PROTOTYPE TOWARDS SECURE SHARING OF PATIENT'S MEDICAL RECORDS OVER THE INTERNET

Case Study: Mbarara diagnostic center

Kasozi Brandon sad

Registration Number: 2013-M132-20025

Uganda Martyrs University

November 2016

PROTOTYPE TOWARD A SECURE SHARING PATIENTS MEDICAL RECORDS OVER THE INTERNET

Case Study: Mbarara diagnostic center

A postgraduate dissertation

Presented to

Faculty of Science

In partial fulfillment of the requirements for the award of the degree

Master of Science in Information Systems

Uganda Martyrs University

Kasozi Brandon sad

2013-M132-20025

November 2016

DEDICATION

This piece of work is dedicated to the late **Epedu Richard** who taught me how to be a man, to my godfather who showed me the way. To **Martha Nakakande** that made sure I fulfill the dream. To the lady from Kigezi who never went to school but strived to make sure her son gets the education. To the boys and girls who try to make a living on streets because the streets have been our home for long time, it’s their funds that made this happen.

ACKNOWLEDGEMENT

I would like to acknowledge and appreciate the support that I got from different people throughout this course. First and foremost to my supervisor **Dr. Ssembatya Richard** for the intellectual support and guidance that he provided during this research and the entire course. Despite all the errors he didn’t give up on me. In special way thank Auntie Joyce Nampa took me in when Richard was gone. I thank the friends who helped to guide me throughout the implementation of this project. Among these they include Oboth Andrew, Elizabeth Kittaka, Ashaba Robert, Babirye Lucy, Martin Mukama, Nakato Constance and the entire class for having always corrected me where I seemed to go wrong. This project wouldn’t be a success if it weren’t for the input of the respondents who participated in a participatory design. In a special way I would like to appreciate and thank the management of Mbarara Diagnostic lab.

Last but not least, to all the people that I may not have mentioned by name but played big parts in making this project a success. Without your contribution and sacrifice of time I would not have reached this level.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

CCHIT	Certification Commission for Health Information Technology
CPHL	Central Public Health Laboratories
ePHI	Electronic Protected Health Information
FIPS	Federal Information Processing Standard
HIPAA	Health Insurance Profit Accountability Act
HL7.	Health Level 7,
HVAC	Heating, Ventilation and Air Conditioning
LIS	Laboratory Information System
LMS	Lab Management System
MLRS	Medical Laboratory record system
MOH	Ministry of Health
NRC	National Research Council
OS	Operating System
PD	Participatory Design
PHIPA	Personal Health Information Protection Act
RBAC	Role Based Access Control,
SSL	Secure Sockets Layer

UMLTA	Uganda Medical Laboratory Technology Association

ABSTRACT

Medical laboratory testing plays a crucial role in the detection, diagnosis and treatment of diseases in patients. Any attempt to alter clinical data can be a life threat to a patient. However, file sharing Privacy concern is arguably the major barrier that hinders the deployment of electronic health record (EHR) systems, which are considered more efficient, less error-prone, and of higher availability compared to traditional paper record systems. Systems used for diagnosis and treatment have been considered as one of the major hindrances of which data integrity and confidentiality are still an issue because they involve a manual process of obtaining patient records and their retrieval.

In this project an EHR system is developed for case study that is Mbarara Diagnostic center, which is a privately owned laboratory that also provides clinical services with improved security features as its core. The system uses cryptography tools for data encryption that is AES (Advanced encryption standard). The system also caters for user session time out when idol so as to avoid masqueraders from unauthorized access and data modification.

To achieve the objectives of this project, data was collected using paper prototyping as a technique for requirements gathering and elicitation. This approach helped identify fault early in the systems design process. The requirements collected were thematically analyzed and used to design the web based EHR system.

The system developed seeks to provide a cheaper alternative to existing EHR systems. Furthermore to improve quality of data captured for easy access and secured sharing between authorized parties. In addition it will boost client's confidence in services provided at the facility.

CHAPTER ONE

1.0 INTRODUCTION

An Electronic Health Record (EHR) is a record of health-related information on an individual that is created, gathered, managed, and consulted by authorized healthcare professionals in a digital format (HIPAA, 2009). EHRs can exist on standalone computers, networked server computers, removable disks or mobile devices and can be accessible online from interconnected network systems providing the opportunity for healthcare organizations to improve health care delivery. Electronic health records enable the efficient communication of medical information and thus reduce operating costs and administrative workload (Gunter & Terry, 2005). EHRs are built to share information with other health care providers and organizations including laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, and school and workplace clinics – so they contain information from all clinicians involved in a patient’s care. Providing continuous access to patients’ electronic data including lab records improves the quality of health care (Tierney et al, 2006).

This is because Radiologic images, laboratory test results, medications, allergies, and other clinical information are increasingly being stored and viewed on computers. Andriole (2014) emphasizes that it’s a responsibility of physicians to protect these records and ensure their privacy and confidentiality.

Patient privacy refers to the right of patients to determine when, how and to what extent their health information is shared with others. It involves maintaining confidentiality and sharing identifying data, known as protected health information (PHI), only with healthcare providers and related professionals who need it in order to care for the patient.

Patient information security includes the steps healthcare providers must take to guard this patients' "protected health information" commonly referred to as PHI, from unauthorized access or breaches of privacy or confidentiality. Security also refers to maintaining the integrity of electronic medical information, and ensuring availability to those who need access and are authorized to view such clinical data, including images, for the purposes of patient care. The federal government requires the secure handling of electronic media and PHI with standards put forth in the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

The secure management of electronic medical information may have an impact on the quality of patient care, patient rights, and healthcare professionals and their current work practices and legal responsibilities (radiologyinfo.org). Doctors can make the best decisions about medical care if they have access to all relevant information in their patients' medical histories (ncbi.nlm.nih.gov). Inability to access data may delay clinical management decisions and could adversely impact patient care (Sittig and Singh, 2011). Electronic medical records (EMR) incorporate the following components within their system security policies and procedures authorization, authentication, availability, confidentiality, data integrity and nonrepudiation. The methods available for authorization or access controls include single sign-on databases or lists assigning rights and privileges of users to access certain resources, automatic account logoff after a specified period of inactivity to prevent access by invalid users, and physical access controls.

Therefore a Prototype for a Secure Medical Laboratory Management System that has the above components was developed during this project. Mbarara Diagnostic center was used as the case study.

1.1 Background of Study

The World Health Organization's declaration of Health for All by the Year 2000 highlighted the need for better healthcare services, not only at the hospital (secondary) level, but also for primary healthcare and community health services like Mbarara Diagnostic Center. This has required a change of focus in healthcare in many areas to ensure, if possible, that the implementation of an electronic health record covers healthcare delivery services across a broad spectrum of healthcare. The USA, UK, Australia and some European countries have adopted this concept. This is achieved by promoting the development of a longitudinal electronic health record. These are aimed at improving the delivery of healthcare and ensuring that care given to an individual by various healthcare practitioners from many different settings in their lifetime is maintained in a single record and readily available. This is considered by many to be the ideal situation. This type of system would require a computer program that captures data at the time and place where healthcare is provided, whether at a hospital or primary care level over an extended period of time. It would enable healthcare information, such as a person's allergies, recent test results or prescribing history to be readily available at all times to assist with decisions on diagnoses, treatment and medication at all levels of healthcare (WHO, 2006).

This makes data protection and security critical components of routine pathology practice because laboratories are legally required to securely store and transmit electronic patient data (Storbrauck, 2015). The convenience of data access and distribution enables health providers to access and share data in order to promote quality care; however it poses a great threat to the patients' privacy if it is not controlled (Li et al, 2005).

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) govern the privacy and protection of medical information and health records. The HIPAA security standards final rule mandate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of ePHI. Importantly, security failures often lead to privacy breaches, invoking the HIPAA privacy rule as well.

In South Africa Health professional council of South Africa (HPCSA) governs medical practices. It defines the medical records, how they should be kept and retrieved for use in medical scenarios. This body requires that medical professionals should seek authorizations from clients if they are to use their data for research. All forms of tests that is visual, audio and any other test notes should be taken recorded with details like date and time plus the location. HPCSA makes record keeping mandatory in all health practitioners in South Africa. It requires all the medical labs and operators be registered and issued certificates that authorize them to operate. It also stops health practitioner from altering records in case of changes to records date, time and person doing changes be registered, signature captured in the system and also the reason for an amendment or error should also be specified on the record. Health records should be stored in a safe place and if they are in electronic format, safeguarded by passwords. Practitioners should satisfy themselves that they understand the HPCSA's guidelines with regard to the retention of patient records on computer compact discs. Health records should be stored for a period of not less than six (6) years as from the date they became dormant. In the case of minors and those patients who are mentally incompetent, health care practitioners should keep the records for a longer period for minors under age of 18 their records should be kept until they are 21 then for mentally incompetent patients the records should be kept for the duration of the patient's lifetime (HPCSA Pretoria may 2008).

In Kenya, the Kenya Medical Lab Technicians and Technologists Board (KMLTTB) core of Standards (KeBS) sets the Electronic Medical Record System (EMR) standards that are aligned with International Standards Organization (ISO) and Health Level Seven (**HL7**) standards. The responsibility of implementing these standards rests on hand of various shareholders.

In Uganda, the health care system is decentralized into districts with Hospitals and Health Centers (HC) where increasing levels of health care complexity are offered at each level (II, III, and IV). Laboratory services are offered at HC III and HC IV and are commensurate with the complexity of medical services accessible at each level. There are also more comprehensive medical laboratory services offered at Regional and National Referral Hospitals. Management, coordination and supervisory roles and responsibilities of the different levels are not clearly defined. Activities related to disease surveillance and investigation of outbreaks fall under the department of National Disease Control (NDC), while all clinical laboratories within facilities fall under the department for Clinical services. Central Public Health Laboratories (CPHL) falls under the NDC, but by virtue of its activities carries out work related to both departments in the Ministry (MOH, 2009). The registration of private medical laboratories is a regulatory requirement pursuant to the authority conferred upon Allied health professional council (AHPC) under section 29 of the Act. This Act is intended to provide Ugandans with quality health laboratory services by guaranteeing accurate and reliable diagnosis, which is a cornerstone of disease management and prevention.

It is because of this that the MOH (2008) emphasizes that Laboratory Systems require setting access controls to the users and auditing trails to check faults in the system. Furthermore, records stored on external devices need to be encrypted for confidentiality. Also, lab systems need to time out on users login sessions (MOH 2008).

This is because the protection of computer equipment, data, information, and computer services from unintended or unauthorized access, unplanned events, and even physical destruction is vital for any individual or organization that uses computers. Therefore Data protection and security are critical components of daily pathology practice that impact the entire information technology (IT) infrastructure including individual workstations, servers, and networks. With increasing connectivity of information systems, laboratory work-stations, and instruments themselves to the Internet, the demand to continuously protect and secure laboratory information can become a daunting task (Mitamura et al, 2005) This has led to increasing threats to the privacy of patients' health records (Fisher and Madge, 1996). This research addresses informatics security issues in the pathology laboratory related to passwords, data encryption, Internet security and emergency security situations. It also addresses the potential impact that newer technologies such as mobile devices have on the privacy and security of electronic protected health information (ePHI).

