

**DOKUZ EYLÜL UNIVERSITY**  
**GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES**

**DESIGN AND IMPLEMENTATION OF  
MEDICAL CLOUD DATABASE SERVICE  
SYSTEM BASED ON MOBILE COMPUTING**

**by**

**Miftaudeen ABDUL-RAHMAN**

**July, 2019**

**İZMİR**

# **DESIGN AND IMPLEMENTATION OF MEDICAL CLOUD DATABASE SERVICE SYSTEM BASED ON MOBILE COMPUTING**

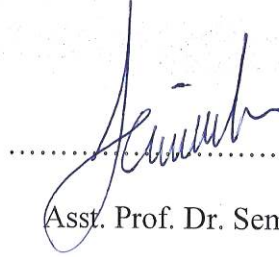
**A Thesis submitted to the  
Graduate School of Natural and Applied Sciences of Dokuz Eylül University  
In Partial Fulfillment of the Requirements for the Degree of Master of Science  
in Computer Engineering Program**

**by  
Miftaudeen ABDUL-RAHMAN**


**July, 2019  
İZMİR**


## M.Sc. THESIS EXAMINATION RESULT FORM

We have read the thesis entitled “**DESIGN AND IMPLEMENTATION OF MEDICAL CLOUD DATABASE SERVICE SYSTEM BASED ON MOBILE COMPUTING**” completed by **MIFTAUDEEN ABDUL-RAHMAN** under supervision of **ASST. PROF. DR. SEMIH UTKU** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science

  
.....  
Asst. Prof. Dr. Semih UTKU

Supervisor

Assoc. Prof. Dr. Derya BİRANT  
  
.....  
(Jury Member)

Doc. Dr. Tugba OZGEN CIZTOK  
  
.....  
(Jury Member)

  
.....  
Prof. Dr. Kadriye ERTEKİN  
Director

Graduate School of Natural and Applied Sciences

## **ACKNOWLEDGMENTS**

Throughout the writing of this thesis and my studies, I have received a great deal of support and assistance. Many people contributed in different ways and capacities. I wish to acknowledge their assistance.

Firstly, my highest appreciation and gratefulness goes to the Almighty God for his infinite blessings.

Secondly, I would like to express my deepest gratitude to my supervisor, Asst. Prof. Dr. Semih UTKU, for his invaluable guidance and persistence throughout my candidature. His experience and directions were paramount to completing my thesis.

My extra gratitude goes to Turkish government scholarship (YTB), for the financial and all other supports they provided me.

I would also like to thank my colleagues who contributed in this process including, Asli Bahce and Vladimir Radevski for their effort and support.

My sincere gratefulness also goes to all members in the Department of Computer Engineering as well as the faculty members of the Graduate School of Natural and Applied Sciences of Dokuz Eylül University.

Nobody has been more important to me in the pursuit of my career than the members of my family have, I would like to thank my parents and my supportive brothers, for their limitless love, support and care, most importantly, my loving and caring mother. I could not have asked for more. I dedicate this achievement to them.

Miftaudeen ABDUL-RAHMAN

# **DESIGN AND IMPLEMENTATION OF MEDICAL CLOUD DATABASE SERVICE SYSTEM BASED ON MOBILE COMPUTING**

## **ABSTRACT**

In modern healthcare environments, a fundamental requirement for achieving a ubiquitous system is the provision of an easy access to a distributed health records of patients at the point of healthcare or treatment in a unified and integrated manner in the cloud. Nevertheless, integrating crucial patient health records from different hospitals at a center in the cloud raises concerns about security, privacy and authorization measures to be implemented. In this work NFC (Near Field Communication) technology is presented to prevent attacks. NFC allows secure exchange of small amounts of data by proximity or touch. In addition, access control measures must guarantee that only authorized users have access to such Critical records and for a legitimate motives, or otherwise for illegitimate motives and unauthorized users, access to the records must be denied at the data center. The aim of this paper is to propose a unified access control scheme capable of supporting a selective sharing of patients compounded electronic health records (EHRs), by using different standards of granularity and more importantly providing the required privacy protection and security for the aggregated data. Moreover, for mobility and easy access, a medical passport card system is proposed using NFC technology. A simulation work of a normal healthcare service system and a comparison of that to the proposed system has been carried out, which showed a more advancement in the treatment process and at the same time cost effective.

**Keywords:** Cloud computing, electronic health record, medical passport system, access control, NFC technology

# MOBİL BİLGİ İŞLEME DAYALI TIBBİ BULUT VERİ TABANI SERVİS SİSTEMİNİN TASARIMI VE UYGULANMASI

## ÖZ

Modern sağlık ortamlarında, her yerden ulaşılabilen bir sistemle; sağlık hizmeti alan veya tedavi noktasındaki hastaların dağılmış sağlık kayıtlarına birleşik ve entegre bir şekilde kolay erişim sağlanması temel bir gereklilik olmuştur. Bununla birlikte, farklı hastanelerdeki kritik hasta sağlığı kayıtlarının buluttaki bir merkezde birleştirilmesi; uygulanacak güvenlik, mahremiyet ve yetkilendirme önlemleriyle ilgili kaygıları doğurmaktadır. Çalışmamızda NFC (Near Field Communication) teknolojisi, saldırıların önlenmesi amacıyla kullanılmıştır. NFC teknolojisi belirli miktarda verinin kısa mesafeden ya da dokunuşla güvenli bir şekilde değişimini sağlar. Bununla birlikte, geliştirilen erişim kontrol önlemleri sayesinde, yalnızca yetkili kullanıcıların kart üzerindeki kritik kayıtlara erişimine izin vermelidir. Aksi halde yasal olmayan bir şekilde, kritik hasta veri içeriklerine yetkisiz kullanıcılar tarafından erişiminin onay verilmediğinin garanti etmesi gerekmektedir. Bu çalışmanın temel amacı, toplanan hasta verilerine gerekli gizlilik koruması ve güvenliği standartlarda sağlayarak, hastaların seçici elektronik sağlık kayıtlarının (EHR) birleşik bir erişim kontrol sistemi önermektir. Ayrıca, mobilite ve kolay erişim için, NFC teknolojisi kullanılarak güvenli tıbbi bir pasaport kart sistemi önerilmiştir. Çalışma, normal bir sağlık hizmeti sisteminin simülasyon çalışması ile denenmiştir. Normal sağlık sistemi ile önerilen sistemin karşılaştırılması yapılarak, tedavi sürecinde daha hızlı davranabilen ve aynı zamanda daha uygun maliyetli bir ortamın sağlandığı gösterilmiştir.

**Anahtar kelimeler:** Bulut bilişim, elektronik sağlık kayıtları, tıbbi pasaport sistemi, erişim kontrolü, NFC teknolojisi

## CONTENTS

	Page
M.Sc THESIS EXAMINATION RESULT FORM.....	ii
ACKNOWLEDGEMENTS .....	iii
ABSTRACT.....	iv
ÖZ .....	v
LIST OF FIGURES .....	viii
LIST OF TABLES .....	x
<b>CHAPTER ONE – INTRODUCTION .....</b>	<b>1</b>
1.1 Overview .....	1
1.2 Thesis Organization.....	4
<b>CHAPTER TWO – CLOUD COMPUTING.....</b>	<b>5</b>
2.1 Cloud Computing Architecture and Implementation .....	5
2.2 Cloud Service Delivery Models .....	6
2.3 Mobile Cloud Computing .....	9
2.4 Issues with Mobile Cloud Computing .....	10
2.4.1 Privacy .....	11
2.4.2 Secured Data Access .....	11
<b>CHAPTER THREE – RELATED WORKS .....</b>	<b>13</b>
<b>CHAPTER FOUR – PROPOSED SOLUTION .....</b>	<b>16</b>
4.1 Medical Passport System .....	16
4.1.1 Confidential Medical Records .....	17
4.2 Authentication and Message Protocol .....	22

4.2.1 Proposed MPS Protocol .....	22
4.2.2 Broker-Based Composite EHRS Authorization .....	23
4.3 System Architecture .....	25
4.3.1 System Description.....	25
4.4 Electronic Medical Record (EMR) Mining .....	27
4.4.1 Standard Data Exchange Method .....	27
4.5 What kinds of healthcare information can Medical Passport Store? .....	28
<b>CHAPTER FIVE – EVALUATION .....</b>	<b>30</b>
5.1 Security Test Results .....	30
5.2 Healthcare Simulation .....	31
5.2.1 Registration Desk .....	32
5.2.2 Basic Evaluation Stage .....	32
5.2.3 Advanced Evaluation Stage .....	33
5.2.4 Lab Work Stage.....	33
5.2.5 Checkout .....	33
5.3 Comparison Between the Current System and Our Proposed System.....	33
<b>CHAPTER SIX – DISCUSSION AND CONCLUSION .....</b>	<b>35</b>
6.1 Discussion .....	35
6.2 Conclusion.....	36
6.3 Future Works .....	37
<b>REFERENCES.....</b>	<b>38</b>



## LIST OF FIGURES

	Page
Figure 2.1 Architecture of cloud computing .....	5
Figure 2.2 Types of Cloud computing deployment .....	7
Figure 2.3 Cloud delivery models .....	9
Figure 4.1 Custom MPS Protocol .....	23
Figure 4.2 Architecture of a Medical Cloud Database Service System .....	25
Figure 4.3 HL7 web services .....	28
Figure 4.4 Kinds of healthcare information Medical Passport stores .....	29
Figure 5.1 Simulation of a healthcare process in a hospital.....	32

## LIST OF TABLES

	Page
Table 4.1 Patient's personal details.....	17
Table 4.2 Child's birth details.....	19
Table 5.1 Comparison between current system and the proposed system.....	34



# **CHAPTER ONE**

## **INTRODUCTION**

### **1.1 Overview**

The rapid growth in wireless technologies led Ubiquitous Systems (US) get more important duties on health sector. With the involvement of US, patients will get better quality of services from hospitals. These ubiquitous systems will satisfy patients more and give them the right treatment. Furthermore, mobile systems are growing with advances in wireless technologies, which enables them to be integrated into Hospital Information Systems (HISs) easily. In addition, adapting ubiquitous systems to HIS happens with low cost and labor. Wireless sensors such as Radio Frequency Identification (RFID), Near Field Communication (NFC) or small sensors have become the fundamental components of the ubiquitous systems with combination of mobile systems and wireless technologies. On the other hand, US with wireless communication technology has some issues, such as transferring data in correct form and in right time, not losing data during transmission and most importantly, transferring data in a secure way.

