously provided (e.g web-based email), but customers do not have to install the software and it is not necessary to involve with managing issues like operation system, network, storage, and so forth (Buxmann, et al., 2008).

The meaning of Paas is that customers can create or deploy software onto cloud infrastructure and use a program language. As like as SaaS, the customers do not have responsibility to involve with network, storage, and related issues (Keller & Rexford, 2010). The meaning of IaaS is that the customer is able to put their services or software onto infrastructure computing and manage some computing resources (e.g applications and operation systems), but cannot manage the cloud infrastructure. Iaas has the most facilities for a customer to offer a service (e.g., host firewalls) to other customers in comparison with Saas and PaaS. By using Iaas, the customers cannot manage cloud infrastructure, but can control operation system and network components (Bhardwaj et al., 2010).

There are four development models for cloud computing including public cloud, private cloud, community cloud, and hybrid cloud. Private cloud will be used when an organization wants to prepare an internal database just for own self. Private cloud does not allow the cloud infrastructure to be available in the public (Armbrust et al., 2010). The organizations or individuals can use public cloud when they want to deliver these cloud infrastructure-based services to public via multi-tenant platform. (Jansen and Grance, 2011).

The term of community cloud is used when some organizations want to access to some special issues and concerns among themselves. No other organization can access to these companies (Marinos and Briscoe, 2009). The meaning of hybrid cloud is used when the cloud is a mixed cloud of other forms, namely, private, public or community (Lupse et al., 2012).

2.3 Pervasive Mobile Healthcare System

Mobile healthcare system means the usage of technology like wireless, network, virtual resources, sharing system, and mobile improves healthcare conditions and obtains health goals (Kay, 2011). It is very clear that using new technology is necessary to promote the health sector, for example using different clinical information or communication technologies are helpful. There are many other terms which are used in this situation like e-healthcare, medical information, health informatics, telenurse, telemedicine, tele-care, or tele-health and so forth. There is not a separate definition for these terms, but e-health can refer to the usage of Internet in healthcare area and mobile health can be defined as the usage of mobile to improve the health sector (Pagliari, 2005).

The reason to use mobile healthcare has two aims. The first one is that all information about a patient is accessible anywhere anytime and patient's location is not important for obtaining his/her medical records. The second one is that the patient must be free of computing issues. One important benefit of using mobile healthcare is emergency response and management that by which patients can monitor themselves (Varshney, 2003). Mobile healthcare system has many advantages for patients and clinical staff, but some issues related to this matter must be solved because, in the real world, to manage the information through mobile devices makes some challenges like physical storage, permission issues, privacy and security, and so forth (Doukas et al., 2010).

The probability of medical errors in the healthcare area will increase when doctors have limited access to patient's information such as when they want to make decision about a patient. Mobile healthcare can solve this problem because it makes an effective communication between patients and doctors (Leape, 1994). Daily life of citizens can be improved by preparing and combining some devices and technologies including bandwidth, General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS) and some sensors like blood pressure apparatus. One important area which will be advanced by using these technologies is healthcare area (Van Halteren, 2004).

To improve mobile healthcare, the Commission of the European Union has developed a project called the MobiHealth project which focuses on the patient monitoring by using wireless technology and sensors. This project defines a special wireless system around the human body which called body area network (BAN). This system has been made to support patients with chronic illnesses. Patients can be monitored by this service via the advanced wire-less communications and integration of sensors to a wireless body area network (see Fig. 1). By using this system, patients can manage and handle their conditions (Van Halteren, 2004).

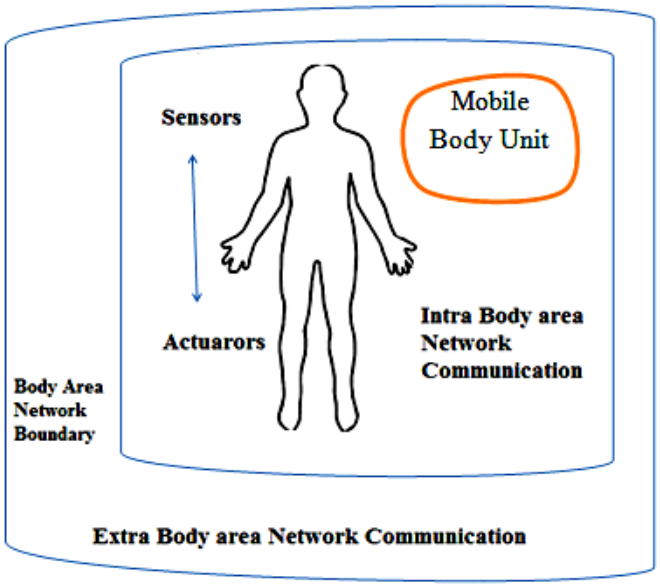

Fig 1. Healthcare BAN architecture.