This is because making sure that the data contained in laboratory software remain protected and secure at all times is critical for daily pathology practice. Accordingly, security policies and procedures have to be in place and enforced in the laboratory. Major security elements that should be addressed include prevention of unauthorized access to patient's medical records (confidentiality), prevention of unauthorized alterations or loss to data (integrity), and prevention of compromises to availability of data to authorized individuals. Hence, incomplete or unavailable data is not considered secure. In order to develop an effective security program, security measures must be designed to allow authorized end-users access to information in a timely manner.

1.2 Problem statement

Despite the high level of patient desire to protect their records, health systems in Uganda do not adequately protect patients' records. For example, a study conducted at Mengo hospital and Mbarara university referral hospital reveals that all the clinical employees including doctors, nurses, receptionists and technicians have access to all the health records for all the patients in the EHR system.

Furthermore, these EHR systems are expensive for private sector clinics since they are only available in government hospitals that are funded by western governments, USAID/UKAID. They also require expensive hardware to operate which makes it hard to implement in the private sector in an economy like Uganda (developing countries) with low income (Kamadjeu, et al, 2005; Omary et al., 2009; Kalogriopoulos et al., 2009).

In this project, the researcher presents a cheaper alternative that supports major clinical tasks, solving security issues that have been previously sighted with in the available systems. The new designed system will avail its users with easy access to clinical records and applications but most importantly will also guarantee security of clinical data. This will be made possible by encrypting sensitive clinical records and setting up of user roles, rights and session logout when system is idol. With encrypted records even if the hardware is stolen one cannot access the records without the decryption key. The system also does not require a lot of processing power it can run on computers with low specifications.

1.3. Main Objective

The main objective of this project was to ensure security of patient's lab records by developing a secure laboratoray management system that is a cheaper alternative for a resource constrained environments

1.3.1 Specific Objectives

i) To analyze the current system and review literature related to the system to be developed.

ii) To design an architecture that supports encryption of health care records which is cheaper and affordable for use in resource constrained settings

iii) To develop the system so as to transform the design into a working system

iv) To test and validate the system so as to ensure that it functions properly and satisfies the user requirements.

1.3 Scope

The project was aimed at the development of a secure laboratory management system for Mbarara Diagnostic center with in estimated period of 1 year. The system should collect, store, keep track of clients and disseminate the records in form of reports to only authorized parties. Mbarara diagnostic lab is a privately owned lab and has been used as the case study

1.5.1Geographical Scope

The study was carried out at Mbarara diagnostic center and the reason for this was because of easy accessibility and increasing popularity of the lab as the leading privately owned lab in the region and its high level of cliental.

1.5.2 Time Scope

Time is the most important and most scarce resource at our disposal. As such, this study was carried out within a period of 1 year. Within this period, relevant documents and data were collected and analyzed to finally develop the system.

1.5.3 Technical Scope

This study analyzed the current Information Technology infrastructure that is being used in the lab management and the focus was on security of the system and the smooth running of the operations.

1.5.4 Functional Scope

This study was confined to the study and development of lab management system. The System focuses on securing lab client information and its dissemination. Its also provides books of accounts and keeps track of lab supplies and their expiry dates

1.6 Significance

The main significance of the project is that it will meet the major goal of access control within MDLC systems that is to provide systems access control by ensuring that only authorized users have access to patient's information (Tuyikeze, 2005; Smith etal. 2010). The National Institute of Standards and Technology (NIST), it provides four criteria on how EHR systems should function and all these criteria will be met by the proposed system in the following ways:-

The first criteria require that users be given a unique name and/or identification number for tracking and as one of the user requirements of the system is that each user will be given a unique user name and password in order to be able to use the proposed system. The second criteria requires administrative facilities to assign privileges to users and groups and the third criteria requires that EHR systems must implement either one of user-based access control (UBAC), context-based access control (CBAC) or role-based access control (RBAC). The proposed system through the system administrator users will be granted rights based RBAC and their rights / permissions can be removed without having to delete them thus meeting the NIST standards.

Encryption of medical records for sharing plays a major role in safeguarding files against unauthorized access. On May 26, 2002, AES replaced the DES as the algorithm of choice for the government. AES is described by the standard known as FIPS-197. This new standard specifies Rijndael as a FIPS-approved symmetric encryption algorithm that may be used to protect sensitive information (healthit.gov). Therefore the proposed system will be able to encrypt data/file using AES standard that is recommended by FIPS-197 as an efficient security standard and with this system records will be shared and accessed by only authorized parties with the decryption key and also preventing modification attacks.

The proposed system will replace paper-based medical records, which can be incomplete, fragmented (different parts in different locations), hard to read and (at times) hard to find. Provide a single, shareable, up to date, accurate, rapidly retrievable source of information, potentially available anywhere at any time. Require less space and administrative resources (Abraham, Joanna and Madhu C. Reddy 2010.).

Also provide Easy accessibility to medical records with in the different departments of the case study at a given time is also beneficial (Mosby; 2004). This improved access will lead to better communication between care providers and save time that is wasted during the process of search through paper files for a record and improving quality of the service delivery.

The developed system will help to maintain data and information trail that can be readily analysed for medical audit, research and quality assurance, epidemiological monitoring, and disease surveillance (Abumelha, Manal, et al. 2016).

.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter offers a critical review of prior studies relevant to Electronic Health Records (EHRs). Firstly, the chapter provides an overview of EHRS, followed by EHRS systems and lastly security models, which are the main research areas the thesis contributes. The related work on EHRs is described under three general themes, namely: PHR systems models, legal and system standards, and security models with the goal of identifying and re-applying a security model that fits within the constraints of Uganda. Other subsections of this chapter identify key research gaps and explore the design EHR technologies for patients. Based on the results, the chapter sets out a research agenda for the dissertation, and justifies the selection of the security model that we used in our EHR system

2.1 Definitions

i) **A digital signature** is an electronic rather than a written signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged.

ii) Electronic Data Interchange (**EDI**) is the inter-organizational, computer-to-computer exchange of structured information in a standard, machine process able format.

iii) Health Level Seven (**HL7**) is a specification for a health data-interchange standard designed to facilitate the transfer of health data resident on different and disparate computer systems in a health care setting. HL7 facilitates the transfer of laboratory results, pharmacy data and other information between different computer systems.

iv) **A Key is a** variable value created using a mathematical formula. Public keys are obtained from the certificate authority, while private keys are contained within each user’s computer system.

v) **Private Key** is a mathematically derived code provided by a certificate authority. The private key is stored in the user’s computer and is not accessible to the public. It can be combined with the public key to encrypt and decrypt messages.

vi) **Public key** is a mathematically derived code provided by a certificate authority. The public key is stored in the digital certificate and can be combined with the private key to encrypt and decrypt messages.

vii) **Public key infrastructure (PKI)** software application that allows users to encrypt and send Information securely over a public network.

viii) **Encryption** The process of converting data into a form or code that cannot be understood by unauthorized persons.

ix) Electronic Health Record (**eHR)** these are stored health information

2.2 Over view on major goals of information systems and data exchange

An important requirement of any information management system is to protect data and resources against unauthorized disclosure (secrecy) and unauthorized or improper modifications (integrity), while at the same time ensuring their availability to legitimate users (no denials-of-service). Enforcing protection therefore requires that every access to a system and its resources be controlled and that only authorized accesses can take place. This process goes under the name of access control. The development of an access control system requires the definition of the regulations according to which access is to be controlled and their implementation as functions executable by a computer system. The researcher explores the idea of security control for electronic health records in resource-constrained environments through literature review. There are two doctrines for developing electronic health records:

i) Data stored should be exchanged according to public standards

ii) And then records access controls (Mandl et al, 2001).

The researcher reviews literature on the international health systems standards, access control approaches and their requirements. The researcher also reviews security policies.

2.2.1 International Health System Standards

In this section, the researcher reviews literature on the US Health Insurance Portability and Accountability Act of 1996, Health Level 7 and the European Directive 95/46/EC on protection of personal data.

According to Oppliger (1996), international standards can be defined as documented agreements containing precise criteria that must be followed consistently as rules, guidelines or definitions of characteristics to ensure that any products, materials, processes or services are fit for their purpose. The acceptance and adoption of these standards is recognized by very many states and governments in Europe, Asia, Canada and some African countries (Tuyikeze, 2005; Tuyikeze & Pottas, 2005).

2.2.2 HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), was released in the US in 1996 with a compliance date of April 14, 2003 to help improve health care delivery by streamlining health insurance coverage. HIPAA sets standards for privacy of individually identifiable health records (Kulynych and Korn, 2003). It regulates health providers such as hospitals on the permissible use and disclosure of identifiable health records (Kulynych and Korn, 2003). It specifies that without written patient authorization of a highly prescriptive and purpose specific form, the health providers may only make certain use of identifiable health records and may only disclose it to third parties for sanctioned purposes that are minimum necessary to accomplish treatment (Kulynych and Korn, 2003). This act regulates both electronic and paper records. HIPAA requires that patients be provided a privacy notice to educate them about their rights. This should indicate who will be able to see and use their medical records, what use will require the patient's specific authorization and their right to inspect, copy and change their medical records (Annas, 2003). The providers are required to provide an accounting of all disclosures. The authorization to release patient's information must contain at least the description of the information to be released, the name of the person or entity authorized to release this information, a description of each of the purpose of the requested use or disclosure, an expiration date and the signature of the individual and date (Annas, 2003). HIPAA states that providers should not use consent as a condition for treatment and that the health system should have an emergency access procedure.

In Conclusion, HIPAA emphasizes that patients have a right to have their personal medical records kept private and that the providers should be accountable for all the disclosures. Patient centered access control has been proposed as an ideal solution to managing access to their own electronic health information to meet HIPAA standard requirements.

2.2.3 HL7

Health Level 7, (HL7) Organization was founded by a group of health care computer system users who started developing the HL7 protocol that allows sharing clinical data with each other and has since then become the global standard (HL7 Standard). The mission of HL7 is: “To provide global standards for the exchange, management and integration of data that supports clinical patient care and the management of delivery and evaluation of health care services. Specifically to create flexible, cost effective approaches, standards, guidelines, methodologies and enable health care information. Originally developed in 1987, HL7 is now in use in more than twenty countries around the world. HL7 contains messages for almost every conceivable healthcare application area, including the following:

- Registration
- Orders (clinical and other)
- Results and observations
- Queries
- Finances
- Laboratory automation
- Document control
- Scheduling and logistics
- Personnel administration
- Patient care planning
- Network synchronization
- Master files and indexes

2.2.2.1 what does an HL7 interface do?

An HL7 interface bridges the gaps between your facilities patient registration system, transcription solution and EMR/EHR by using a standard messaging protocol. Because hospitals and other healthcare providers usually have different systems for different aspects of services, they are often unable to communicate with each other. HL7 alleviates that problem by providing the framework for the exchange, integration, sharing and retrieval of electronic health information. HL7 interfaces provide an encrypted and secure means of transferring files. The HL7 is "Level Seven" because its message formats are layered upon the seventh level of the Open Systems Interconnection (OSI) protocol of the International Standards Organization (ISO). Unlike other standards, HL7 specifies almost no restrictions whatsoever on the protocols to be used in the lower layers of the interface. The definitions in HL7 concentrate on the logical arrangement of data and what is meant by information in various parts of the message.