There are different methodologies to create a secure data transfer and to prevent unauthorized access to medical information in hospitals. Barcode technology is one of them. However, there are problems with the barcode technology such as; low image quality, easy to copy, sometimes hard to identify easily by touching or reading (Wilson & Sullivan, 2004). A much better technology to prevent accessing sensible data is the RFID technologies. It is easy to identify RFID tags and difficult to copy them. Using right encryption methods and securing encryption keys on RFID tags may be the key to making a well-designed infrastructure. In theory, RFID technology has a well-designed security mechanism (Wei, Chao, & Quan, 2014). However, there are different attacks and vulnerabilities that exist in the RFID technology. If RFID tag is not well protected, it is possible to sniff, listen traffic or have denial of service (DoS) attack with third party unauthorized readers (Hutter, Schmidt, & Plos, 2008).

NFC technology is presented to prevent these attacks. NFC is a short-range data-transmission system, which has a wireless communication protocol, and data exchange formats that supports secure exchange of small amounts of data either by proximity or touch (Pateriya & Sharma, 2011). The standard is based on existing RFID standards including ISO/IEC 14443 (Agrawal & Bhuraria, 2012).

This work focuses mainly on the most common diseases such as; Ischemic heart diseases, Stroke, Respiratory cancers, Diabetes mellitus, Alzheimer's disease and other dementias, Tuberculosis and Cirrhosis (Pietrangelo, 2017). These are diseases that progressed slowly and perhaps several of them are partially preventable if necessary care is taken. Nevertheless, person's location and the availability of preventive and quality healthcare are factors that can be considered as unpreventable.

Medical history and other related information about these common diseases is a very important factor in providing a treatment. NFC based Medical Passport System which will store patient's demographics, medical information and history will ensure a suitable and a secure method of accessing patient medical history anytime anywhere and thus making it easier to deliver the needed information to healthcare providers to enable them give the best care possible. With the Medical Passport System patients do not have to repeatedly fill out multiple forms in order to provide their health history to different medical facilities, departments or caregivers before a procedure, especially during travel. In addition, there is no longer the need to waste time to complete forms with questions that do not relate to them.

Cloud computing has become an increasing computing model of late, as such attracting so much interest from the academic sector as well as the industry sector (Mell & Grance, 2011). The new model enables the handling and management of both hardware and software resources to be moved to third-party service providers. This results in so much cost efficiency as the cost on infrastructure is saved at the same time accessibility and availability is made easy regardless of place and time. For efficient provision of healthcare services and management of medical data, accessibility to healthcare-related data needs to be made ubiquitous. For that matter,

it would be of a high benefit to both patients and healthcare providers to move traditional Health Information Systems (HIS) to the cloud.

However, as sensible information is being moved to the cloud, issues of security, managing user's identity, secure access control measures, selective sharing of patient's records, integration of policies and so on and so forth, requires a proper attention and handling in order to make the proposed paradigm a success (Wu, Ahn, & Hu, 2012; Wu, Ruoyu, Gail-Joon, & Hongxin, 2012; Takabi, Hassan, James, & Ahn, 2010; Ahn et al., 2010). When patients health records stored in the systems of various healthcare providers are moved to the cloud computing environment, easy and safe transfer becomes an important challenge. Thus, among other challenges this paper focuses mainly on a secure transfer and control measures in the cloud computing environment. Sharing of important medical records involving multiple entities is a critical process, it therefore requires that patients' privacy be given a priority in the security and privacy mechanisms, for a successful integration of HISs and applicable over various heterogeneous systems in the cloud, where control of patients' HIS is fully handled by third parties. In situations where the data that is being shared over the cloud involves critical records of patient such as patient's personal information and details of medical histories, previous test results and so on. There is the need for a guaranteed safe and secured access to such sensitive information which should also be limited to only the legitimate parties who have the need to know.

In this study, Medical Passport System (MPS) has been developed with a secured structure. The system provides a secure way of verifying the patient information and establishing a secured medical data transfer based on mobile cloud computing. MPS consists of NFC tags, and mobile tablets are used by hospital staffs to authenticate the right user. NFC data communication protocol is implemented on the server by modified NFC official protocol. In MPS, authentication and data security process are carried out in the server. Tablets are utilized to identify the NFC tags and relay the data to the Picture archiving and communication system (PACS-Server). Furthermore, the pre-shared encrypted keys are used for patient authentication to avoid vulnerability.

The MPS-Mobile is also connected to HIS. Basic information about the patient is transferred from HIS Server to PACS-Server. The PACS-Server uses HL7's Version 2.x (V2) messaging standard. MPS-Mobile application was developed based on the Clinical Context Object Workgroup (CCOW) standard. Confidentiality, maintaining data integrity and ensuring data security should be planned according to HL7 for prevention of medical errors (Benson & Tim, 2012). Next section presents the related work.

## **1.2 Thesis Organization**

This thesis is categorized into six chapters as follows: Chapter One gives the introduction and an overview of the topic. Chapter Two presents information on Cloud computing, the architecture of cloud computing, mobile cloud computing, the importance of mobile cloud computing in healthcare sector and some issues related to its application in the healthcare sector. Chapter Three gives a summary of related works and other related studies. Chapter Four presents the proposed design and implementation of medical cloud database service system, based on mobile computing. Chapter Five gives an evaluation of the proposed system through security test, healthcare simulation and a comparison between the current system and the proposed system. Lastly, Chapter Six presents the discussion part as well as the conclusion and future works.

## CHAPTER TWO

### CLOUD COMPUTING

Cloud computing is the method in which resources are provided on an on-demand basis to a local client, typically through the internet. Cloud computing has become an increasing computing model of late, as such attracting so much interest from the academic sector as well as the industry sector (Mell & Grance, 2011). The new model enables the handling and management of both hardware and software resources to be moved to third party service providers. This results in so much cost efficiency as the cost on infrastructure is saved at the same time accessibility and availability is made easy regardless of place and time.

#### 2.1 Cloud Computing Architecture and Implementation

Cloud Computing architecture comprises of the integration of various components and sub-components of cloud by which the system structure is composed. Basically cloud architecture can be categorized into two components: Front-end and Back-end, connected to each other through a network or the internet. Figure 2.1 shows the general architecture of cloud computing.

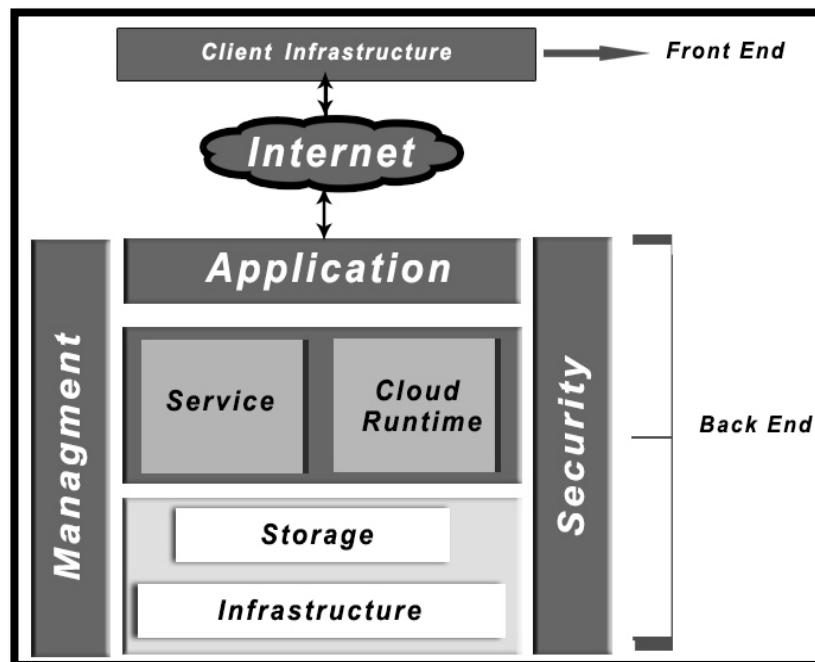


Figure 2.1 Architecture of cloud computing

## **A. Front End**

The Front-end refers to the part of cloud computing with a user interface that is visible to the end user (i.e. client), through which the cloud system can be accessed. Several cloud computing systems use different interfaces, examples of these include web browsers such as: Chrome, Safari, Firefox, etc.

## **B. Back End**

The back-end refers to the service provider part and it includes all the components that constitute the cloud computing services. These components are comprised of various servers, computers, huge data storage systems, virtual machines, deployment models, security mechanisms, other programs, etc. The back-end is also responsible for providing secure mechanisms, traffic control and management of the connected computers for inter communication.

## **2.2 Cloud Service Delivery Models**

A cloud delivery model defines the potentials delivered to end users and the supported applications. The cloud models are delivered in three fundamental delivery models, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), often referred to as the “SPI MODEL”. These models can be deployed through the cloud services such as public cloud, private cloud, community cloud and hybrid cloud.

**Private cloud** – This is a type of cloud computing that is dedicated to delivering similar advantages as public cloud, except that it focuses only on a single proprietary architecture. Unlike public clouds, the private cloud is dedicated to fulfilling the needs and goals of a single organization. One of the benefits of the private clouds is that, it seeks to combat greatly issues of data control and security. The infrastructure of this cloud may exist on the premises of the organization or externally hosted (off premises).