2.4 Mobile Healthcare System Based on Cloud Computing

There are many researches about improving healthcare system based on cloud computing which focus on mobile as the most important device to make communication between the patient and the system. The researcher summarizes some of the most important articles which focused on architecture are related to mobile healthcare system based on cloud computing. The first study is about the architecture which offered by Ben Jeddou (2011). This system has three subsystems which includes input-output, local, and remote subsystem. The important part of input-

output subsystem is sensory input which can collect the varying data types. It collects data form the sensors which are attached to the patients or patient's entourage.

The second part, namely, local subsystem provides data for healthcare system. It uses a computer to store data. The remote subsystem does some processing on collected data and store data in health medical records. Remote subsystem can monitor and check data because it resides on healthcare service provider. It can determine whether the patient's condition is crucial or not. This system uses ad hoc wireless networks, wireless LANs, GSM and satellite to send and receive information (Ben Jeddou, 2011).

The model which designed by Ben Jeddou (2011) named two track unified process. This model has two branches that include functional and technical branches. These two branches have four equal factors consisting of recipe, test and coding, detailed and preliminary design but each of them has two separated factors. Capturing of business requirements and analysis are two factors of functional branch while capturing of technical requirements and generic design are technical branch's factors. In this system, the healthcare activity cycle will be started by physician and he/she has to consult with- the patient to collect patient's data, then the doctor will send this information by his mobile to database. Of course, extract transform and load (ETL) is a tool which helps doctors to store patient's data to data warehouse. In the next stage the doctor analyzes all information about patient including new data and historical data and predicts what event will happen for the patient in coming month (Ben Jeddou, 2011).

The second study is about the architecture which suggested by Suresh and Robin (2011). They suggested an integrated architecture for monitoring patients based on three sensors, namely, web camera, gyroscope and accelerometer. Doctors, nurses, and caretakers can access to data. The raw data is filtered by filtered modules before they sent to database. These modules will eliminate the redundant data. To make a voice relationship between doctor's and patient's voice over Internet a protocol (VOIP) is employed. There is a module for checking authoritative issues that gives permission to the same person who has right to use the system. The author employed a peripheral interface controller (PIC) to recognize which sensor is active because three kinds of sensors employed in this system which contains temperature, accelerometer, and biomedical sensors. Using filtering and voice communication are two strength points of this architecture. The weaknesses of this study are that there is not an authentic system between patient and cloud database, author has not mentioned the limitation of mobile devices, and data management issues have not been considered.

The third study, Somasundaram et al. (2011), used cloud computing for managing medical image data whose name is Hospital Management System (HMS). It is a mobile application based on cloud computing by which the doctor and the patient can view patients' data. This application needs android OS. This application is powered by EyeOS cloud platform. All information will be analyzed by doctors or clinical staff and patients' data must be updated by the physicians. The images provided by this system are based on DICOM protocol and all of them have JPG format. This system has two modules, namely, server and client modules.

To use this system, doctors or patients can open the application, then enter their ID and password, and finally after authorizing procedure, the information will be listed based on checked boxes and user can select some or all check boxes and see his/her information. To set and fit the screen size of images with different mobiles, the Android SDK is used. It can support various types of images like MRI, X-Ray and CT. The format of images is JPG which are supported by DICOM protocol.

As the forth system, Lupse et al. (2012) suggested architecture for pervasive healthcare to manage the information in Gynecology and pediatrics & Obstetrics departments because the level of transferring data between these two departments is high. The suggested system by Lupse is based on cloud computing. In order to respect the privacy and security issues the private cloud has been selected which helps the system develop, but authentication process must be executed when a person wants to access to the medical information. The advantage of his suggested system is the ability of exchanging data between two medical information systems. It means his proposed architecture has interoperability feature.

The standard communication which is used in this architecture called Health Level Seven Clinical Document Architecture (HL7 CDA). This standard is a document markup standard which provides a semantic structure to exchange the clinical documents. CDA has three levels including level one, level two, and level three which the last level has more additional constrains on the document. Based on CDA standard in order to transfer a document, at first it has convert to XML code (Lupse et al., 2012).

Every department must be connected to the cloud to use the application, and a local network can support this system. The application can develop based on the demand of every department. When a baby is born, his/her data will be processed and stored by the Obstetrics & Gynecologists application and database. If a physician from the pediatrics department needs these data, a request will be send and the Ob-Gyn application will change the sheet of new born baby to XML code based on HL7 CDA standard and then send it to pediatrics database. It will be accessible by the physician who asked this sheet (Lupse et al., 2012).

In this article, security and data management issues are handled very well, but it focused on exchanging of the data between two departments which are placed in the same building. It has not considered remote monitoring issues when the patient is at home and wants to be observed by the clinical staff. The limitation of mobile device to run heavy algorithm is another weaknesses of this system.