2.2.3.1 what are the benefits of an HL7 interface?

Costs for healthcare facilities to interface are reduced because HL7 is the worldwide health interface standard and all service and solution providers should be knowledgeable and able to integrate. By using a HL7 interface engine, health providers can realize the benefits of existing information systems without major reinvestment in new technologies, lowering costs and extending the life and efficiencies of current systems. There is also opportunity to link to systems outside the healthcare provider such as providers of outsourced services like radiology and transcription.

The HL7 interface also improves workflow by allowing medical professionals to focus on their core business activities and provide quality healthcare. Instead of having to write specifications from scratch each time data needs to be sent between two systems, we can make reference to a uniform document whose definitions assist in providing a common understanding to both systems. Below is a table showing a summary of some selected international health standard as given by ISO (2015).

2.2.4 Health Information Privacy Regulations

In the last four decades healthcare industry has undergo tremendous changes driven by advances in technology and legislation such as the 1973 Health Maintenance Organizations Act. As personal health information is digitized, transmitted and mined for effective care provision, new forms of threat to patients' privacy are becoming evident. In view of these emerging threats and the overarching goal of providing cost effective healthcare services to all citizens, several important federal regulations have been enacted including the Privacy and Security Rules under HIPAA (1996) and State Alliance for eHealth (2007). The technology component involved in managing health information and necessity of disclosure to third parties has led to stipulations of privacy compliance and provision of security safeguards under HIPAA (Mercuri 2004). The Privacy Rule of HIPAA addresses the use and disclosure of a patient's protected health information by healthcare plans, medical providers, and clearinghouses, also referred as covered entities. By virtue of their contact with patients, covered entities are the primary agents of capturing a patient's health information for a variety of purposes including treatment, payment, managing healthcare operations, medical research, and subcontracting (Choi et al. 2006). The Security Rule of HIPAA requires covered entities to ensure implementation of administrative safeguards in the form of policies and personnel, physical safeguards to information infrastructure, and technical safeguards to monitor and control intra and inter organizational information access (ibid.)

Apart from HIPAA, by 2007, nearly 60 Health IT related laws have been enacted in 34 states, plus the District of Columbia (RTI 2007). Moreover, the US Congress has been considering various new legislation including ―Health Information Privacy and Security Act‖ (US Congress 2007a), National Health Information Technology and Privacy Advancement Act of 2007‖ (US Congress 2007b), and ―Technologies for Restoring Users' Security and Trust in Health Information Act of 2008‖ (US Congress 2008).

Therefore, this new legislation is intended to improve the privacy protection offered under previous regulations by creating incentives to de-identify health information for purposes necessary, establishing health information technology and privacy systems, bringing equity to healthcare provision, and increasing private enterprise participation in patient privacy

2.3 Threats to Information Privacy

Threats to patient privacy and information security could be categorized into two broad areas:

i) Organizational threats that arise from inappropriate access of patient data by either internal agents abusing their privileges or external agents exploiting vulnerability of information systems, and

ii) Systemic threats that arise from an agent in the information flow chain exploiting the disclosed data beyond its intended use (NRC 1997).

2.3.1 Organizational Threats

Organizational threats may assume different forms, such as an employee who accesses data without any legitimate need or an outside attacker (hacker) that infiltrates organization‘s information infrastructure to steal data or render it inoperable.

At the outset, these organizational threats could be characterized by four components – motives, resources, accessibility, and technical capability (1997). Depending on these components, different threats may pose different level of risk to organization requiring NRC different mitigation and prevention strategies. Motives could be both of economic or noneconomic nature. For some, such as insurers, employers, and journalists, patient records may have economic value, while others may have noneconomic motives such as a person involved in romantic relationship. These attackers may have resources ranging from modest financial backing and computing skills to a well-funded infrastructure to threaten a patient as well as the operations of a healthcare organization. The attackers may require different types of access to carry out their exploits, such as access to the site, system authorization, and data authorization. In addition, threats could depend on technical capability of attackers who may be novice or sophisticated programmers. Moreover, with the growing underground cyber economy (Knapp and Boulton 2006), an individual with the intent to acquire data and possessing adequate financial resources may be able to buy services of sophisticated hackers to breach healthcare data.

Organizational threats could be categorized into five levels, in the increasing order of sophistication (NRC 1997; Rindfleisch 1997):

i) Accidental disclosure: healthcare personnel unintentionally disclose patient information to others, example. Email message sent to wrong address or an information leak through peer-to-peer file sharing.

ii) Insider curiosity: an insider with data access privilege pries upon a patient‘s records out of curiosity or for their own purpose, example a nurse accessing information about a fellow employee to determine possibility of sexually transmitted disease in colleague; or medical personnel accessing potentially embarrassing health information about a celebrity and transmitting to media

iii) Data breach by insider: insiders who access patient information and transmit to outsiders for profit or taking revenge on patient

iv) Data breach by outsider with physical intrusion: an outsider who enters the physical facility either by coercion or forced entry and gains access to system

v) Unauthorized intrusion of network system: an outsider, including former vengeful employees, patients, or hackers who intrude into organization‘s network system from outside and gain access to patient information or render the system inoperable

2.3.2 Systemic Threats

Etzioni (1999), in discussing the Limits to Privacy‘, makes a strong case that a major threat to patient privacy occurs not from outside of the information flow chain in healthcare industry but from insiders who are legally privileged to access patient information. For example, insurance firms may deny life insurance to patients based on their medical conditions, or an employer having access to employees‘ medical records may deny promotion, or worse, terminate employment. Patients and payer organizations may incur financial losses as a result of malpractices including up coding of diagnoses, and rendering of medically unnecessary services. In summary, healthcare information systems could be subjected to security threats from one or more sources including imposter agents, unauthorized use of resources, unauthorized disclosure of information, unauthorized alteration of resources, and unauthorized denial of service (Win et al. 2006). Denial-of-service attacks via Internet worms or viruses, equipment malfunctions arising from file deletion or corrupted data, and the lack of contingency plans pertaining to offsite backup, data restoration procedures, and similar activities may also trigger HIPAA violations (Mercuri 2004).

2.4 Access Control Approaches

In this section we review approach especially the Role Based Access control model. Computer systems have multiply users, leading to heighten need for data security issues. System administrators and software developers' focus on different kind of access control to ensure only authorized users are given access the data resources of the system. One kind of access control that evolved was role based access control (RBAC) With role-based systems administrators create roles based job functions performed in the company. They are granted permission according to those roles. They then assign users roles basing on their specific job responsibilities and qualifications. Roles can represent specific tasks such as that of a physician or pharmacist, person may have the competency to manage several departments but can be assign a role to manage only one. Roles can reflect specific duty assignments rotated through multiple users. Role define both specific individuals allowed to access a resource and to what extent the resource is are accessed for example an operators role may be to access all the computer resources but not to change any permission granted and an auditors role might be only to access audit trails. Roles are used for systems administration for networked environment.

Particular combination of users and permissions brought together by roles tend to change over time. Permissions are associated with roles on the other hand more stable they tend to change less than the people who fill the positions that the roles represent therefore basing security on roles is rather than permission is simpler. Users can be easily reassigned new roles as needs of the company change. Similarly as a company acquires new applications and systems roles can have new permissions granted and existing revoked.

2.4.1 The NIST Model for Role Based Access Control (RBAC)

The National Institute of Standards and Technology (NIST) demonstrates that RBAC addresses many different needs for commercial and government sector as access control requirements were found to be determined by a needs of a costumers, stock holder and insurer's confidence; personal information privacy, prevention of an authorized financial asserts distribution and unauthorized long distance telephone call and adherence to professional standards. Study found out that in many organizations: -

i) Based on access control decisions the roles of an individual user take on parts of the organization

ii) Preferred to centrally control and maintain access control rights that reflect organizational protection guidelines

iii) Viewed their access control needs as unique, believing that commercially available products lacked adequate flexibility

The NIST model for role based access control (RBAC) is organized into four levels of increasing functional capabilities; flat RBAC, hierarchical RBAC, constrained RBAC and symmetric RBAC which are cumulative with each adding one new requirement (Sandhu et al, 2001). RBAC diverges from the user identity level to a role one where permissions are granted based on functional roles in the enterprise and not the individual; and users are assigned to these roles or a set of roles (Sandhu et al, 2001).

2.4.1.1 How RBAC works

RBAC has four elements: users, roles, permissions and sessions; NIST RBAC elaborates permissions by introducing operations and objects sub entities (Sandhu et al, 2001). The diagram below illustrates how these elements relate to each other. In flat RBAC, users are assigned to roles, permissions are assigned to roles so users inherit permissions from being members of these roles. This can be implemented in a many to many setup where a user can be a member of several roles or a role can have several users (Sandhu et al, 2001). The other levels have increasing functional capabilities from flat RBAC.

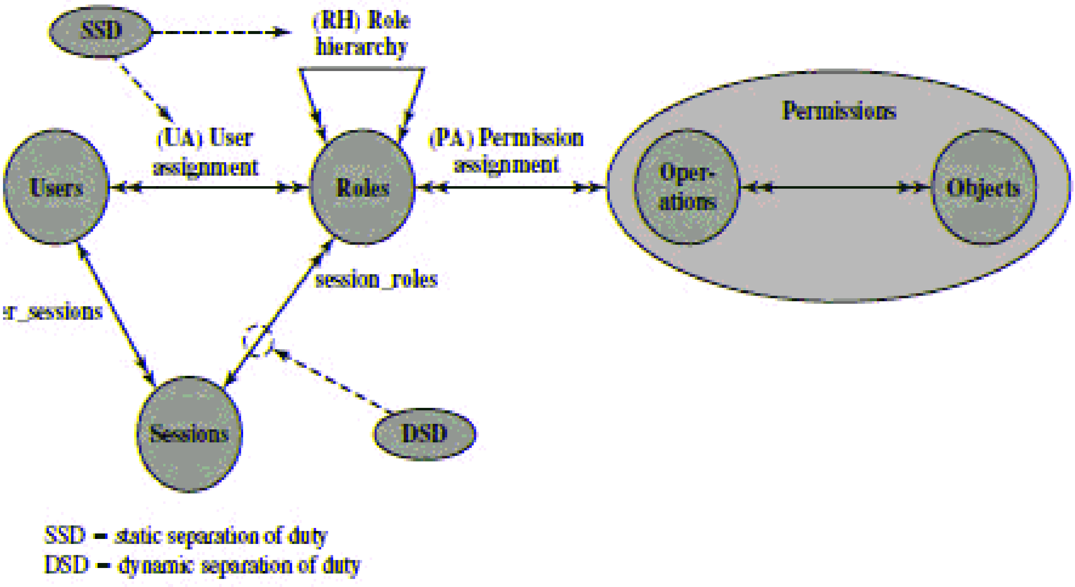


Figure 2.1: NIST RBAC (Sandhu et al, 2001)

Hierarchical RBAC requires role hierarchies such that a senior role acquires the permissions of its juniors (Sandhu et al, 2001). Constrained RBAC enforces separation of duties where responsibility and authority for an action is spread over multiple users to reduce the risk of committing a fraudulent act by requiring the involvement of more than one user (Sandhu et al, 2001). Symmetric RBAC requires permission role review such that the roles to which certain permissions are assigned can be determined as well as permissions assigned to a specific role (Sandhu et al, 2001).