**Community Cloud** – This type of cloud computing is where cloud services are provided to a group of people or organizations with a shared interest, requirements, mission or policies. The management of community cloud can be a third party service provider or the parties involved, and the infrastructure may exist on or off premises.

**Public Cloud** – This is a type of cloud computing where the cloud services are made accessible to customers or the general public through a multi-tenant environment. Public cloud includes all the services and functionality of elasticity and the responsibility model of cloud. The physical infrastructure is controlled and managed by third party service providers such as Amazon Web Services (AWS) or Microsoft Azure. The infrastructure in this type is located off premises (i.e., within the service provider's data centers), where all clients can access but with limited configuration, security protections, and availability discrepancies.

**Hybrid Cloud** – This type of cloud computing is a combination of two or more clouds (private, community, or public), to form a unified cloud. The deployment of Hybrid cloud however requires a high standard of software and service compatibility, information exchange, and portability between the combined parties. Thus enabling cloud bursting for load-balancing between the clouds. With the hybrid cloud, service providers may leverage third party cloud providers in order to increase computing flexibility. Figure 2.2 depicts the differences between the cloud deployments types.

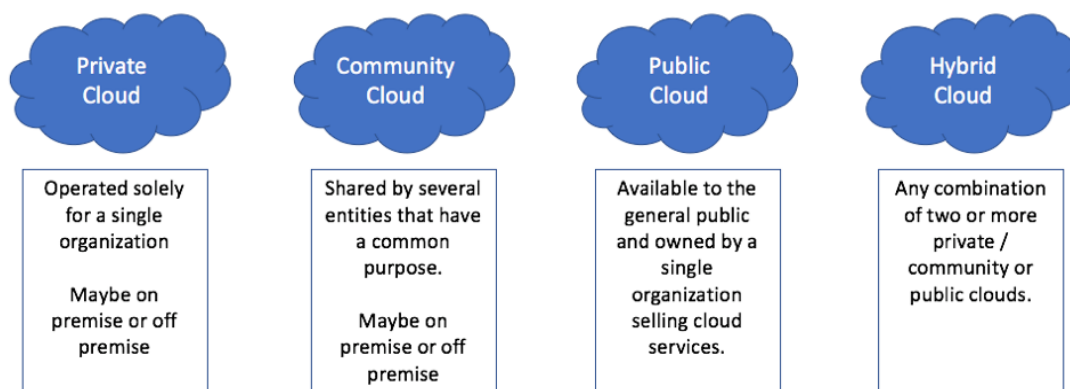


Figure 2.2 Types of Cloud computing deployment

### **A. Software as a Service (SaaS)**

In the SaaS model, end users or customers are able to access provider's applications on the cloud from their devices, usually through a web interface. In this model, services are offered as applications to users on demand basis. In the SaaS model a single instance runs on the service provider's cloud which supports multiple access instances on the client's side. Thus reducing cost for both the service provider and the customer, since customers does not need to spend money on software licensing or servers, and as well, since only a single instance is required to be hosted and maintained, it reduces cost effectively for the service provider. In the SaaS model, the service providers such as Google, Salesforce, Microsoft, Zoho, etc. solely own the management and control of cloud infrastructure, including servers, network, systems and applications.

### **B. Platform as a Service (PaaS)**

The PaaS model offers a development environment as a service, which can be used by clients to build and deploy their applications. This model supports programming languages and other tools such as Python, .Net, Java, Apache Server, MySQL Server etc. that client can leverage without the need to install an OS or maintain an infrastructure. Even though clients do not have the eligibility to manage or control cloud infrastructure like servers, storage and other hardware, they still owns the control and management of the applications deployed and may possibly share some security responsibilities over the hosting environment. Some examples of PaaS are: Google's App Engine, Force.com, AWS Windows Azure, etc.

### **C. Infrastructure as a Service (IaaS)**

The Infrastructure as a service (IaaS) model serves as a substructure of the other models, whereupon a PaaS is built, and upon which a SaaS is built. In this model, service providers such as Microsoft Azure, Google Compute Engine (GCE), Amazon, GoGrid, 3 Tera etc. provide primary computing privileges to clients to enable them control over storage, networks, servers and other computing capabilities.

The services are provided to clients in a form of rent, and thus clients do not own or manage the cloud infrastructure, but rather has the control over operating systems, storage systems, deployed applications, and may also be able to select networking components (e.g., firewalls, load balancers etc.). Fig 2.3 presents the relationship between all the cloud delivery models.

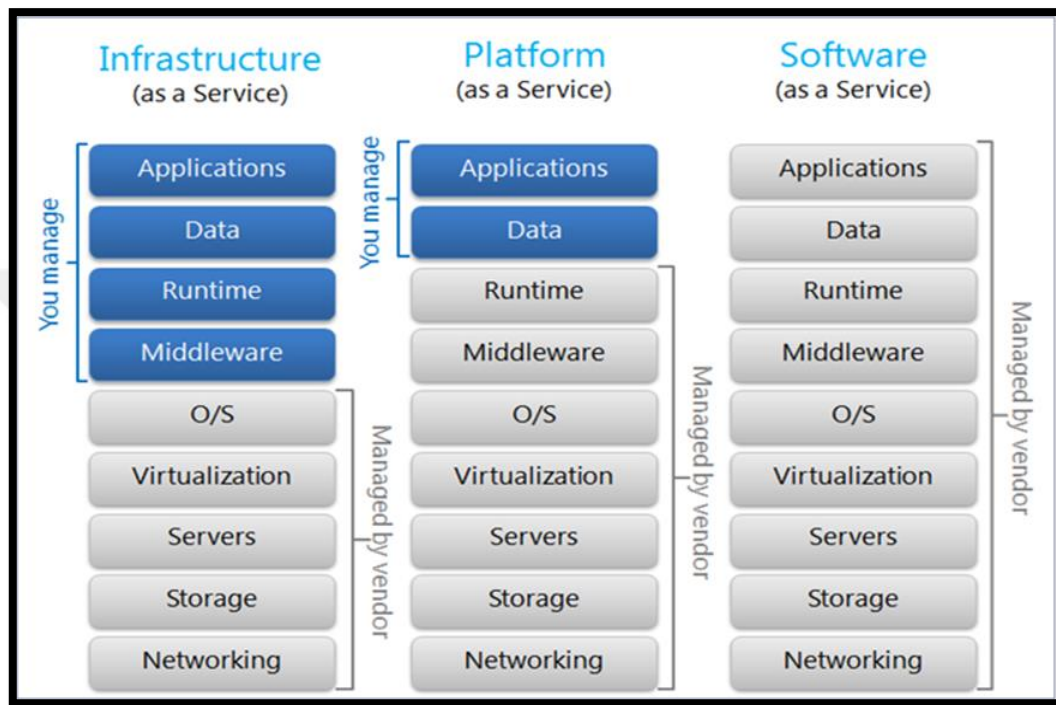


Figure 2.3 Cloud delivery models (Benson & Tim, 2012)

## 2.3 Mobile Cloud Computing

Whereas Cloud computing is the method in which resources are provided on an on-demand basis to a local client, typically through the internet. Mobile cloud computing (MCC) can simply be referred to as cloud computing which involves the use of mobile devices.

Mobile cloud computing in healthcare sector can play a vital role in improving operations as well as reducing cost effectively. Application of mobile devices in cloud computing provides pervasive and ubiquitous access to data stored in the cloud which is very essential in decision making in the healthcare sector for a proper diagnosis and treatment, and also helps in reducing possible medical errors.

Among the numerous head starts of cloud computing is reducing downtime and cost on expenditure for servers and other computer hardware equipment. In order to handle stress on a company's system in situations where strain and traffic are greatly variable, lots of money is spent on the needed hardware.

Moreover, mobile cloud computing brings about a significant benefit to cloud computing, in the sense that, it solves the problem of restrictions on mobile devices due to the mobility features such as smaller sizes and light weights. In order to perform intensive tasks, longer battery life and other hardware and software developments are required. Thus, when resources are moved to the cloud, mobile devices are only used as intermediary to show results and all the operations are done on the cloud. This also achieves the needs of users to stay connected and get access anytime anywhere as well as decreasing cost effectively.

Several papers have been written proposing divers approaches to mobile cloud computing where mobile devices serve as a client and other non-mobile devices as servers or mainframe. In this approach, mobile devices serve as an intermediary between users and the cloud, to enable a pervasive and ubiquitous access to cloud services.

Finally, this paper will also focus on issues that could hinder the widespread use of mobile cloud computing such as privacy, security and other concerns related to cloud computing, often specifically to mobile cloud computing.

## **2.4 Issues with Mobile Cloud Computing**

Contrary to standard computing, Cloud computing as a new paradigm where management of the data stored on the cloud is being handled by third parties, users have many concerns, which include reliability, data ownership, privacy and security. Whereas mobile cloud increases accessibility as well as decreases cost more effectively, these issues become especially crucial with mobile devices, thus, methods and techniques needed to tackle these issues shall be discussed.

### ***2.4.1 Privacy***

Privacy in the cloud is a major concern of users in general. When data is being moved to the cloud and users lose control of it, their major worry is that, the data could become vulnerable, or the parties who own the management and control of the data could sell or give the information to government agencies without the knowledge and permission of users.

The issue of privacy in mobile cloud computing, where mobile devices are involved raises yet another concern. Mobile devices use some applications such as Location-aware applications and services that sometimes require access or knowledge about user's location.

However, one method sometimes used to alleviate this issue is location cloaking, where by the information submitted is made ambiguous. This method however reduces the quality of Location-aware services since the request sent to the server by the mobile client is too ambiguous, inconsequential results could be given as a result. Thus, there is the need for a solution to both privacy concerns as well as location-aware applications.