As the fifth study, another architecture proposed by Chun et al. (2011) deals with mobile hardware limitation. what is considerable in comparison between a mobile and a laptop is that mobile devices has many constrains including the capacity of memory, the level of power supply, and the lack of running complex applications, algorithms or

modules. Chun et al. (2011) suggested a system called clone cloud. It can automatically transform mobile applications to benefit from the cloud. When the mobile device wants to execute a task, a virtual clone will be made based on the mobile device execution environment in cloud (see Fig. 2). It means all task executions will be transferred to clone cloud as a virtual device.

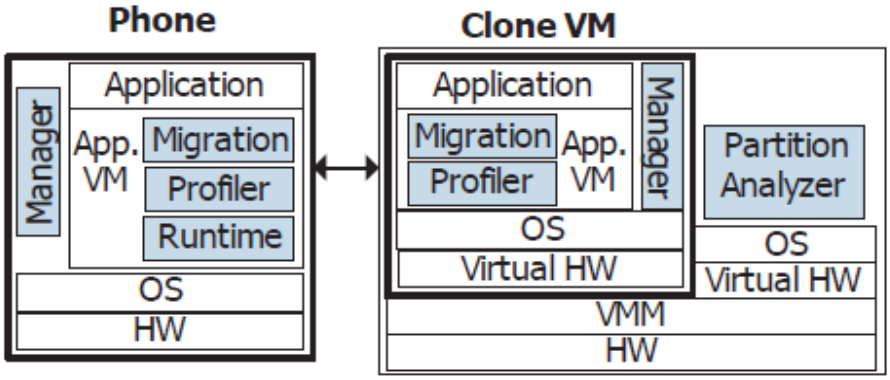

Fig 2. Clone Cloud Architecture based on Mobile Device Environment Source: Chun et al. (2011).

The system works based on application partitioning and thread migrating. At runtime (see Fig. 3), executing the algorithm in mobile device is not necessary and just a thread which points to the algorithm in mobile device will migrate to clone and the algorithm will execute there for the remainder of the partition, and re-integrating the migrated thread back to the mobile device (Chun et al., 2011).

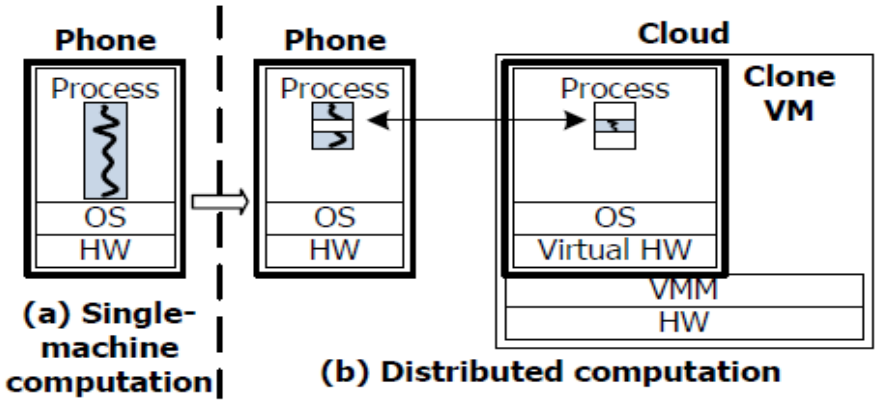

Fig 3. Single and Distributed execution in clone cloud Source: Chun et al. (2011).

Clone cloud can automatically transfer the computation of mobile device into the computation of both mobile device and cloud. Partitioning helps the system to deal with the mobile device limitation (e.g. memory) because this feature makes an opportunity that the speed of application execution increases 20 times and energy consumption decreases 20-fold. The partitioning mechanism in Clone Cloud is off-line, and it selects which thread must retain on the mobile device and which thread migrates to the cloud. This study considered the mobile limitation very well, but its weakness is the lack of strong security to protect the patients' data. Patients can only send their data when the Internet is available.

As the sixth study we consider the newest architecture which proposed by Yuan et al. (2013). He and his colleagues had a research to improve the data management dimension of architectures in healthcare application on mobile cloud computing. They believe that in mobile cloud computing area, the majority of healthcare system has only focused on reducing the consumption of mobile device's memory and power supply, and there is no enough explanation about the issues related to data management like concurrency control and security issues.

Fig. 4 shows the architecture which proposed by Yuan et al. (2013). This architecture has five important components including mobile device, data storage cloud, security cloud, application cloud, and authorized parties. Healthcare data

sent from mobile device or authorized parties to cloud which has security algorithm, then security algorithm will be executed and healthcare data will be encrypted and saved in data storage cloud. When the mobile device or authorized parties requests for services, their request will be sent to cloud which has application, then the application will acquire its needed data from data storage cloud. The application will decrypt data for processing and the result of this process will be encrypted and finally will be sent to the user (Yuan et al., 2013).