2.4.1.2 Strength of RBAC

Roles are persistent in an organization compared to user turnover and can be hierarchical such that one role includes all permission of another role or overlapping, this makes implementation less complex when assigning permissions in a large enterprise (Sandhu et al, 2001).

2.4.1.3 Weakness of RBAC

RBAC has default rights for users based on their roles. This implies that a doctor for example inherits rights that the doctors' role is defined. This access approach by itself does not satisfy requirements for HIPAA.

2.4.2 Multilevel Security

Multilevel Security, MLS was developed by the Department of Defense in the US in the1970s to control confidentiality and information flow in information systems (Gasser, 1998). It maintains different levels of access to classified information on multi access resource sharing information systems (Gasser, 1998).

2.4.2 .1 How MLS works

MLS defines that every data has a classification and every user possesses a clearance. The security levels are unclassified, confidential, secret and top secret which are hierarchical. Multi-level security leverages on Bell La Padula security model (Bell and La Padula, 1974) properties that state:

i) Simple Security Property:

A subject can read from an object as long as the subject's security level is the same as, or higher than, the object's security level. This is known as the no read up property.

ii) *-Property:

A subject can write to an object as long as the subject's security level is the same as or lower than the object's security level. This is known as the no write down property(Bell and La Padula, 1974)

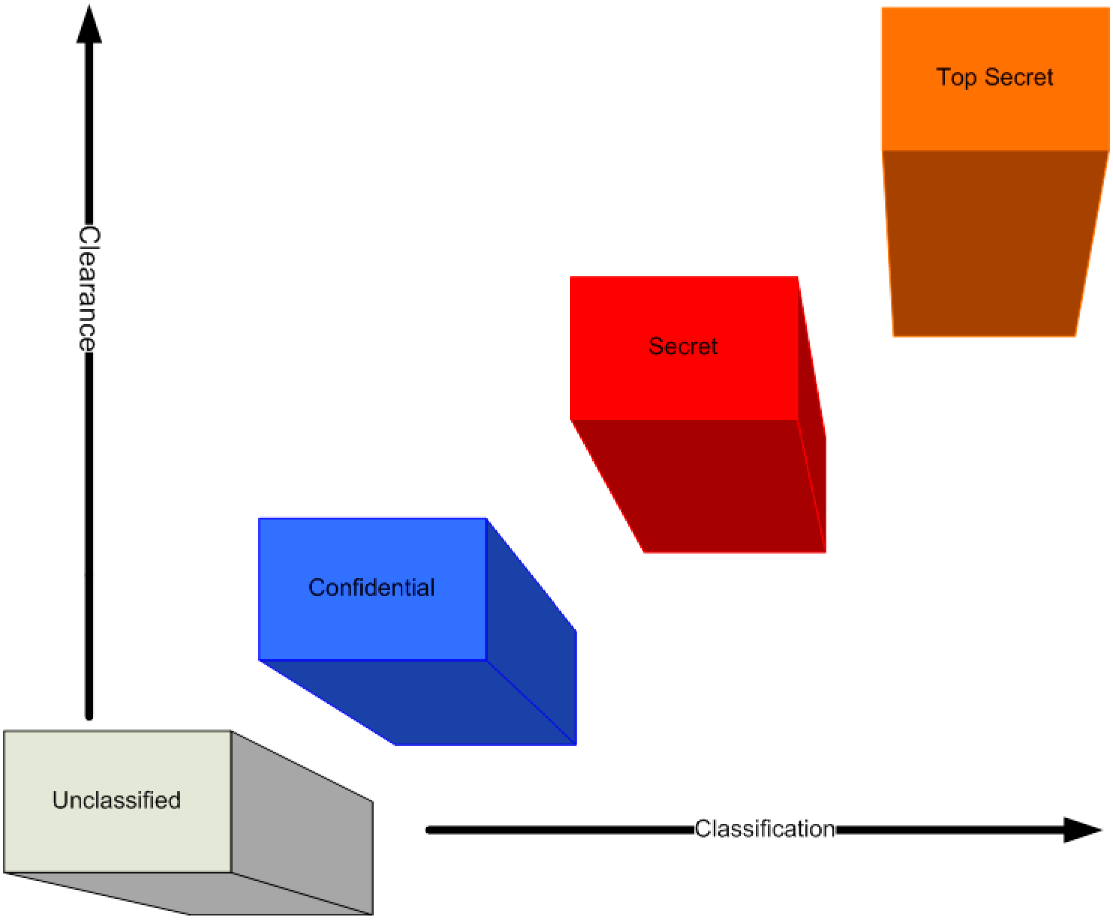


Figure 2.2: MLS Security Levels

The MLS classification and clearance is made up of two components; a security level and a compartment. The security levels are similar to Bell La Padula's unclassified, confidential, secret and top secret levels above while the compartment is defined explicitly and can be a project such as Project A or Cuba (Gasser, 1998). The object's classification contains the security level and the compartments (security-level, explicit-compartment) for example (Secret, Nigeria, Project D, CDC). In this example a user with clearance Secret without all the three compartments will not be able to read a file with this classification. This implements a need to know access control mechanism.

2.4.2 .2 Strength of MLS

Based on the Bell La Padula model, MLS permits users or processes to read only information classified at only or below their clearance. It prevents them from reading information whose classification exceeds their clearance (No read up). MLS also prevents users or processes from passing highly classified information to users or processes that do not possess this clearance whether intentionally or not (No write down), (Gasser, 1998). Use of compartments implements a “need to know” basis of information flow.

2.4.2.3 Weakness of MLS

The fact that MLS is based on classification of information and clearance of the users prior to authorization limits its use in situations where the information sharing parties do not have prior knowledge of each other.

2.4.2.4 RBAC Verses MLS

RBAC defines roles with rights and users are assigned to roles so that users have default rights by being members of certain roles. MLS requires that a user has a given clearance and an explicit compartment. Therefore RBAC does not implement explicit authorization while MLS does using compartments.

2.4.3 Discretionary Access Control (DAC)

DAC was developed to implement Access Control Matrices defined by Lampson in his paper on system protection. In the DAC module the patient will specify who can access his eHR. He will populate an Access Control List (ACL) with the healthcare practitioners who he prefers to be able to access his eHR. The patient also has the capability to specify the access level of each of the users in terms of a sensitivity label in the ACL, which is done using the MAC. The matrices are in three-dimensional, rows are the subjects and columns are the objects. The mapping of the pairing of objects and subjects results into set of rights that subjects have over objects. DAC allows subject discretion to decide access rights on the objects they own. Because Access Control Matrices have one row for every subject and one column for every object, the number of entries is intuitively the number of subjects times the number of objects. This means that O (n) growth in subjects and objects results in O (n^2) growth in the size of the matrix. The size of the access control matrix would not be a concern if the matrix were dense, however, most subjects have no access rights on most objects so, in practice, the matrix is very sparse.

If access control information was maintained in this matrix form, large quantities of space would be wasted and lookups would be very expensive. Thus, DAC access settings are typically stored as either per-object file permission modes (default on UNIX) or as lists.

2.4.3.1 Strength of DAC

A primary benefit associated with the use of DAC is enabling fine-grained control over system objects. Through the use offline-grained controls, DAC can easily be used to implement least-privilege access. Individual objects can have access control restrictions to limit individual subject access to the minimum rights needed. DAC is also intuitive in implementation and is mostly invisible to users so it is regarded as the most cost-effective for home and small-business users. [S. Smalley]

2.4.3.2 Limitations of DAC

DAC has its own limitations Allowing users to control object access permissions has a side-effect of opening the system up to Trojan horse susceptibility. Maintenance of the system and verification of security principals is extremely difficulty or DAC systems because users control access rights to owned objects. This result into a Safety Problem, the lack of constraints on copy privileges, is another liability inherent to DAC. The lack of constraints on copying information from one file to another makes it difficult to maintain safety policies and verify that safety policies have are not compromised while opening potential exploits for Trojan horses.

2.4.4 PKI-based Access Control

Public Key Infrastructure based access control is a security framework that uses the concept of a trusted third party to ensure confidentiality, integrity, non-repudiation and accountability during information sharing (Bourka et al, 2003). PKI controls the issuing and management of digital certificates that are used in combination with encryption to achieve this. The goal of access control within E-health systems is to provide systems access control by ensuring that only authorized users have access to patient’s information (Tuyikeze, 2005; Smith etal., 2010).

2.4.4.1 How PKI works

Public Key Infrastructure is based on asymmetric cryptography where a pair of keys; public and private keys are used. What one key encrypts, only the other key can decrypt. The public key is published to the public while a user keeps the private key secret. A sender uses the receiver’s public key to encrypt data that can only be decrypted by using the receiver’s private key. This provides for data confidentiality.

A sender can use his private key to perform a one-way hash function on the message and attach the value to the message, this is known as a digital signature. He then uses the receiver's public key to encrypt the message and send it together with the has value. The receiver uses his private key to decrypt the message, performs a hash function on the message using the sender's public key and if the value is the same as the attached value then the sender is who he claims to be. This provides for authentication, confidentiality, integrity, on repudiation and accountability.

Asymmetric cryptography is very resource intensive due to number encryption iterations and is often used in combination with symmetric cryptography such that when authentication is complete, then the two parties can share a secret key that is used for the lesser resource intensive symmetric encryption. To prevent a masquerader from posting a public key to which he knows the corresponding private key, a trusted third party signs the public keys and appends the owner's name such that the sender can verify that receiver's public key before engaging with a masquerader. This is known as a digital certificate and the trusted third party is known as a certificate authority. A digital certificate also contains the expiration date and the name of the certificate authority (Mavridis et al, 2001).

2.4.4.2 Strength of PKI

PKI-based access control is effective at authenticating users from different security domains using a trusted third party such as a certificate authority. The same concept provides for information confidentiality, integrity, non-repudiation and accountability. PKI-based access control can even be used in environments where the parties do not have any prior knowledge of each other.

2.4.4.3 Weakness of PKI

Public Key Infrastructure operations are very resource intensive and pose a challenge in resource limited environments.

2.4.5 Digital Signatures

The move from paper medical records to digital versions has helped improve data sharing, convenience and efficiency in the healthcare industry yet signatures are still required from patients to give their authorization to share or use their Protected Health Information (PHI). Under the Privacy Rule, patients are allowed access to their healthcare data on request (reviewed by Pritts, 2008). The Omnibus Rule, which placed a restriction on the use of PHI for marketing purposes, requires patients to sign a document to confirm that they agree to receive marketing communications. Obtaining written consent from patients is essential under the Health Insurance Portability and Accountability Act (HIPAA). Covered Entities (CEs) must be able to produce consent forms in the case of a compliance audit or a legal dispute. A signed document will confirm that patient consent has been obtained. However in a digital age, pen and ink signatures should not be necessary.