In attempts to balance between privacy and effectiveness of location-aware applications, Researchers from the university of Hong Kong Polytechnic University have proposed an imprecise location-based range query (ILRQ) which aims at making users location ambiguous and as well prevent tracking users previous locations.

### ***2.4.2 Secured Data Access***

In addition to the aforementioned concerns of cloud computing, safe and secure data accessibility is another important issue. Users need to be able to access their data ubiquitously, especially in situations where system functionalities relies totally on the data stored in the cloud, any failure to access the data can cause a significant damages. Thus, accessibility needs to be made easy and ubiquitous.

In addition, accessibility needs to be safe and secured, such that only the right parties are granted permission to access data stored in the cloud and unauthorized persons denied access.

The desire to stay connected and get access pervasively is being tackled by Mobile cloud computing, nevertheless, accessing the cloud data through mobile devices can be vulnerable. Thus, proper methods needs to be kept in place to handle a safe and secured access with mobile devices.



### **CHAPTER THREE**

#### **RELATED WORKS**

An integrated access control scheme supportive of a patient-based selective sharing of patients' compounded Electronic Health Records (EHRs) in different standards, adapting data accumulation and other required privacy protections has been proposed in (Jin et al., 2011). This approach however requires that all healthcare providers embrace an integrated EHR schema, which is rather not practicable in cloud environments.

Contrary to the above, this method supports EHRs accumulation from diverse healthcare providers taking into account different EHR data schemas in cloud environments. As part of the security requirements for Electronic Health in the cloud, in (Zhang, R., & Ling, 2010), an EHR security reference model that supports the sharing of EHRs is proposed. For privacy protection of Electronic Health Records in the cloud, a patient-centered digital right management (DRM) has been proposed in (Jafari et al., 2011), based on patient preferences. This approach is however not very precise and also does not support what is required for a selective EHR sharing. A mobile querying of disseminated XML database within a widespread of healthcare systems, has been examined by Al Kukhun et al (Kukhun, Dana, Sedes, & Florence, 2008). The method however is not based on cloud and thus, does not take into consideration the requirements of HER unification from various healthcare providers. In (Li et al., 2010), an attribute based encryption (ABE) techniques has been leveraged, to present a new access control infrastructure for privacy patient personal health records in cloud computing. Basically, this approach aims at ensuring that EHRs are shared only among a selected set of users. Sharing of selective parts of access control entities with the rightful users approach has been proposed in (Takabi, Hassan, James, & Ahn, 2010). This approach however does not support mobility, such as using smart phones and tablets in the sharing of EHR for consumers. In contributing to the requirements of a safe and secure sharing of data in the cloud computing environment, a solution for sharing of Electronic Health Records (EHRs) among varied healthcare providers has been proposed in (Saif et al., 2011), by applying a technique of engineering network resolution for data sharing. This work

mainly focuses on two main delegations: role-based and signature-based. The Signature-based is in charge of making a secure path for fundamental delegation and retrieval, whereas the Role-based is responsible for providing dynamics for availability, change and delegates' status. In addition, this paper has also implemented basic access control using public key encryption techniques to ensure secure sharing of data as well as protection of patients' privacy among all the participating healthcare providers. Nevertheless, the application of proxy sign-in in the system makes it vulnerable to yet another high security risk.

Ubiquitous mobile information systems have been on demand over numerous fields, because of the swift propagation of wireless and mobile technologies. In addition, mobile communication has become one of the most important and popular infrastructure for our lives. Mobile technologies give great opportunities for many industries. Mobile applications have been focused on wireless sensor nodes such as RFID tags, NFC tags and mini sensor nodes, particularly for hospital environments with mobile devices. Healthcare solutions are sliding into the Ubiquitous healthcare technique, merging a varied sensors and mixed networks. The ubiquitous hospital network allows users to record patient's health records and to have the information related to the patient or treatment from HIS by utilizing mobile devices. Barcode, RFID and NFC technologies are being used in ubiquitous health information system to improve the quality of the current healthcare system.

With the advancement of mobile technologies, healthcare systems could better be improved by leveraging mobile devices with NFC and Bluetooth interfaces, smartcard technology on temper resistant secure element (SE) for the storage of patient details and data security as well as a HealthSecure service on a hybrid cloud for security and health record management (Ngai et al., 2009). The main focus of this paper constitute three proposed applications as (i) Medical errors reduction through a Secure Medical Tags and ii) Storing Electronic Health Record (EHR) based on Secure NFC Tags through a Secure Healthcard, and a mobile device using NFC P2P Mode or Card Emulation Mode.



Sanchez et al., (Sánchez et al., 2012) proposed PharmaFabula project to recognize medicines and reports for the patient information. They proposed the utilization of NFC technology in the medical field for helping blind users. The e-MAR (Landman et al., 2014) is used to assess the effectiveness of the NFC technology in these solutions as a tool for training and some other tasks. NFC enabled mobile device is used to track self-reported patient outcomes (Wu, Ruoyu, Gail-Joon, & Hongxin, 2012) and medication compliance in both routine treatment and clinical trials (Chen et al., 2012). Benelli et al. proposed other applications for NFC health care (Benelli et al., 2010). These previous NFC health care applications have limited evaluations, and have no security primitives. In contrast our approach focuses on authentication and Secured NFC data transfer using mobile devices and cloud computing.

Cloud computing as an emerging paradigm dedicated to improving network systems, a development of a three-tier cloud based application has been proposed aims at improving the traditional healthcare system involving varied healthcare providers (Rainer & Schahram, 2005). By using the eHealth cloud, huge sums of eHealth data are stored continuously, and as this continues, the need for a new research solution is required. Thus extracting useful data from the large amount of electronic medical records (EMR) is needed for proper decision making in the healthcare sector. Data mining process has been proposed to analyze huge sets of raw data, discover hidden patterns and to come out with useful data which essential for a proper decision-making in the healthcare sector. This can be achieved by applying the HL7 standard exchange method. HL7 is a widely accepted standard for the exchange, integration, sharing and retrieval of eHealth data. This method has been adopted globally and it has a well-defined standard for sharing of eHealth data.

This study takes into account all the shortcomings and lapses of previous related works to make a difference by proposing a design of a robust, pervasive, ubiquitous nevertheless a simplified and effective system that aims at ensuring security, privacy, reliability and availability of patient's records. Next section is a discussion of our proposed solution.

## **CHAPTER FOUR**

### **PROPOSED SOLUTION**

The biggest impediment and the most crucial issue patients have is privacy of e-healthcare deployment (Benelli et al., 2010). In this study a renewed, and initiation of near field communication NFC-enabled (MPS-Mobile) development is proposed for the authentication and Secured NFC data transfer for patients. The difference between the conceptual work (Özcanhan et al., 2014) and this paper is the secured NFC card approach. In the conceptual study, two different timestamps are kept, but when implementing the system, two different timestamps are XORed and then, stored in the MP-Card that simplifies the operation without any information lost as the previous timestamp is already stored in the database. MPS-Mobile is a mobile device equipped with NFC reader and a server side wireless communication protocol to support a secure exchange of data by either proximity or touch.

#### **4.1 Medical Passport System**

The Medical Passport System (MPS) is a card that is used to store or retrieve patient's health records, medical histories and other relevant information for a smooth and better treatment process. Access to patient's medical records is very crucial in achieving a better treatment devoid of medical errors. This scenario is even more vital in cases of emergencies, where patients are not in the condition to answer questions about medical histories, medication, allergies, etc. Thus, the patient's medical records need to be kept updated on a regular basis.

The information contained on this card is considered crucial and confidential, and is therefore protected by law. Other parties who might have access to it such as doctors or any medical practitioner is expected to protect its privacy and therefore, information on the card can only be shared with whom it may concern or authorized parties. Thus, a disclosure of the information found on the card without the knowledge and authorization of the patient will make the person responsible for any damages in a court of law (Indiana, 2017).

#### **4.1.1 Confidential Medical Records**

Presented in this part are details contained in medical records, based on which rightful decisions can be taken and possible medical errors can be avoided (Indiana, 2017).

Table 4.1 Patient's personal details

	Last Name	First Name	Middle Name
Name			
Medical_id #			
Date of Birth			
Ethnicity			
Native Language			
Mother's Name			
Father's Name			

#### **MEDICAL-ALERT**

(Critical medical conditions including Ischemic heart diseases, Stroke, Respiratory cancers, Diabetes mellitus, Alzheimer's disease, sickle-cell diseases, etc.)

---

---

---

---

---

#### **ALLERGIES**

(Bee stings, medications, foods)

---

---

---

---

**ADVERSE (DRUG) REACTIONS**

(Rashes, ashes, jaundice, anemia, a decrease in the white blood cell count, kidney damage, etc.)

---

---

---

---

---

**ASSISTIVE DEVICES/EQUIPMENT**

(Glasses, cognitive aids, hearing aid, mobility aids, etc.)

---

---

---

---

---

**SPECIAL DIET**

---

---

---

---

## MEDICAL HISTORY OF A CHILD

Table 4.2 Child's birth details

	Hospital of Birth
Hospital Name	
City	
State	
Zip	
Child's Birth Weight (lbs. and ozs)	

## PROBLEMS RELATED TO PREGNANCY OR DELIVERY

---



---



---



---



---

## SPECIAL CARE NURSERY HISTORY

(Reason for staying in a special care nursery, duration of stay, etc.)