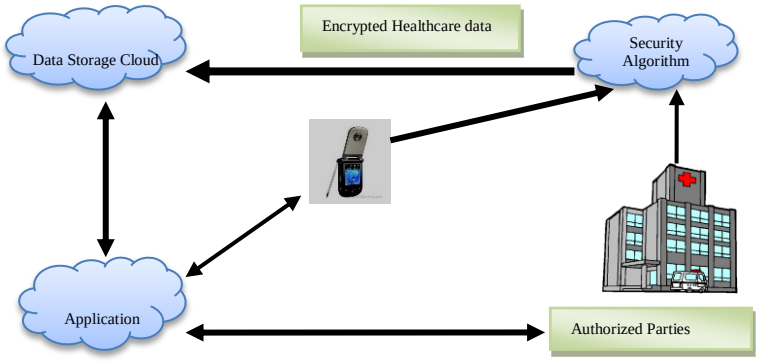

Fig.4 Mobile Cloud Computer Architecture (Yuan et al., 2013).

This system has some benefits because the proposed architecture considered both mobile limitation and data management issues (especially security concerns). The application will be run in cloud, thus the mobile does not need to consume large memory or CPU to execute application. Security algorithm will encrypt data before sending to data storage, thus misused actions will be failed if it happens. Unfortunately, the data which sent from mobile device and authorized parties to security cloud may deal with security problem because, at first, these data must place in security cloud, then security algorithm encrypts them. Time consuming may also happen because all parts have separately placed and this condition will increase the delay between user's request for service and getting answer.

3. Research Methodology

3.1 Comparative Studies for the Proposed Architecture.

Comparative studies of previous researches, that were explained in literature review, about maternity data management, cloud computing, pervasive mobile healthcare system, and mobile healthcare system on cloud computing have resulted in some key points. These results help us to select the best and suitable components to overcome the security & privacy and mobile device limitation problems for proposing architecture. The first result is that the best type of cloud for storing patients' data is private cloud. The private cloud is selected as a developed model of cloud because the primary security and confidence issues will be respected by using this type of cloud. The second result is that the best developed model of cloud is Platform as a Service (PaaS), because it is usually used for commercial idea when a special service is offered.

The third result is that all architectures that proposed by different authors have the same backbone. They have five layers including user's mobile, network operators, Internet services providers, application service. The first and important component of this backbone is mobile device which is improving day by day in terms of CPU speed, memory capacity and power supply. The mobile devices send patient's data to the mobile network via wireless. In the next stage, data will be transferred to the Internet and will be saved in cloud storage (Dinh et al., 2011). These stages face two problems. The first one is to misuse patient's data because of insufficient security & privacy warranty. The second problem is insufficient power supply and memory of mobile. Fig. 5 shows a general view of architecture's backbone for mobile healthcare system on cloud computing.

Aforementioned architecture's backbone which uses in healthcare system has some strength and weaknesses. These items which are shown in Table 1, is a general view of strength and weaknesses of existing mobile healthcare systems on cloud computing.

3.2 Study about Security & Privacy, Storage, and Power Supply of Mobile

To consider security & privacy, storage, and power supply of mobile issues Chun & Maniatis (2009) categorized a few smartphones and laptops to consider the level of their similarity in case of running healthcare application (Table 2). They believe that the new smartphones improved a lot because of new hardware technology. A lot of work can be done by new smartphones like uploading video, playing game, capturing, editing and so forth, and they are well adapted to running applications. However, they still have problem to run heavy algorithms because of the constraints of CPU speed limitation, memory storage, and small power supply.