A Digital signature is a method of signing an electronic document that identifies and authenticates a particular person as the source of the electronic document and indicates that person's approval of (and accountability for) the information contained in the electronic document (May 3, 2015, HIPAA Journal). A number of technical solutions for the use of digital signatures have been identified and evaluated, with PKI being the Australian Government preferred solution. PKI is a trusted framework adopted by Australian Government to provide authentication and confidentiality for online transactions through the use of digital keys and certificates. For the healthcare sector, PKI enables the transfer of sensitive medical information across the Internet, without compromising the individual's right to privacy.

PKI digital certificates may be issued to an organization ('location certificates') or to an individual ('Individual Certificates'). Location certificates allow a number of people at the same location to sign, encrypt and exchange messages electronically with other certificate subscribers. The location certificate provides confidentiality, authentication, and integrity of the information that is transmitted. Signing a message using the location certificate confirms the location that the message came from, but not from which individual. Individual certificates are specific to an individual and are used to sign, encrypt and exchange messages electronically with other certificate subscribers. Individual certificates provide authentication, confidentiality, integrity and non-repudiation. Ideally, the electronic exchange of information should utilize individual certificates for signing because:

i) A valid document must unambiguously identify the implementer as the signer of the document; and

ii) A document may contain personal and potentially sensitive information. However the anecdotal evidence suggests that, in practice the implementation of individual certificates over location certificates has been problematic. Therefore, the implementation of digital signatures using PKI requires careful consideration of the practical issues surrounding the use of individual and location certificates in the Healthcare sector. One possibility might be that PKI location certificates are used in combination with another method of authentication, e.g. username and password, underpinned by legal or policy frameworks.

A digital signature has the same legal holding as your hand written signature. This was introduced in the Commonwealth Electronic Transactions Act in 1999.

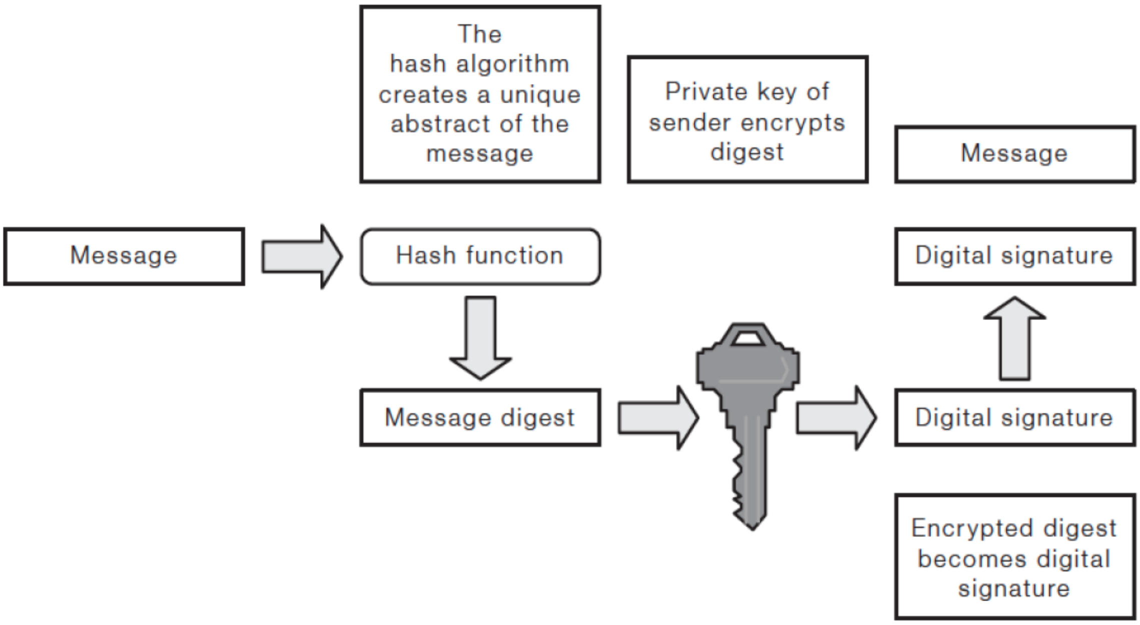

The hash algorithm creates a unique abstract of the message
Private key of sender encrypts digest
Message
Message
Hash function
Digital signature
Message digest
Digital signature
Encrypted digest becomes digital signature

Figure 2.3: Overview of a Digital Signature Process

2.4.5.1 Strength of Digital Signatures

i) Digital signature is embedded and cannot be lost

ii) Message remains compliant

iii) Usual message transformations remain possible

iv) Can add copy doctors and new MSH ID

v) Signature can be stripped off if desired

vi) Message can be archived

vii) Any PKI could be used

viii) Digital signature can be re-evaluated at any time

ix) Can transform to XML if desired

2.4.6 Attribute Based Access Control, (ABAC)

Similar to the above approach, the attribute based access control uses attribute certificates only that these certificates do not contain a public key (Mavridis et al, 2001). An attribute certificate contains the account holder's specific attributes similar to policies that specify his or her access control information such as role, security clearance or group membership (Mavridis et al, 2001). It can be used for part of the authorization processes that is not identity based such as in the military where access is based on rank. Attribute certificates also need to be signed by a trusted third party known as attribute authority (Mavridis et al, 2001) that is responsible for their issuing and entire lifetime up to revocation.

2.4.6.1 Strength of ABAC

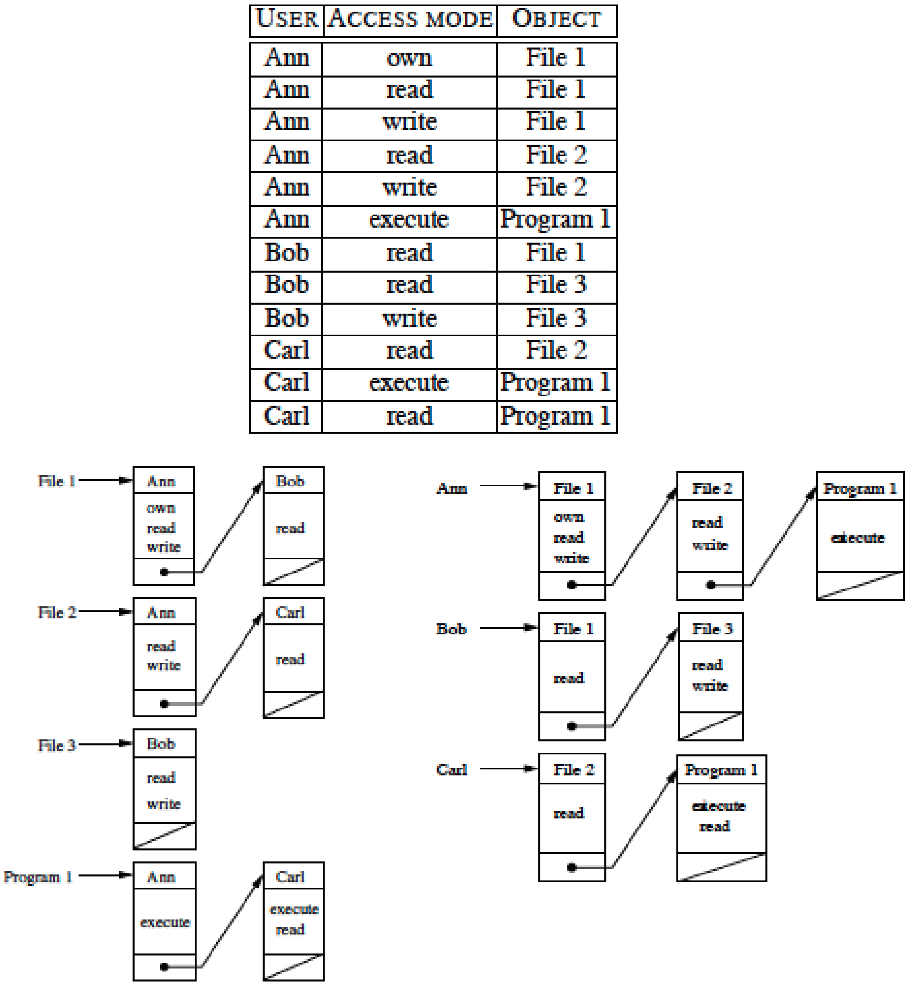
ABAC is effective at authorization of users from different security domains using a trusted third party even in environments where the parties do not have any prior knowledge of each other.

2.4.6.2 Weakness of ABAC

ABAC does not use public keys and therefore does not cater for security during transmission.

2.4.7 Access control lists (ACLs)

ACLS is a representation of objects rights as a table of subjects is mapped to their individual rights over objects. Access control models assume that the users are authorized to access the information system. After authorization, the access control mechanism will define what information each authorized user can access (Malin and Airoldi, 2007). ACLs are the default representation of access rights on UNIX systems and essentially correspond to individual columns in the system Access Control Matrix. ACLs are effective but not time-efficient with a low number of subjects. Typically, the operating system knows who the user of a process is but doesn't know what rights the user has over objects on the system. ACLs require the operating system to either perform a rights lookup on each object access or somehow maintain the subjects active access rights. Because of this rights management issue, and the difficulty in performing multi-object rights modifications for individual users, ACLs don't scale well on systems with large numbers of subjects or objects.



USER	ACCESS MODE	OBJECT
Ann	own	File 1
Ann	read	File 1
Ann	write	File 1
Ann	read	File 2
Ann	write	File 2
Ann	execute	Program 1
Bob	read	File 1
Bob	read	File 3
Bob	write	File 3
Carl	read	File 2
Carl	execute	Program 1
Carl	read	Program 1

Figure 2.4: Authorization table, ACLs, and capabilities

2.4.7.1 Strength of ACLs

For ACLs is sufficient for a subject to present the appropriate capability to gain access to an object. It presents an advantage to distributed systems since it permits to avoid repeat authentication to the subject

The advantage of this is that ACLs can be efficiently represented as small bit-vectors. For instance, in the popular Unix operating system, each user in the system belongs to exactly one group and each file has an owner (generally the user who created it), and is associated with a group (usually the group of its owner).

2.4.7.2 Weakness of ACLs

With ACLs it is immediate to check the authorizations holding on an object, while retrieving all the authorizations of a subject requires the examination of the ACLs for all the objects. Analogously, with capabilities, it is immediate to determine the privileges of a subject, while retrieving the entire accesses executable on an object requires the examination of all the different capabilities. These aspects affect the efficiency of authorization revocation upon deletion of either subjects or objects

2.4.8 Surrogate Trust Negotiation, (STN)

Trust negotiation allows two parties that are previously unknown to each other outside a local security domain to transact securely through a handshake like process of requesting and providing digital credentials and policies (Vawdrey et al, 2003). These digital credentials are digitally signed by a trusted issuer and are used to verify the owner's attributes (Vawdrey et al, 2003). PKI-based and Attribute based access control approaches are examples of trust negotiation.

2.4.8.1 How STN works

Surrogate Trust Negotiation (Vawdrey et al, 2003) brings the concept of trust negotiation based authentication and authorization to mobile devices. Mobile devices usually operate outside a single security domain (Vawdrey et al, 2003) and trust negotiation is appropriate for their transactions. STN provides a mechanism that effectively combines the capabilities of network proxies, software agents and modern cryptographic systems to extend trust negotiation to mobile environments. In this protocol, the resource intensive task of public key cryptography is off loaded to trust agents. "Trust agents are autonomous software modules on secure, offsite computers that act as surrogates for mobile devices, performing cryptographic operations and managing credentials, policies, secret keys for use in trust negotiation.” (Vawdrey et al, 2003) STN allows resource limited devices to participate in trust negotiation using trust agents.