---



---



---



---



---

## CHRONIC HEALTH DISEASES

- |  |  |
|--|--|
| <input type="checkbox"/> Ear Infection | <input type="checkbox"/> Urinary Problems    |
| <input type="checkbox"/> Eczema        | <input type="checkbox"/> Bone/Joint Problems |
| <input type="checkbox"/> Asthma        | <input type="checkbox"/> Heart               |
| <input type="checkbox"/> Seizures      | <input type="checkbox"/> Diabetes            |

☐ Developmental Delay

☐ Other

Explain:

---

---

---

---

---

### **TRAUMA**

(e.g., fractures, head injuries, burns)

---

---

### **CHILDHOOD ILLNESSES**

Chickenpox	<input type="checkbox"/>	German measles (Rubella)	<input type="checkbox"/>
Infectious Mononucleosis	<input type="checkbox"/>	Measles (Rubella)	<input type="checkbox"/>
Meningitis	<input type="checkbox"/>	Mumps	<input type="checkbox"/>
Roseola	<input type="checkbox"/>	Scarlet Fever	<input type="checkbox"/>
Other			

---

---

---

### **SENSORY PROBLEMS**

Vision ☐

Hearing ☐

Other ☐

Start Date

Start Date

Start Date

Explain:

---

---

---

---

---

**ADDICTIONS:**

Cigarettes ☐

Drug Use ☐

Alcohol ☐

Other

---

---

---

---

**BIOLOGICAL FAMILY HISTORY**

**Maternal History**

☐ Diabetes

☐ High Blood Pressure

☐ Substance Abuse

☐ Kidney Problems

☐ Asthma

☐ Epilepsy, Seizures

☐ Birth Defects

☐ Deafness

☐ Death Under 50 Yrs.

☐ Heart Attack Under 60 Yrs.

☐ Positive TB Skin Test

☐ Stroke

☐ Stomach/Intestinal

☐ Mental Retardation

☐ Psychiatric Problems

☐ Blood Disease:

☐ (a) Anemia (b) Sickle Cell

☐ Other

---

---

---

---

**BIOLOGICAL FAMILY HISTORY**

**Paternal History**

☐ Diabetes

☐ High Blood Pressure

☐ Substance Abuse

☐ Heart Attack Under 60 Yrs.

☐ Positive TB Skin Test

☐ Stroke

<input type="checkbox"/> Kidney Problems	<input type="checkbox"/> Stomach/Intestinal
<input type="checkbox"/> Asthma	<input type="checkbox"/> Mental Retardation
<input type="checkbox"/> Epilepsy, Seizures	<input type="checkbox"/> Psychiatric Problems
<input type="checkbox"/> Birth Defects	<input type="checkbox"/> Blood Disease:
<input type="checkbox"/> Deafness	<input type="checkbox"/> (a) Anemia (b) Sickle Cell
<input type="checkbox"/> Death Under 50 Yrs.	<input type="checkbox"/> Other

---



---



---



---

MPS-Mobile will be developed using an easy to find tablet running Android operating system and having NFC support. One of the major benefits of the MPS-Mobile includes the increasing security of data transfer. The main contribution of this paper is the proposal of a robust secure ubiquitous healthcare application and Mobile cloud computing, using Android based mobile devices with NFC. Authentication operation is performed by NFC authenticate protocol in PACS-Server. The standard NXP Mifare DesFire EV1 protocol works on tablet with NFC card. In each operation, there are different calculations like Cipher-based Message Authentication Code (CMAC), wrapping etc. In the protocol, these operations are made on NFC enabled device and requests are sent to NFC card by mobile devices. In this study, this protocol is modified and all the operations are carried out on the PACS-Server. Thus, a mobile device just works as an ambassador to send and receive messages between server and the card. Next section talks about the custom MPS protocol.

## 4.2 Authentication and Message Protocol

### 4.2.1 Proposed MPS Protocol

In this study, 13.56 MHz HF contactless cards will be used. They provide a more secured mechanism with AES encryption support. In the PACS-Server application, a random app ID and a secure key are being created and a write command is being generated with this random data. After creating the message, server sends commands to the mobile device and mobile device runs the command on the NFC card. This



scenario creates an application on the card with pre-created secure key. With this approach, only one application is being used on the card. In all further operations, server creates commands with finding card application ID from the database by using card's unique secure key. With this methodology, the tablet doesn't need to know neither card application ID nor its secure key. Also, the mobile device doesn't need to know which command should be sent to the card or what the response of the card is. Tablet only becomes the communication bridge between the card and the server. Also remaining applications of the card are free to use for further improvements or by other applications.

This protocol is re-written on the server to ensure NFC cards are being used by right personnel that are registered with the system, shown as Figure 1. Both mobile device and the server calculate data using protocol and server compares them. If they are the same, server decides NFC card is already registered with the system. This approach is being used for specific operations.

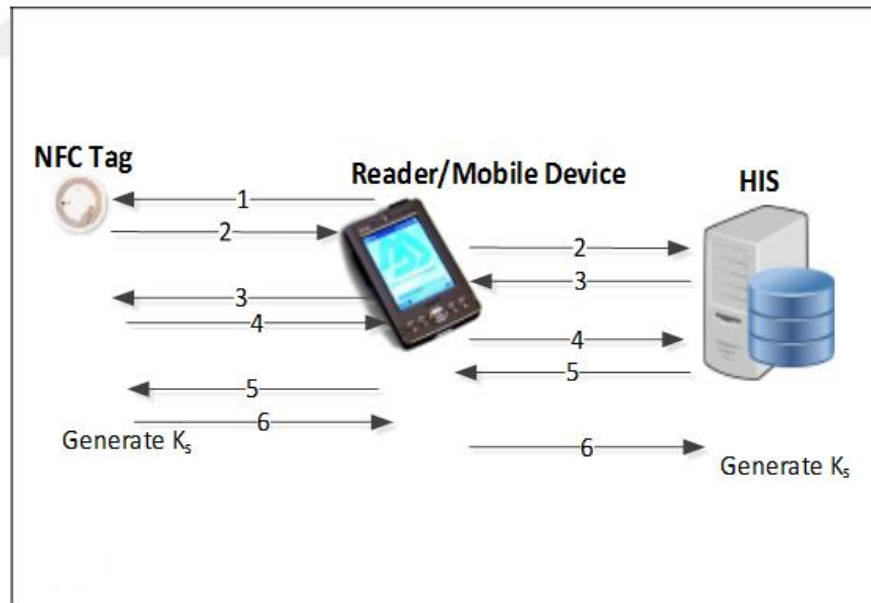


Figure 4.1 Custom MPS Protocol (Özcanhan et al., 2014)

#### ***4.2.2 Broker-Based Composite EHRS Authorization***

A Broker-based authorization is used to grant authority to a user or group of users to enable them perform specific tasks against a broker and its resources. A broker-based in the cloud-computing environment is used to manage access and selective sharing of patients' health records that are integrated from various healthcare providers (Wu et al., 2012). An overview of the general architecture of the approach is shown in Fig.4.2 below. Cloud computing provides numerous advantages such as cost effective, ubiquity, higher interoperability and so on. Thus to achieve these advantages, various Healthcare providers from varied domains move their Electronic Health Record systems to the cloud on either a single cloud or multiple clouds, such as public cloud, private cloud, or a mixture of both, (hybrid cloud), depending on their requirements.

As shown in the figure below, two sub-modules (EHR Aggregator sub-module and the Policy Manager sub-module) have been included in the Composite EHRS Access Broker (CEAB) module, which serves as a Middleware between users and the system. The EHR Aggregator sub-module is in charge of retrieving and gathering distributed EHRs among various clouds to form a virtual composite EHRs. The Policy Manager sub-module on the other hand is used to manage the sharing process by controlling the specifications and enforcement of access control policies. Four main stakeholders including Patients, Authorized users or Patient's Caretaker, Healthcare Practitioners and Administrators. Patients are the rightful owners of EHRs and are therefore have the right to define access control policies to manage who can access the system and which portions of it. Authorized users (Patient's Caretaker) are also given access to the EHRs of the patient. Healthcare practitioners who are usually associated with specific healthcare providers also gets access to the EHRs. In addition, for administrative purposes, administrators also gets access to EHRs.