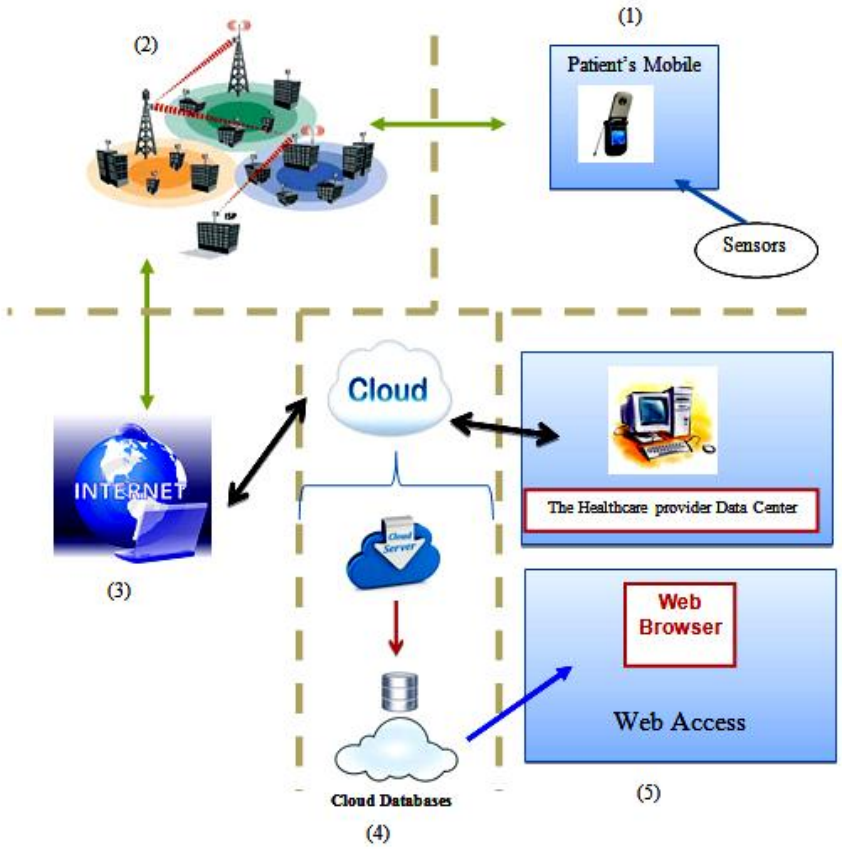

Fig. 5 Backbone for Mobile Healthcare Data management Source: Dinh et al. (2011).

Table 1
Strength and Weaknesses of Healthcare Systems.

Strength	Weakness
- Data collection can be done on time	- Quality, completeness, availability, accessibility issues
- High percentage of bureaucratic issues will be eliminated	- Difficulty of running heavy application
- Remote monitoring is possible	- Sometimes power supply is not enough
- Time-saving	- Memory limitation
- Cost-saving	- CPU constraint
- Reduce medicine errors	- Security & privacy challenges
- Data sharing	- Do not work without Internet

Table 2
Few Model of Mobiles and Computers specification Source: (Chun & Maniatis, 2009).

Phone/Computer	CPU	RAM	Battery (talk time in hours)
IPhone 3G	412 MHz	512 MB	5
Android HTC G1	528 MHz	192 MB	6
Blackberry Bold	624 MHz	128 MB	4.5
MacBook Pro Laptop	2.5 GHz 2-core	4GB	-
Dell Precision T7400	3.3 GHz 4-core	8GB	-

Healthcare applications are very heavy algorithms. They can easily be run in laptop, desktop, and computer, however running these applications in mobile confronted with some limitations. On the other hand, when we speak about mobile healthcare systems, users expect to execute healthcare applications in their mobile. To consider this problem the best solution is to use clone cloud (Chun & Maniatis, 2009).

To propose the best architecture, we investigate how many methods can be applied to new architecture to overcome security & privacy issues and mobile devices limitation. Then we will select the best method to use in our architecture in the next section. There are three methods to use mobile on cloud computing architecture. These three methods are under the effect of security & privacy, storage, and power supply. The first method is to place complex and massive algorithm in the mobile device. In This way, the

mobile device needs a lot of CPU power, memory, and big power supply for running application (see Fig. 6). By using this method, a high percentage of security problems will be solved because we can locate advanced security algorithm in the mobile device. However, existing studies show that no mobile healthcare system works based on this method. The second method is to prevent running a complex algorithm in the mobile device. This method can be implemented by using two clouds including healthcare application &security algorithm and data storage cloud (Fig. 7). The cloud which has healthcare application & security algorithm can be used as a bridge between mobile device and data storage cloud.

This method will solve the limitation problems of mobile for running heavy algorithms. The mobile device will request the application cloud, and then the application cloud will obtain required data from data storage cloud (Yuan et al., 2013). However, this method has security& privacy problem because when the patients want to send data via mobile, there is no security algorithm to encrypt data.

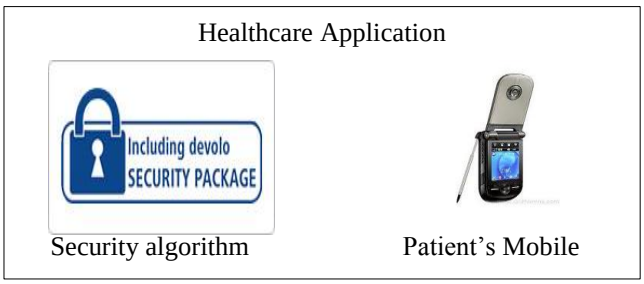

Fig. 6. Mobile with Security algorithm and healthcare application.