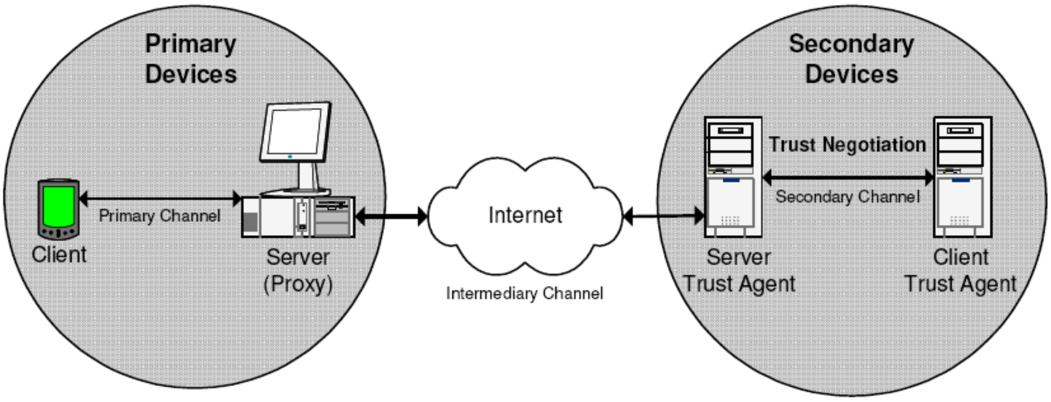


Figure 2.5: Surrogate Trust Negotiation (Sundelin, 2003)

2.4.8.2 Strengths of STN

Mobile technologies such as GSM are widespread and available even in resource-limited settings. A mechanism that can achieve health systems standards using mobile technologies would be ideal for resource limited settings.

2.5 Cryptograph

Cryptography involves the study and practice of hiding information through the use of keys, which are associated with Web-based applications, ATMs, Ecommerce, computer passwords, and the many more. Encryption is the process of converting normal text to unreadable form. Decryption is the process of converting encrypted text to normal text in the readable form.

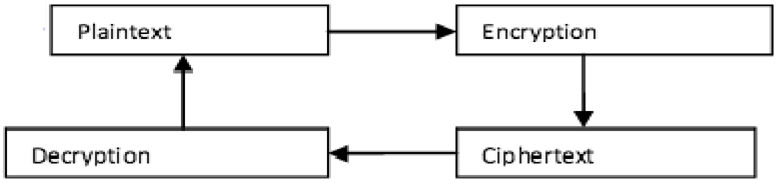


Figure 2.6: Conventional Encryption Model

There is a prevailing myth that secrecy is good for security, and since cryptography is based on secrets, it may not be good for security in a practical sense (Schneier, 2004; Baker, 2005). The mathematics involved in good cryptography is very complex and often difficult to understand, but many software applications tend to hide the details from the user thus making cryptography a useful tool in providing network and data security (Robinson, 2008). Strong public-key cryptography is computationally expensive for small devices, and the alternative may be to incorporate cryptographic hardware into embedded designs (Robinson, 2008).

Cryptograph is a branch of computer science and mathematics and its in two forms symmetric and asymmetric. Symmetric cryptosystems involve the use of single key know as secret key to encrypt and decrypt data messages while as asymmetric cryptosystem use one key (public key) to encrypt messages and second key (secret key) to decrypt messages. Asymmetric cryptosystems can all be know as public key cryptosystems

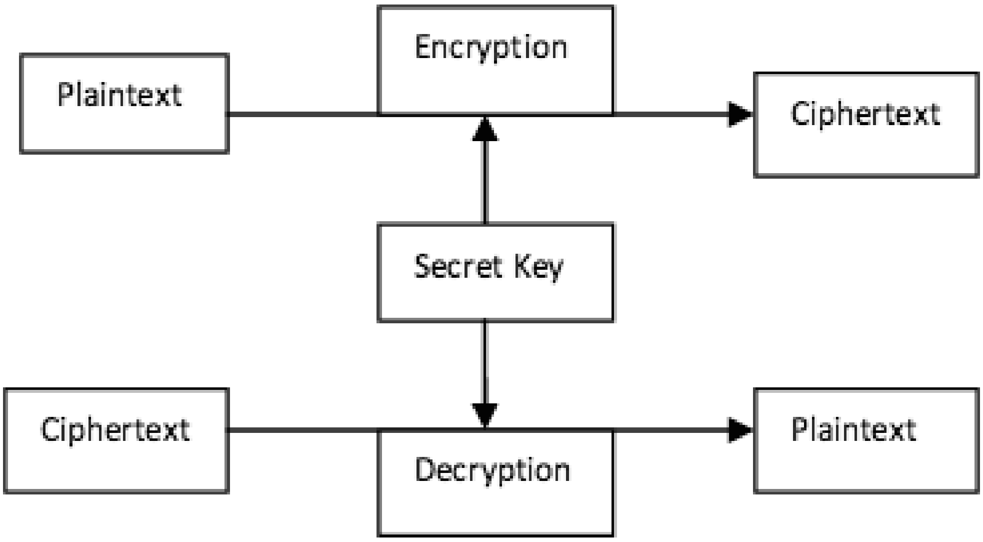


Figure 2.7: Symmetric Key Cryptography Process

Symmetric cryptosystems have always faced is the lack of a secure means for the sharing of the secret key by the individuals who wish to secure their data or communications.

Public key cryptosystem include DES, RSA help to solve the problem of secret key cryptosystems.

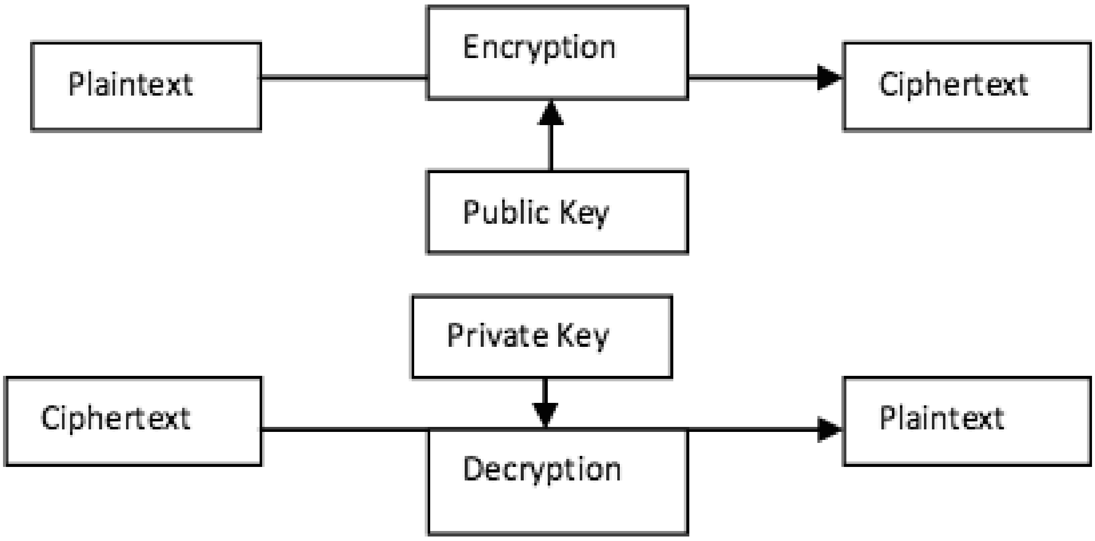


Figure 2.8: Public Key Cryptography Process

2.5.1 Purpose of Cryptography

Cryptography provides a number of security goals to avoid a security issue. Due to security advantages of cryptography it is widely used today. Following are the different goals of cryptography discussed as:

i) Confidentiality

Nobody can read the message not including the future receiver. Information in computer information is transmitted and has to be contact only by the authorized party and not by unauthorized person.

ii) **Authentication**

This process is proving a one's identity. The information received by system then checks the identity of the sender that whether the information is incoming from a authorized person or unauthorized person or wrong identity.

iii) **Integrity**

Only the authorized party is modifying the transmitted information or message. Nobody can change the given message.

iv) **Non-Repudiation**

This is a mechanism to prove that the sender really sent this message. So if any sender denies that he doesn’t send the message; this method not allows doing such type of action to sender.

v) Access control

Only the authorized parties are capable to contact the given information.

2.5.2 Cryptographic Algorithms

2.5.2.1 RSA

This is the most popularly used cryptosystem developed by **R**on Rivest, Adi **S**hamir, and Leonard **A**dleman at the Massachusetts Institute of Technology in 1977 (Robinson, 2008). The RSA algorithm involves the process of generating the public key by multiplying two very large (100 digits or more) randomly chosen prime numbers, and then, by randomly choosing another very large number, called the encryption key. The public key consists of both the encryption key and the product of those two primes. Ron Rivest then developed a simple formula by which someone who wanted to scramble a message could use that public key to do so. Plain text would then be converted to cipher text that would then be transformed that is inclusive of the large product. Using the algorithm developed by Euclid, Ron Rivest provided for decryption key—one that could only be calculated by use of original two prime numbers. Using this encryption key would unravel the cipher text and transform it back into its original plaintext.

What makes the RSA algorithm strong is the mathematics that is involved. Ascertaining the original randomly chosen prime numbers and the large randomly chosen number (encryption key) that was used to form the product that encrypted the data in the first place is nearly impossible (Levy, 2001).

On the other hand, Given that the underlying mathematics is the same for encryption and signing, only in reverse, if an attacker can convince a key holder to sign an unformatted encrypted message using the same key then she gets the original.

2.5.2.2 Pretty Good Privacy (PGP)

It was developed by Phil Zimmerman beginning in early 1991 (Levy, 2001). The strength of the keys that are created to encrypt and decrypt data or communications is a function of the length of those keys. Typically the longer the key, the stronger that key is. For example, a 56-bit key (consisting of 56 bits of data) would not be as strong as a 128-bit key. And, consequently, a 128-bit key would not be as strong as a 256- or 1024-bit key.

2.5.2.3 Data Encryption Standard (DES)

DES is a symmetric key algorithm, which was developed by IBM in 1977. It uses block size 64 bits, key size 56 bits. DES always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm. DES used 16 rounds of transposition and substitution to encrypt each group of 8(64 bit) plaintext letters and output from each round is one by one. The number of rounds is exponentially proportional to the amount of time and fined a key using a brute-force attack. Therefore the number of rounds increases then the security of the algorithm increases exponentially. DES was clearly no longer invulnerable to the attacks.

The strength of DES lies on two facts:

i) The use of 56-bit keys: 56-bit key is used in encryption; there are 256 possible keys. A brute force attack on such number of keys is impractical.

ii) The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

Weakness has been found in the design of the cipher:

i) Two chosen input to an S-box can create the same output.

ii) The purpose of initial and final permutation is not clear.