### 4.3 System Architecture

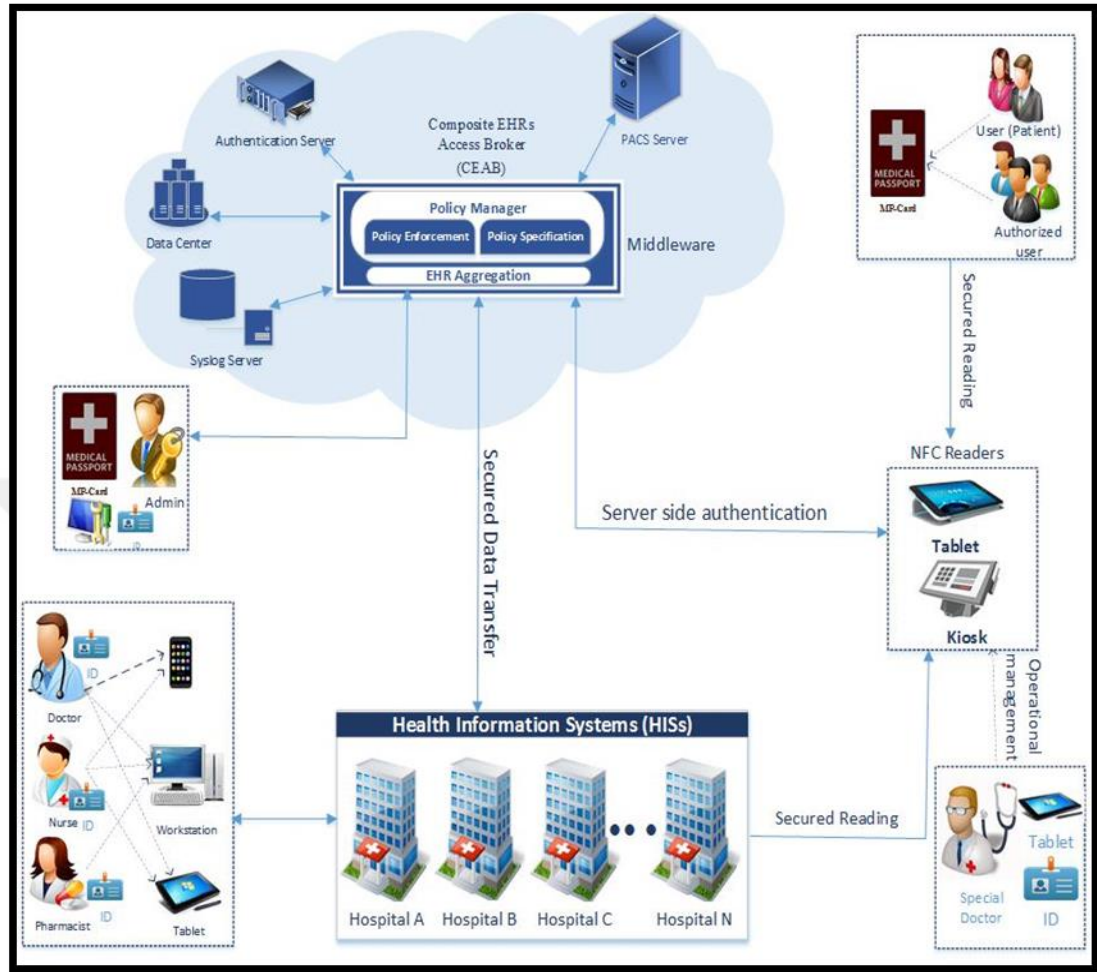


Figure 4.2 Architecture of a Medical Cloud Database Service System

#### 4.3.1 System Description

The system is composed of (a) a Data Center (b) a Syslog Server (c) a PACS Server (d) an Authentication Server and (e) a Unifier Interface Middleware (UIM).

##### (a) The Data Center

The Data center is a centralized repository where computing and networking equipment are kept for data management and accessibility purposes. Thus, cloud datacenter holds a central data warehouse for all the collaborating hospitals, for the

storage and retrieval of medical records. The storage of data is done in an integrated and standard format, thus making it easy to be retrieved from all the participating hospitals through the Unifier Interface Middleware (UIM).

#### **(b) Syslog Server**

Syslog is a standard way for network devices to send log messages within a network to a logging server, known as a Syslog server. A heterogeneous range of devices, which can be used to log varied types of events, supports the Syslog protocol. The syslog reviews the data contained in the log and gives information such as error and warning events connected to the computer operation system. Through this, a user or an admin will be able to identify the cause of a problem.

#### **(c) PACS Server**

PACS is a storage format used in medical imaging technology, which ensures a digital storage, transmission and a suitable access to images from various techniques. This system has both software and hardware components through which electronic images reports can be transmitted digitally, and then uses a workstation for viewing purposes. DICOM (Digital Imaging and Communications in Medicine), is the general format for PACS image storage and transfer. With the DICOM format, PACS system is able to work across various modalities and workstations smoothly (Abdulrahman, Bahce, Utku, & Vladimir, 2018).

#### **(d) Authentication Server**

Authentication is a way of verifying a user, by determining whether a user is actually who or what it declares itself to be. When a potential user tries to access an authentication server, a username and password may be required in order to identify the user. Thus, an authentication server verifies whether or not an entity attempting to access the health information system, which includes updating, transferring, retrieving, etc., has the right to do so. It then grants access to rightful users and denies any other without the right to access the system. Therefore, all authorized users from

all the participating hospitals have a username and a password, with which they log in to the system.

#### **(e) Middleware (Composite EHRs Access Broker (CEAB))**

Middleware is a kind of software that is used to connect multiple Electronic Health Record systems of the collaborating hospitals. The middleware in the cloud serves to provide a standard platform for all the participating hospitals, thus making interaction between these hospitals and the Central database easy and secure. It intercommunicates with all the participating hospitals through network communications, thus each of the hospitals can easily interact with the cloud without the need for it to have its own interface.

### **4.4 Electronic Medical Record (EMR) Mining**

Data mining is the process of extracting useful data from larger data sets in order to find hidden patterns and to create relationships within the data for decision making purposes. This is made possible by analyzing data using a data mining software. EMRs contain detailed patient information including personal data and medical history such as demographics, medications, lab tests, etc. Mining these data and extracting useful data would help improve decision making in the health sector, as EMRs contain detailed health records for large number of patients. For a proper exchange of data in the healthcare, EMR needs to be built on a standard data exchange.

#### ***4.4.1 Standard Data Exchange Method***

The widely accepted method for global health data interoperability and for EMR implementation is the Health Level Seven International (HL7). This method was founded in 1987, is an accredited standard devoted for the provisioning of framework and other related standards. It also enables the exchange, integration, sharing, and retrieval of eHealth data, supporting the management, delivery and evaluation of healthcare services and applications. HL7 has been adopted internationally, including

organizations, healthcare providers, pharmaceutical companies, vendors/suppliers and government stakeholders (Biswas et al., 2014). Users and applications can exchange documents through the HL7 web service for an efficient and well-defined format of sharing healthcare Information. The EMR creates a cloud layer that empowers accessibility to eHealth records for organizations through the HL7. Thus, the HL7 web service makes access to global eHealth data pervasive and ubiquitous for all the participating parties, and ensures safety and security, as shown in the figure 4.3.

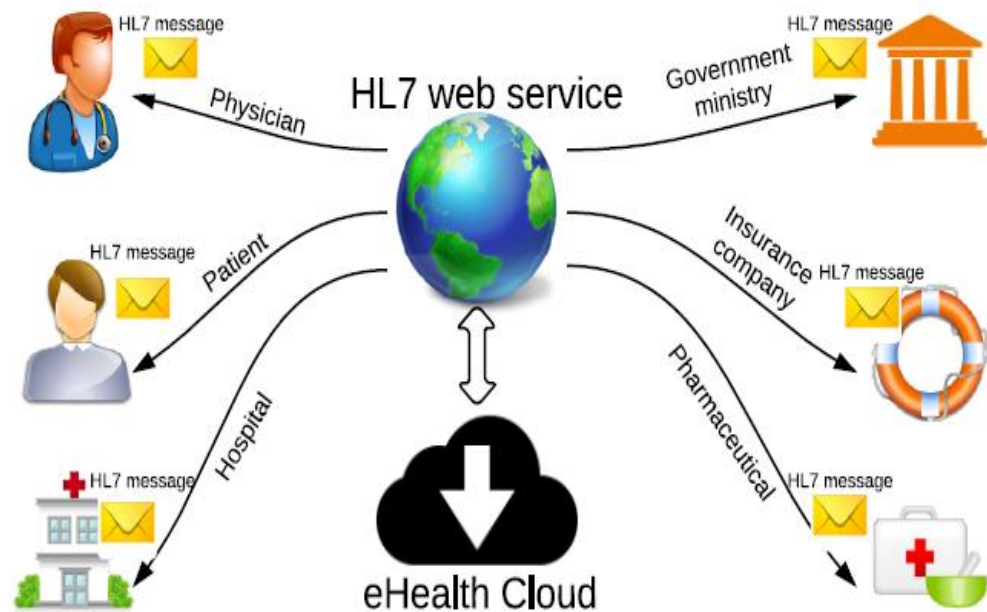


Figure 4.3 HL7 web services (Biswas et al., 2014)

#### 4.5 What kinds of healthcare information can Medical Passport Store?

Medical Passport in a form of a smart card can be used to store a wide variety of patient's information to support healthcare process, by linking it to the health information systems based in the cloud. Figure 4.4 shows examples of the kinds of healthcare information that may be stored on a Medical Passport