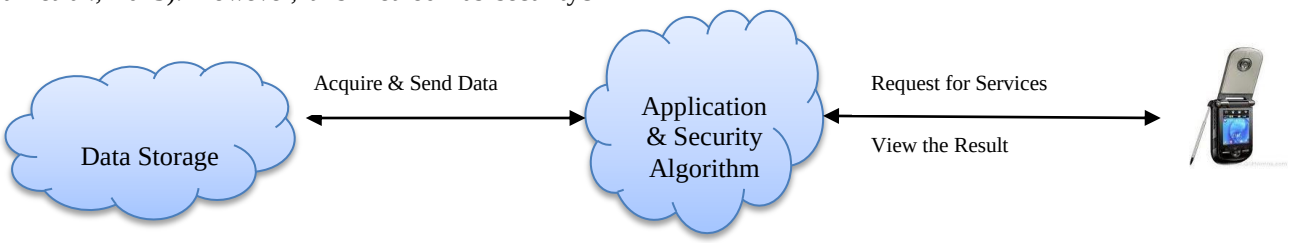

Fig. 7. Solution for Solving Mobile Limitation.

The third method suggested by Chun & Maniatis (2009) that is to use clone cloud. we will use it in our proposed architecture, thus we will explain it in Section 3.3.

3.3 Propose Architecture for the Maternity System

Our proposed architecture created by combining two architectures. The first one is the architecture which proposed by Yuan et al. (2013) and the second one is the architecture which proposed by Chun et al. (2009). In proposed architecture (Fig. 8), there are some labels and numbers which we will use to explain our architecture. Sensors send data to patient's mobile. These sensors will be attached to patient's body and include Blood Pressure Apparatus, Fetal Doppler, Contraction Calculator, and Weight Scale (Label A). The mobile will encrypt patient's data by using the security algorithm which is placed in mobile. To prevent the mobile device limitation for executing security algorithm we use clone cloud (Label B, C, D, and E).

"The system automatically transforms computation on mobile phone into a distributed execution optimized for the network connection to the cloud". Clone Cloud is a system by which the mobile application execution can automatically transfer to cloud for exploiting the cloud advantages. The system has high flexibility for partitioning of application execution and determines which part of application's execution must be transferred to virtual machine (Chun & Maniatis, 2009).

By using this system, unmodified mobile application will be run in virtual machine and simultaneously the execution part of mobile application will be run in the clone. For partitioning the execution of application, static analysis and dynamic profiling will be used. These two items will partition application automatically and optimize execution time and energy (Chun & Maniatis, 2009). At runtime, a thread which has the address of mobile application execution part will migrate to the clone and will activate this part in clone for executing. After execution of the special part of application in cloud, the migrated thread will be back to the mobile deice (Chun & Maniatis, 2009).

Patients and clinical staff in the health clinics or hospitals can send maternity data to data storage cloud after encrypting them (Number1 & 2). Encrypted data will be saved on the cloud (Number 3). Patients or clinical staff can request for E-Maternity services if they need them, (Number 4) and the result will be sent for them in form of decrypted data (Number 8). E-Maternity services as an application will ask necessary data from data storage cloud (Number 5) and data storage cloud also will send these data to E-Maternity service application (Number 6).