2.5.2.4 Triple DES

Triple DES is same as the DES operation. It uses three 64-bit keys and overall key length of 192 bits. We simply type in the entire 192-bit (24 character) key rather than entering each of the invidiously three keys. The procedure for encryption is exactly the same as DES, but this process is repeated three times. It is encrypted with the first key then decrypted with the second key, and finally encrypted again with the third key. This procedure for decrypting something is the same as the procedure for encryption, except it is accept same as reverse process.

2.5.2.5 Advanced Encryption Standard

Vincent Rijmen and Joan Daemen in Belgium selected Rijndael as the AES in Oct-2000 Designed. AES is a symmetric block cipher that can block size128bit, Cipher keys 128,192and

256 bits. Basically, encryption algorithms are divided into three major categories – transposition, substitution, and transposition – substitution technique. AES algorithm uses a round function that is compared of four different byte-oriented transformation such as Sub byte, Shift row, Mix column, Add round key. Number of rounds to be used depend on the length of key e.g. 10 round for 128-bit key, 12 rounds for 192-bit key and 14 rounds for 256 bit keys. AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively. As well as these differences AES differs from DES in that it is not a feistel structure. Recall that in a feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. In this case the entire data block is processed in parallel during each round using substitutions and permutations. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and256 bits respectively. At present the most common key size likely to be used is the 128-bit key. This description of the AES algorithm therefore describes this particular implementation. Rijndael was designed to have the following characteristics:

- Resistance against all known attacks.
- Speed and code compactness on a wide range of platforms.
- Design Simplicity.

The overall structure of AES can be seen in 7.1. The input is a single 128-bit block both for decryption and encryption and is known as the in matrix. This block is copied into a state array, which is modified at each stage of the algorithm and then copied to an output matrix (see figure 7.2). Both the plaintext and key are depicted as a 128-bit square matrix of bytes. This key is then expanded into an array of key schedule words

(the w matrix). It must be noted that the ordering of bytes within the in matrix is by column. The same applies to the w matrix.

AES algorithm not only used for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard is recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size as shown in Figure - 2. It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications. Algorithm Steps used to encrypt 128-bit block

1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9: Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of Final Round Step

ii. Usual Round:

Execute the following operations, which are described above.

1. Sub Bytes
2. Shift Rows
3. Mix Columns
4. Add Round Key, using K (round)

iii. Final Round:

Execute the following operations, which are described above.

1. Sub Bytes
2. Shift Rows
3. Add Round Key, using K (10)

iv. Encryption:

Each round consists of the following four steps:

Sub Bytes: The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

Shift Rows: In the encryption, the transformation is called Shift Rows.

Columns: The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.

Iv Add Round

Key: Add Round Key precedes one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition. The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the “Mix columns” step.

v.

Decryption involves reversing all the steps taken in encryption using inverse functions like

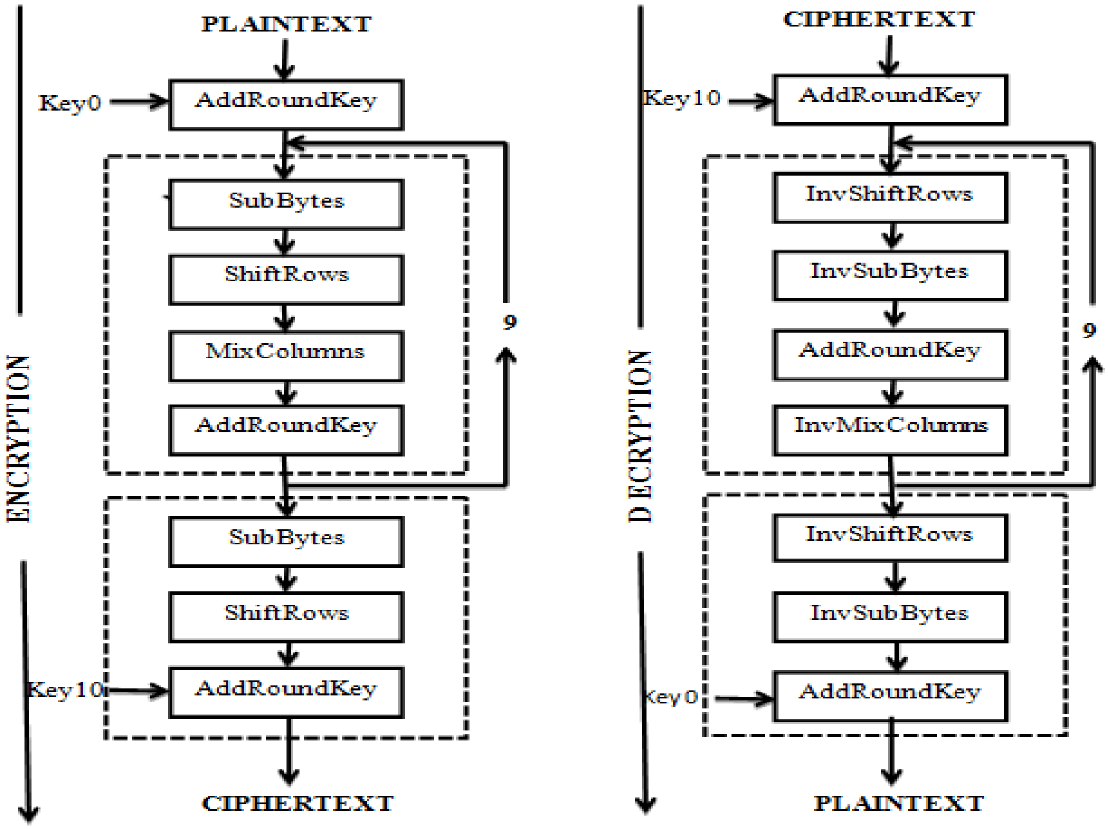
a) Inverse shift rows,

b) Inverse substitute bytes,

c) Add round key, and

d) Inverse mix columns.

The third step consists of XO Ring the output of the previous two steps with four words from the key schedule. And the last round for decryption does not involve the “Inverse mix columns” step.



2.5.2.6 Blowfish Algorithm

Blowfish algorithm is the important type of the symmetric key encryption that has a 64-bit block size and a variable key length from 32 bits to 448 bits in general. It is based on 16 round fiestel cipher network that uses the large key size. The key size is larger as it is difficult to break the code in the blowfish algorithm. Additionally it is exposed to all the attacks apart from the weak key class attack.

2.5.2.7 Diffie-Hellman Algorithm

It is that public key encryption algorithm, using discrete logarithms in a finite field .Two parties allow exchanging a secret key over an insecure medium without any prior secrets. Diffie-Hellman (DH) is a widely used key exchange algorithm. In many cryptographically protocols, two parties wish to begin communicating. Diffie-Hellman protocols are exchange keys and allow the construction of common secret key over an unconfident contact channel. This problem is based on related to discrete logarithms; its name is Diffie-Hellman problem. This problem is hard, as compare to the discrete logarithm problem.

2.5.3 Cryptanalysis classification:

Cryptanalysis is an art and science of breaking the encrypted codes that are created by applying some cryptographic algorithm. Cryptanalysis attacks can classify the following:

i) **Cipher text-only attack** in which the attacker has a part of the cipher text using available information, the attacker tries to find out the corresponding key and decrypt the plain text.

ii) **Known-plaintext attack** (KPA) is an attack model for cryptanalytic wherever the criminal has samples of each the plain text and its encrypted version cipher-text. These will be revealing any secret data like secret keys and codebooks.

iii) **Chosen-plaintext attack** (CPA) is an associate attack model for cryptography that presumes the potential to decide on arbitrary plain text to be encrypted and procure the corresponding cipher-text.

iv) **Chosen-cipher text attack** (CCA) is an attack model for Chosen-cipher text attack A chosen- cipher-text attack (CCA) is an attack model for partially, by selecting a cipher-text and getting its decipherment beneath an unknown key.

v) **Chosen-text attack** is a combination of choosing plain text and chosen cipher-text attack.

vi) **Brute-force attack** this type of attack is a passive attack. The attacker can try all the possibilities of the key until the message is not broken. This is the very slow attack. Suppose that message is encrypted using the 56-bit key then the attacker can try all the possibilities up to 255 bit.

vii) **Dictionary attack** the extension to the Brute-force attack is the Dictionary attack. In the Dictionary attack, it will try also same possibilities but take only those keys bit whose chances of success is more.

vi) **Timing attack** is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. Each consistent operation in a computer takes time to perform

vii) **Man-in-the-middle attack** this is the type of active attack. This differs from the above in that it involves tricking individuals into compromise their keys. The attacker T is placed in the two parties through communication channel who wish to exchange their keys for secure communication.

2.5.4 Performance factors for cryptosystems

The factors used as the performance criteria, are tunability, computational speed, the key length value, the encryption ratio, the security issue, time and throughput of data against attacks.

i) Tunability

It is very popular to define encrypted parts and the encryption parameters used to different applications and requirements.

ii) Computational Speed

In many real-time applications, the encryption and decryption algorithms are fast sufficient to meet real time requirements.

iii) Key Length Value

In the encryption methodologies, the key management is the important feature to shows the how the data is encrypted. The symmetric algorithm uses a variable key length, which is longer. So, the key management is a huge aspect in encryption processing.

iv) Encryption Ratio

The encryption ratio is the measurement of the amount of data that is to be encrypted. Encryption ratio must be minimizing to reduce the complexity on computation.

v) Security Issues

Cryptographic security defines whether encryption scheme is secure against brute force, time attack and different plaintext-cipher text attack. For highly important multimedia application to the encryption scheme should satisfy cryptography security. We measure cryptographic security in the three levels for example low, medium and high.

vi) Time

The time essential by algorithm to total the operation depends on processor speed and algorithm complexity. Less time algorithm takes to entire its operation improved it is.

vii) Throughput

Throughput of the encryption algorithms is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm. Thus, if throughput

increased the power consumption is decrease. In the table Mohit et al (2009) have analyzed DES, Triple DES and RSA three algorithms. DES and Triple DES is symmetric key algorithm and RSA is an asymmetric key algorithm, they have been analyzed on their ability to secure data, time in use to encrypt data and throughput the algorithm requires. Performance of algorithms is different according to the inputs size.

This section presents performance and comparison with respect to various parameters. The encryption ratio is measured in terms of minimum, moderate and maximum. The speed is defined by the following term such as fast, slow, moderate. We specify tenability as either yes or no. The key value is measured in terms of bit value used. Throughput is measured as high and less. Power consumption (used memory) is defined as high and less.

Table 2.1: Comparison of symmetric and Asymmetric encryption

Parameter	**Symmetric encryption**				**Asymmetric encryption**	
	DES	**3DES**	**AES**	**BLOWFISH**	**RSA**	**DIFFIE-HELLMAN**
Key used	Same key used for encryption and decryption	Same key used for encryption and decryption	Same key used for encryption and decryption	Same key used for encryption and decryption	Different key used for encryption and decryption	Key exchange
Through put	Lower than AES	Lower than DES	Lower than blowfish	Very high	Low	Lower than RSA
Encryption ratio	High	Moderate	High	High	High	High
Tunability	No	NO	No	Yes	Yes	Yes
Power consumption	Higher than AES	Higher than DES	High than Blowfish	Very low	High	Lower than RSA
Key length	56 bits	112to 168bits	128,192 or 256bits	32 to 448bits	>1024 Bits	Key exchange

						management
Speed	Fast	Fast	Fast	Fast	Fast	Slow
Security against attacks	Brute force attacks	Brute force, chosen plaintext known text attacks	Chosen plain and know text	Dictionary attacks	Timing attacks	Eaves dropping

Adopted from International Journal of Computational Engineering & Management, ISSN: 2230-7893.