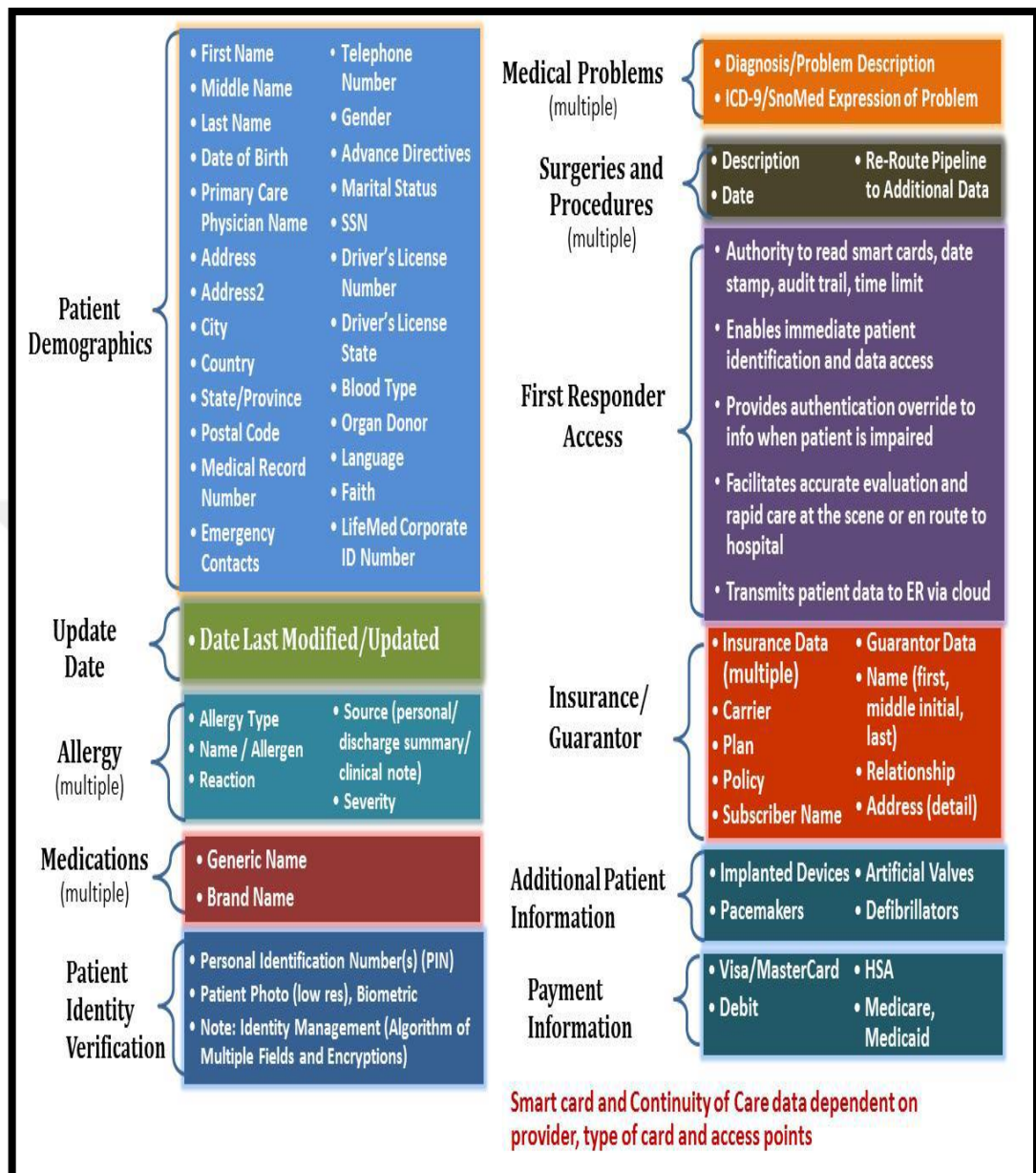


Figure 4.4 Kinds of healthcare information Medical Passport stores (Alliance, 2012)

## **CHAPTER FIVE**

### **EVALUATION**

#### **5.1 Security Test Results**

MPS-Mobile application collects necessary data from the user and sends them to the server in a secure way. All the users have their pre-defined NFC cards on the system. A user must log in to the mobile application with his\her NFC card and user information to start the application. Securing web service and messaging is provided by enabling https and encrypting the body of the soap messages. Also, some sensitive data is hashed to be compared between the mobile device and the server. With all these securing mechanisms in place, to ensure a more secured communication on the hospital network, HTTPS over SSL/TLS is enabled.

Security tests were proceeded with enabling/disabling Tomcat SSL support. A certificate was created using Java key tool and self-signed with OpenSSL to enable SSL support. Port 8080 was dedicated for http and 8443 was dedicated for https connection. With this test, the web server was sniffed with WireShark. Results show that it is possible to get data when SSL is not enabled. When SSL is enabled, it is not possible to get the raw data. Test results show that unauthorized access to sensitive data is not possible in normal circumstances, owing to SSL/TLS, AES encryption and RSA support. Even so, if an attacker cracks SSL and RSA encryption, he will meet encrypted messages, that are encrypted with AES. Thus attacker cannot access decrypted messages without encryption keys.

Notwithstanding, attacks like ‘Man in The Middle Attack’ are still a concern for SSL. In turn, some extra security option is added into the web services. The SOAP messages are encrypted with AES via pre-shared 128 bit keys. Android applications are able to decompile by third party applications. Thus it is possible to get encryption keys and algorithms from cracked devices. This is a big security problem if device is stolen and IT is not notified immediately.



Also there was another problem with cracking android devices. In normal state, NFC commands should be created by device and communication should be between device and NFC cards. But the need to crack android devices has led us to implement a more secure way. To achieve a more secure and reliable way, the device was eliminated as a primary contractor with NFC cards. In this solution all commands are being created by server and all response are sending to server directly as encrypted. In this method tablets are acting as a messenger, without knowing the contents of the messages. All this messages are encrypted. Secure mechanism is coming from Mifare Desfire EV1s. These cards have built in 3DES AES encryption mechanisms. All mechanism is implemented on the server with contacting NXP. Therefore, with knowing key of the card, it is possible to create a communication between server and NFC card. Next section presents the system simulation.

## **5.2 Healthcare Simulation**

Figure 5.1 below is a screenshot of simulation of a healthcare process in a hospital, using Simio software (Pegden & Dennis, 2007). In this simulation one registration desk, one basic evaluation, one advanced evaluation, one lab work and then a checkout are used.

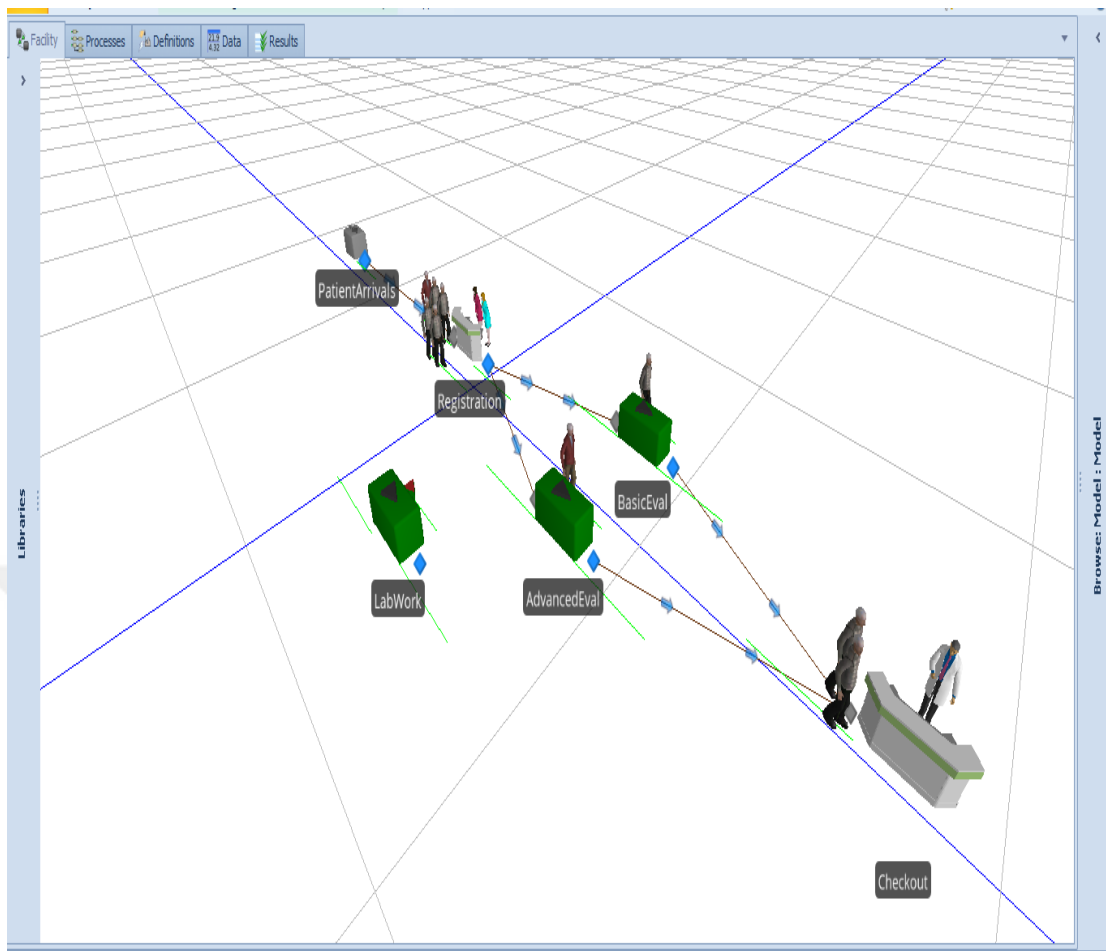


Figure 5.1 Simulation of a healthcare process in a hospital

### 5.2.1 Registration Desk

The registration desk, which is a standard server, is where the registration process of patient is done. This process includes finding patient name, which is a 5-minute delay, and then sending details to nurse, which also takes 10 minutes.

### 5.2.2 Basic Evaluation Stage

This stage is also a standard server with an infinite capacity, preliminarily. Patients who are categorized as mild sick, based on their condition, are the ones who go through the basic evaluation stage. This stage includes several tasks such as, getting vital information, which takes 4 minutes, another 6 minutes for Evaluation with doctor, and then 2 minutes for follow up.

### ***5.2.3 Advanced Evaluation Stage***

The advanced evaluation is for patients categorized as sick type. This stage is also a standard server with an infinite capacity, preliminarily. This stage also include activities as Evaluation with Doctor which takes 15 minutes, and Send Lab Work process, which probably occurs for about 70% of patients.

### ***5.2.4 Lab Work Stage***

At the Lab Work Stage, unlike the previous stages, longer time is spent. The process here includes a SubModel, wherein a 'LabWorkOrder' is created as an EntityType to be sent to the 'Input@LabWork', which is the StartingNode and point of entry for the LabWork stage. This process takes 20 minutes and is considered as the last stage, after which the patient proceeds to the Checkout stage.

### ***5.2.5 Checkout***

The Checkout stage is the last activity for all types of patients, and the process here takes only 1 minute of paperwork.

## **5.3 Comparison Between the Current System and Our Proposed System**

Based on the simulation work performed above it is observed that treatment process in the proposed system using the Medical Passport technology results in a more time saving and accelerated work as compared to the normal treatment process, as shown in the table below. Table 5.1 shows a Simulation Results for the Current HealthCare System and the Proposed System.

Table 5.1 Comparison between current system and the proposed system

	<b>Registration Desks</b>	<b>Basic Evaluation</b>	<b>Advanced Evaluation</b>	<b>Lab Work (LabWorkOrder)</b>	<b>Checkout</b>	<b>Number of patients /day</b>
<b>Current System</b>	15 minutes	12 minutes	15 minutes	20 minutes delay	1 minute	100
<b>Our Proposed system</b>	1 minute	12 minutes	15 minutes	8 minutes delay	1 minute	160

From the above table, comparison between current systems and our proposed system shows that, with our proposed system, much time is saved throughout all the processes, from registration, basic evaluation, advanced evaluation and lab work. Due to the fact that with the Medical Passport card, access to patient records becomes faster and easier. It helps even more when patient moves to a different city or country. With the current system, access to patient medical records or history takes much more time as patients might have to undergo retesting. But with our proposed system based on cloud, access to medical records remains easy anytime anywhere. Also as much time is saved it makes a way for more patients to be attended to. As a result, time is saved, number of patients per day is increased and thus general cost is decreased.