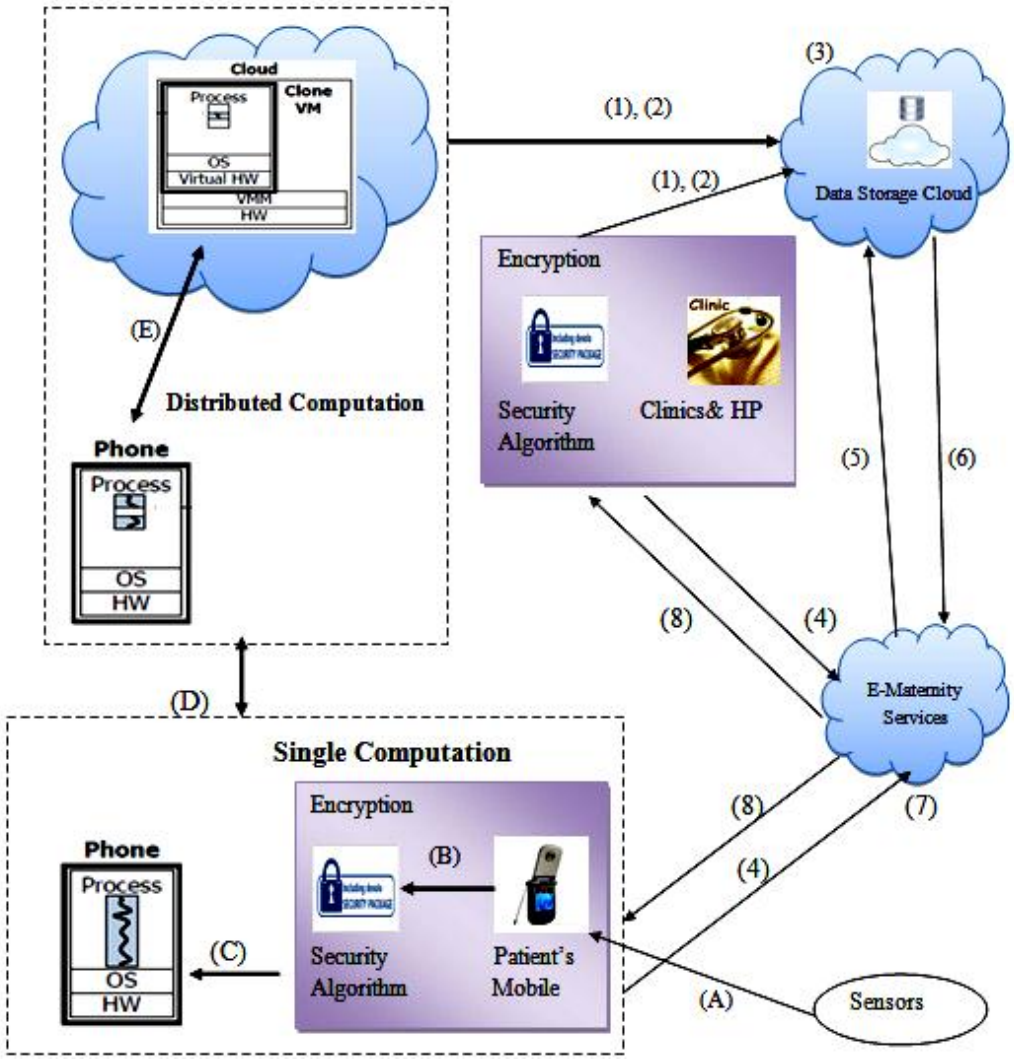

Fig. 8 Architecture of Mobile Maternity Data Management.

The Architecture for Mobile Maternity Data Management (AM2DM) has some benefits which separate it from existing architectures.

The first positive point is that it can use clone cloud to overcome the mobile device limitations because clone cloud helps the speed of the maternity application execution increases 20 times and also the consumption of battery of patient's mobile will decrease 20-fold (Chun & Maniatis, 2009). Clone cloud provides an opportunity by which the patients can use their mobile to execute the maternity application without concerning about mobile limitation. The second benefit is that if a problem happens for clone cloud, the system can continuously work because the patient's mobile can keep its relationship with maternity application (Number 4 and 8), but the benefit of using clone cloud will be eliminated and it is possible the patient faces mobile device limitation.

The third benefit is that we place maternity application in cloud. It means the mobile device avoids from executing maternity application. If maternity application runs in mobile it uses the memory and CPU of patient's mobile. This idea will reduce the probability of happening mobile limitation problem when the clone cloud does not work. The forth benefit is that we have separated security algorithm and placed it in the mobile. It will do warranty the security of system. When a patient wants to send data, encrypted data will be sent and encrypted result will come back to mobile device.

4. Conclusion

The new proposed architecture which we called the Architecture for Mobile Maternity Data Management (AM2DM) is different from existing architectures. It is a combination of two models which explained in literature review including clone cloud which introduced by Chun et al. (2009) and mobile cloud architecture which proposed by Yuan et al. (2013). Now we will consider the differences between AM2DM and existing architectures (based on literature review) at a glance.

Architecture offered by Ben Jeddou (2011) uses variable devices to attach the patients who suffer chronic diseases but there are some illnesses that prevent the patient to control these devices like patients who suffer from

Alzheimer. Architecture introduced by Suresh and Robin (2011) is an integrated architecture for monitoring patients based on three sensors, namely, web camera, gyroscope, and accelerometer but they did not mentioned about mobile limitation and security issues.

Architecture given by Somasundaram et al. (2011) can record images of X-ray and MRI but they did not mentioned about mobile limitation like CPU speed and memory capacity for using scan images. Architecture suggested by Lupse et al. (2012) focus to exchange patient's data between two departments including Pediatrics department and Obstetrics & Gynecologist Department. it supports maternity women but cannot support home-rest gravid women.

Architecture offered by Chun et al. (2011) is based on clone cloud and it is the best idea for solving mobile limitation but it cannot work without virtual machine. Architecture given by Yuan et al. (2013) is the newest architecture and has high flexibility but it has security problem. The strengths of AM2DM is it can covers some weaknesses of above architectures that proposed by different authors. It overcomes the mobile limitation because it uses Clone cloud as a part of its architecture. If the clone part goes to failure, it can use the second part of architecture which derived from Yuan et al. (2013) but in this situation the mobile limitation will increase the response time.

AM2DM solve the security problem which it is possible to happen in Yuan's model because the security algorithm moves to patients mobile and data can be encrypted before sending. The mobile limitation cannot make bad effect on system because clone cloud system makes an opportunity to transform mobile application execution to the cloud. In term of maternity data management AM2DM id the best to solve security issues because the last copy of patient's mobile will be stored in clone cloud and if patients loss their mobile or damage it, all data can be recovered. Additionally, in this architecture the security algorithm place as a program in patient's mobile and all data will be encrypted before sending to destination.

Unfortunately, like others architecture there is some weaknesses in AM2DM. The first one is to use the clone cloud, the patient's mobile must be enjoyed strong connectivity with more powerful machines which can be a laptop, computer, or cloud (Chun et al., 2011). The second one is the system just designed to support the maternity women (especially home-rest women) during the nine months or less.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Stoica, I. (2010). A view of Cloud Computing. Communications of the ACM, 53(4), 50-58.

BenJeddou, M., (2011). Pervasive Mobile Healthcare System Based on Cloud Computing. Available http://www.mysciencework.com/en/MyScienceNews/ 2962/pervasive-mobile-healthcare-system-based-on-cloud-computing#.US93g6JHLcw. Last accessed 12 Feb. 2013.

Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2011). A Survey on Security Issues in Cloud Computing. arXiv preprint arXiv:1109.5388, 1-15.

Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud Computing: A Study of Infrastructure as a Service (IAAS). International Journal of Engineering and Information Technology, 2(1), 60-63.

Buxmann, P., Hess, T., & Lehmann, S. (2008). Software as a Service. Wirtschaftsinformatik, 50(6), 500-503.

Chun, B. G., & Maniatis, P. (2009). Augmented smartphone applications through clone cloud execution. Paper presented at the Proc. of the 8th Workshop on Hot Topics in Operating Systems (HotOS), Monte Verita, Switzerland. 1-5

Chun, B. G., Ihm, S., Maniatis, P., Naik, M., & Patti, A. (2011). Clonecloud: elastic execution between mobile device and cloud. Paper presented at the Proceedings of the sixth conference on Computer systems, 181-194.

Deelman, E., & Chervenak, A. (2008). Data management challenges of data-intensive scientific workflows. Paper presented at the Cluster Computing and the Grid,. The 8th IEEE International Symposium.

Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2011). A survey of mobile cloud computing: architecture, applications, and approaches. Wireless Communications and Mobile Computing, P. 1-38.

Doukas, C., Pliakas, T., & Maglogiannis, I. (2010). Mobile healthcare information management utilizing Cloud Computing and Android OS. Paper presented at the Conf Proc IEEE Eng Med Biol Soc.

Imielinski, T., & Badrinath, B. (2004). Mobile wireless computing: challenges in data management. Communications of the ACM, 37(10), 18-28.

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST: National Institute of Standards and Technology, Tech. Rep. 800-144, 2011. Accessible: http://arxiv.org/ftp/arxiv/papers/1109/ 1109.5388.pdf. Last accessed 23th Nov. 2013.

Kay, M. (2011). mHealth: New horizons for health through mobile technologies. World Health Organization, 66-71.

Keller, E., & Rexford, J. (2010). The "Platform as a service" model for networking. INM/WREN, 1-6.

Kenney, N., & Macfarlane, A. (2009). Identifying problems with data collection at a local level: survey of NHS maternity units in England. BMJ, 319(7210), 619-622

Leape, L. L. (1994). Error in medicine. JAMA-Journal of the American Medical Association-US Edition, 272(23), 1851-1856.

Lupse, O. S., Vida, M. M., & Stoicu-Tivadar, L. (2012). Cloud Computing and Interoperability in Healthcare Information Systems. Paper presented at the INTELLI 2012, The First International Conference on Intelligent Systems and Applications, 81-85.

Marinos, A., & Briscoe, G. (2009). Community cloud computing. Cloud Computing, 472-484.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft). NIST special publication, 800, 145.

Pagliari, C., Sloan, D., Gregor, P., Sullivan, F., Detmer, D., Kahan, J., Oortwijn, W., and MacGillivray, S., (2005). What Is eHealth (4): A Scoping Exercise to Map the Field, Journal of Medical Internet Research, 7,1-6

Somasundaram, M., Gitanjali, S., Govardhani, T., Priya, G. L., & Sivakumar, R., (2011). Medical Image Data Management System in Mobile Cloud Computing Environment. International Conference on Signal, Image Processing and ApplicationsWith workshop of ICEEA, 2(9), 11-15.

Van Halteren, A., Bults, R., Wac, K., Konstantas, D., Widya, I., Dokovski, N., Herzog, R. (2004). Mobile patient monitoring: The mobihealth system, The Journal on Information Technology in Healthcare 2(5), 365-373.

Varshney, U., (2003), Pervasive Healthcare, IEEE Computer Magazine 36(12),138-140.

Yuan, J.N.Z., Ping, Z.Z., Wen, Y.H., Husain, W., (2013). Healthcare Applications on Mobile Cloud Computing, The Third International Conference on Digital Information Processing and Communications (ICDIPC 2013), Dubai, 514-522. ISBN : 978-09853483-3-5.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7-18.