## **CHAPTER SIX**

### **DISCUSSION AND CONCLUSION**

#### **6.1 Discussion**

This paper aims to create a ubiquitous system for the storage of patient health records in the cloud by integration from various Hospital Information Management Systems (HIMs) and to provide a safe access to this information anytime anywhere by utilizing NFC technologies. This will facilitate and improve treatment processes in the hospitals, reduce the work of personnel, as less time will be spent to access patient records and history. Patient data security is one of the most important concerns; which is attained with proposed improvements, using different encryption methods and approaches. To ensure a more secure system, NFC cards are used to authenticate users after logging in to the application with their user name and password. NFC cards are not able to be copied. This prevents accessing data with an un-registered NFC cards. For management of access and or sharing of EHRs integrated from varied healthcare providers in the cloud, a broker-based authorization approach is also proposed which support selective sharing and also manages access to system in the cloud. This approach consist of two sub-modules: (a) the EHR Aggregator sub-module and (b) the Policy Manager sub-module. The EHR Aggregator sub-module is responsible for retrieving and aggregating Electronic Health Records among various clouds to form a virtually compounded one, whilst the Policy Manager sub-module is responsible for supporting the definition and implementation of access control policies to manage the sharing of composite EHRs. By this patient health records can only be accessed by patients and people who are been authorized by the patient.

One of the major benefits of the system is using the Medical Passport card technology for patients, which stores both patient's personal information as well as medical records. With this card, patients can access their medical records easily anytime anywhere, and thus patients will not have to re-test in case they travel or visit a hospital different from their previous hospital. Doctors, nurses and pharmacists use a well-known NFC card similar to their credit cards. In the patients

case, the Medical passport acts as an NFC card. To increase portability, tablets are used in the system. The tablets are regular Android based tablets that the users do not need to be trained to use.

A simulation of a healthcare system has been carried out in a hospital, the outcome of which is compared to that of the proposed system as shown in the table above. It can be seen that at the registration desk 1 minute delay instead of 15 minutes, at the lab work 8 minutes delay instead of 20 minutes, and the number of patients per day has also increased from 100 to 160 patients.

The overall impact of the system is pervasive and ubiquitous healthcare service, time saving, accelerated treatment process with relatively lower cost.

## **6.2 Conclusion**

In this study, a robust pervasive and ubiquitous healthcare service system, based on mobile cloud computing has been designed and implemented. With the benefits offered by cloud computing and mobile devices, adapting the use of them in healthcare systems brings about more advancements and accelerated treatment process, as much time is saved, the work of personnel lessens and costs of healthcare delivery is reduced in the broader sense. To achieve this in our study, patient health records are being integrated from various HISs at a center in the cloud and a secured measures are adopted in order to access and or share these critical information safely. 13.56 MHz HF contactless NFC cards are used. They provide a more secured mechanism with AES encryption support. Their use also provide a secure data transmission mode on every item in the system. With the NFC cards as a Medical passport, mobility of patients from hospital to a different hospital, city to city or country to country, access to medical records is made easier. In addition, issues related to the selective sharing of EHRs in cloud computing environment has been identified and segmented. Thus, the broker-based authorization mechanism presented will ensure that only those with authority to do so can have access to EHRs and are able to selectively share portions of the EHRs with healthcare practitioners or family members.

### **6.3 Future Works**

As part of our future work, we would treat a more thorough authentication methods and more advanced security measures on our system. In addition, effective and more secured mechanisms for the sharing of HER in the cloud environment will be focused on. For ubiquity purposes, our approach will also focus on supporting the use of smart devices such as mobile phones and tablets in accessing and sharing of the EHRs.



## REFERENCES

- Abdulrahman, M., Bahce, A. Utku, S., & Vladimir, S. (2018). Medical image data management system in mobile cloud computing environment. *2nd International Students Science Congress*, (58-59).
- Agrawal, P., & Bhuraria, S. (2012). Near field communication. *SETLabs Bridfings*, 67–74.
- Ahn, J., G., Hu, H., Lee, J., & Meng, Y. (2010). Representing and reasoning about web access control policies. *2010 IEEE 34th Annual Computer Software and Applications Conference* (137-146). Arizona: IEEE.
- Al Kukhun, D., & Sedes, F. (2008, June). Adaptive solutions for access control within pervasive healthcare systems. In *International Conference on Smart Homes and Health Telematics* (42-53). Berlin, Heidelberg: Springer.
- Alliance, S. C. (2012). Smart Card Technology in US Healthcare: Frequently Asked Questions. *Estados Unidos: Smart Card Alliance*.
- Benelli, G., Parrino, S., & Pozzebon, A. (2010). RFID Applications for Sanitary Environments. *Sustainable Radio Frequency Identification Solutions*, 175.
- Benson, T. (2012). *Principles of health interoperability HL7 and SNOMED*. Berlin, Heidelberg: Springer Science & Business Media.
- Biswas, S., Akhter, T., Kaiser, M. S., & Mamun, S. A. (2014). An integrated approach to improve healthcare system. In *2014 17th International Conference on Computer and Information Technology (ICCIT)* (286-291). IEEE.



- Chen, Y. Y., Huang, D. C., Tsai, M. L., & Jan, J. K. (2012). A design of tamper resistant prescription RFID access control system. *Journal of Medical Systems*, 36(5), 2795-2801.
- Coskun, V., Ozdenizci, B., & Ok, K. (2013). A survey on near field communication (NFC) technology. *Wireless personal communications*, 71(3), 2259-2294.
- Hutter, M., Schmidt, J. M., & Plos, T. (2008, August). RFID and its vulnerability to faults. In *International Workshop on Cryptographic Hardware and Embedded Systems* (363-379). Berlin, Heidelberg: Springer.
- Indiana, S. o. (2017, May). *Medical Passport*. Retrieved may 25, 2019, from In.gov: <https://www.in.gov>
- Jafari, M., Safavi-Naini, R., & Sheppard, N. P. (2011, October). A rights management approach to protection of privacy in a cloud of electronic health records. In *Proceedings of the 11th annual ACM workshop on Digital rights management* (23-30). ACM.
- Jin, J., Ahn, G. J., Hu, H., Covington, M. J., & Zhang, X. (2011). Patient-centric authorization framework for electronic healthcare services. *Computers & Security*, 30(2-3), 116-127.
- Landman, A., Neri, P. M., Robertson, A., McEvoy, D., Dinsmore, M., Sweet, M., & Miles, S. (2014). Efficiency and usability of a near field communication-enabled tablet for medication administration. *JMIR mHealth and uHealth*, 2(2), e26.
- Li, M., Yu, S., Ren, K., & Lou, W. (2010, September). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In *International conference on security and privacy in communication systems* (89-106). Berlin, Heidelberg: Springer.

- Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud*. Gaithersburg: National Institute of Standards and Technology.
- Ngai, E. W., Poon, J. K. L., Suk, F. F. C., & Ng, C. C. (2009). Design of an RFID-based healthcare management system using an information system design theory. *Information Systems Frontiers*, 11(4), 405-417.
- Özcanhan, M. H., Dalkılıç, G., & Utku, S. (2014). Cryptographically supported NFC tags in medication for better inpatient safety. *Journal of Medical Systems*, 38(8), 61.
- Pateriya, R. K., & Sharma, S. (2011, June). The evolution of RFID security and privacy: a research survey. In *2011 International Conference on Communication Systems and Network Technologies* (115-119). IEEE.
- Pegden, C. D. (2007, December). SIMIO: a new simulation system based on intelligent objects. In *Proceedings of the 39th conference on Winter simulation: 40 years! The best is yet to come* (2293-2300). IEEE Press.
- Pietrangelo, K. A. (2017). Retrieved July 15, 2018, from <https://www.healthline.com>
- Anzböck, R., & Dustdar, S. (2005). Modeling and implementing medical web services. *Data & Knowledge Engineering*, 55(2), 203-236.
- Saif, S. M., Wani, S. A., Maheswaran, M., & Khan, S. A. (2011). A Network engineering Solution for Data sharing across healthcare providers and protects patients health data privacy using EHR System. *Journal of Global Research in Computer Science*, 2(8), 67-72.
- Sánchez, M. A., Mateos, M., Fraile, J. A., & Pizarro, D. (2012). Touch Me: a new and easier way for accessibility using Smartphones and NFC. In *Highlights on Practical Applications of Agents and Multi-Agent Systems* (307-314). Berlin, Heidelberg: Springer.

- Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, 8(6), 24-31.
- Wei, Z., Chao, F., & Quan, Z. (2014). RFID System security overview. *Network Security Technology & Application*, (9), 77.
- Wilson, K., & Sullivan, M. (2004). Preventing medication errors with smart infusion technology. *American Journal of Health-System Pharmacy*, 61(2), 177-183.
- Wu, R., Ahn, G. J., & Hu, H. (2012, October). Secure sharing of electronic health records in clouds. In *8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)* (711-718). IEEE.
- Wu, R., Ahn, G. J., Hu, H., & Singhal, M. (2010, October). Information flow control in cloud computing. In *6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2010)* (1-7). IEEE.
- Wu, R., Ahn, G. J., & Hu, H. (2012). Towards HIPAA-compliant healthcare systems in cloud computing. *International Journal of Computational Models and Algorithms in Medicine (IJCMAM)*, 3(2), 1-22.
- Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In *2010 IEEE 3rd International Conference on cloud Computing* (268-275). IEEE.