2.5.5 User-centricity identity management

When making services and resources available through computer networks, there is often a need to know who the users are and to control what services they are entitled to use. The identity management has main two parts where the first consists of issuing users with credentials and unique identifiers during the initial registration phase, and the second consists of authenticating users and controlling their access to services and resources based on their identifiers and credentials during the service operation phase. The study conducted by Bhargav-Spantzel et al (2007) differentiated between two predominant notions: relationship-focused and credential-focused identity management. In the former approach, a user only maintains relationships with identity providers (IDPs) and thus every transaction providing identity information is conveyed to the appropriate IDP. In the latter approach, the user must obtain long-term credentials and store them in a local provider database. Most predominant identity management model on the Internet today is the silo model where users handle their own data and provide it to organizations separately. The silo model has weakness of data redundancy and to solve this a better model know as centralized federal modal was introduced such as Microsoft passport which removes inconsistences and redundancies of silo model to provide web users with seamless experiences. Taxonomy for unifying the relationship-focused and credential-focused identity management, and investigated the idea of a universal user-centric system, which incorporates the current approaches. Bhargav-Spantzel et al provided an open search question for a credential-based user-centric system that crosses the boundaries of user-centricity. The study also supports their approach in unifying the notions in user-centricity that could be useful in the field of user-centric federated identity management systems (FIMS).

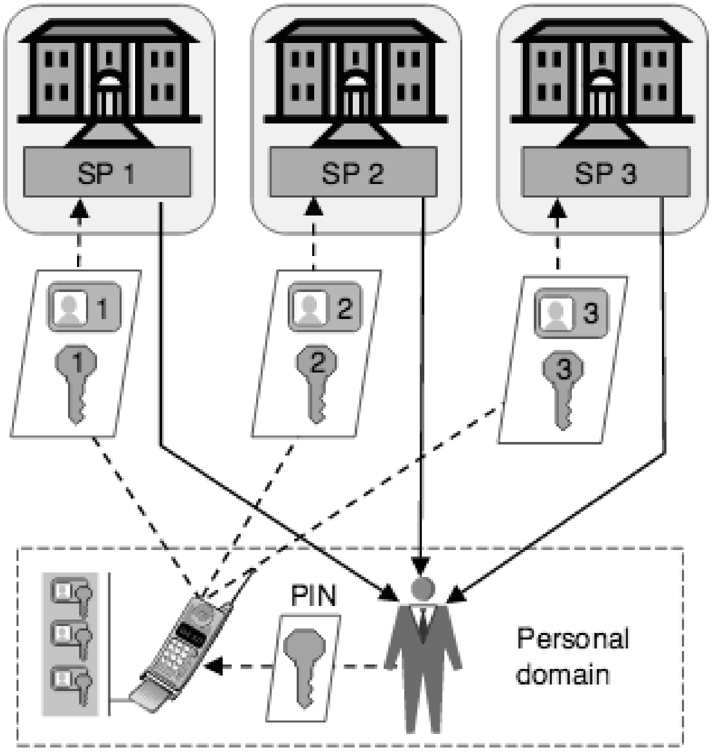


Figure 2.9: User-Centric Identity Model

2.5.5.1 Weakness of User –Centric Identity Model

Problem with many identity management systems is that they are designed to be cost effective from the perspective of the service providers (SP), which sometimes creates inconvenience and poor usability from the users' perspective.

In addition to being SP centric, traditional identity management systems have largely ignored that it is often equally important for users to be able to identify service providers, as it is for service providers to authenticate users. In the case of online service provision through the web, user authentication typically takes place on the application layer, whereas SP authentication takes place on the transport layer through the SSL protocol. In the case of online service provision through the web, user authentication typically takes place on the application layer, whereas SP authentication takes place on the transport layer through the SSL protocol. However, the common scam called

Password phishing illustrates the difficulty of service provider authentication with SSL. This encourages attackers who pause as online bankers and send spam emails requesting users to logon thus acquiring their details

2.6 Patient Centered Access Control Approaches

In this section, the researcher reviews literature on Patient-Centered Access Control Secure System Online, PCASSO Project (Baker and Masys, 1999) and Privacy-aware Patient-controlled Personal Health Record (Huda et al.2009)

2.6.1 PCASSO Project

The Patient-Centered Access Control Secure System Online, PCASSO Project (Baker and Masys, 1999) proposes a system that addresses the vulnerabilities and risks involved in accessing sensitive patient information over the Internet. PCASSO is a research development, deployment and evaluation project funded by the US National Library of Medicine through the National Information Infrastructure Initiative and its intended users are health care providers, medical researchers and patients (Baker and Masys, 1999).

2.6.1.1 How PCASSO works

PCASSO is designed to provide secure Internet access to electronic patient health records to both the patient and providers. It secures data end to end: in the server, in the data repository, access on the network and at the client side (Baker and Masys, 1999). PCASSO uses role based access control, multilevel security and strong device & user authentication (Baker and Masys, 1999).

Role Based Access Control and Explicit Authorization: Every user is associated with one or more roles, which define the level of patient data, the user can see with least privileges and explicit authorization (Baker and Masys, 1999). This implies that a user with a doctor's role may only read data with clearance for doctors and not any higher and only if the patient has authorized this particular doctor to read his or her health record. It also ensures that the users only have need to know access and without default authorizations. Users can only access records that patients have particularly authorized them to. Access to patient data is based on user roles using labels. Patients have access to their whole own records only by default. Providers have access to all the data on all patients when they assume the role of emergency care provider, a role they can only assume for up to 72 hours. A patient's primary health care provider or secondary care provider has access to all the patient's data (Baker and Masys, 1999).

Multi-factor authentication: PCASSO requires users to have a username and password, public/private key and respond to a challenge from the PCASSO server to provide three factor authentication (Baker and Masys, 1999). The username and password are authenticated by a trusted operating system, the digital certificates located on a removable medium such as floppy or flash disk are used to encrypt the data and to authenticate the user to the PCASSO server and the PCASSO server to the user and the challenge response that is only used once to add another level of security in case the user ever lost his username and password together with the removable medium (Baker and Masys, 1999). Each authenticated PCASSO user is granted only the rights to which he or she is authorized on the PCASSO.

Security on the Network: After authentication of the user to the PCASSO server and the PCASSO server to the user, the two exchange a symmetric key that is used to encrypt data flowing between them. PCASSO uses SSLv3 that is widely accepted in healthcare as a strong mechanism for transmitting data over the Internet to provide secure communication between the PCASSO system and the client connection (Baker and Masys, 1999). Protection from the Client Machine: PCASSO does not assume security at the client computer from attacks such as viruses. The client computer downloads an applet application during the authentication phase from the PCASSO system that is constrained and immune to malicious software such as virus or Trojan activities.

High Assurance Server: PCASSO proposes a trusted operating system that can withstand rigorous efforts to compromise its security. This OS should provide role based access control through data labeling with strong isolation between levels of sensitivity within the server.

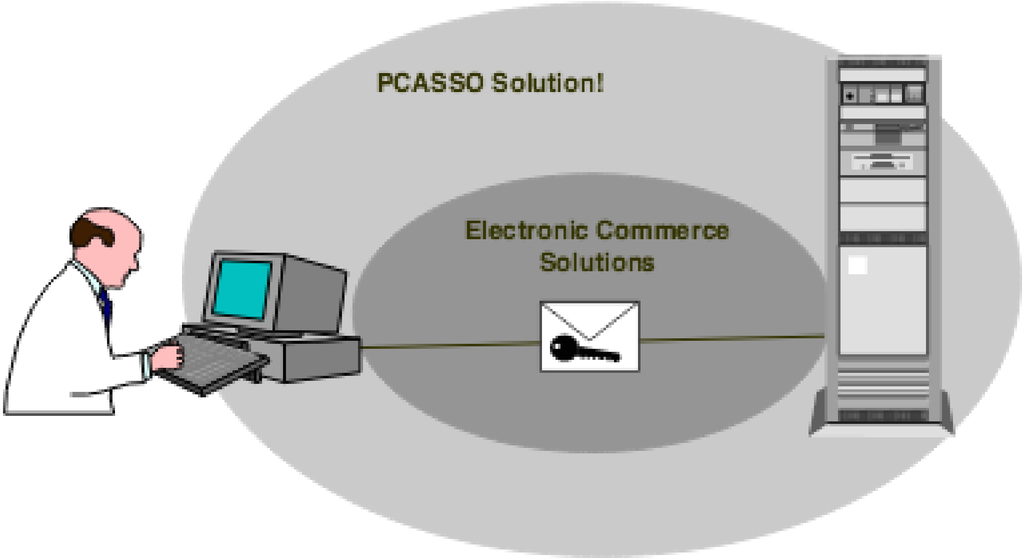


Figure 2.10: PCASSO provides protected server and client environments

2.6.1.2 Strength and weaknesses of PCASSO

PCASSO is designed to provide technical controls for protecting electronic patient data from external threats such as hackers and malicious software and internal threats such as authorized users accessing information they are not authorized to. It provides end-to-end secure patient ubiquitous access to their electronic medical records.

Although PCASSO gives the patient ubiquitous access to his or her electronic medical record, it is not adequate at protecting the patient's electronic medical information from the provider to satisfy HIPAA standard.

2.6.2 Patient Controlled Health Record

Electronic form of personal health records is both a problem and an opportunity. It opens new kind of threats to information leakage because electronic data are easy to copy, especially when the records are online. Thus, most Personal Health Records (PHRs) are kept local and specific to one point of care (Kim and Johnson, 2002). As such, most existing PHRs only provide the patient with limited insight into parts of the patient's health care information. On the other hand, electronic health records help make health care safer, cheaper, and more convenient by providing complete health history, avoiding repeated tests, and allowing appropriate authorities to have ready access to PHRs anytime anywhere. Researchers at RAND Corporation have estimated that full adoption of electronic health record systems in the USA would save $81 billion annually (Hillestad et al ,2005). Emergency room physicians can avoid duplicating diagnostic tests when they can see instantly from digital records that a patient's regular doctor has already ordered the necessary tests. This one efficiency measure alone could save upwards of $60 billion each year in the USA (Willey and Daniel, 2006).

People usually go to the healthcare centers nearby their residence for health services and their health information is kept secured in the local databases of those healthcare centers. However, patients sometimes may need to get services from different healthcare centers for various reasons, including but not limited to (i) unavailability of service on holidays, (ii) need for specialized care at specialized centers, (iii) travelling away from usual residential area, and (iv) moving residence. The stored health information in a healthcare center is usually accessible only to healthcare personnel of that center. For every healthcare center, there are separate systems to record patients' health information, and information flow between systems is limited as illustrated in Figure 2.11. For example the patient in Fig. 2.11 has health records in three different hospitals (A, B and C). Doctors of a particular hospital cannot access the patient's health records that are stored in two other hospitals. As a consequence, patients often need to retell their medical history and redo tests whenever they encounter a new health care provider.

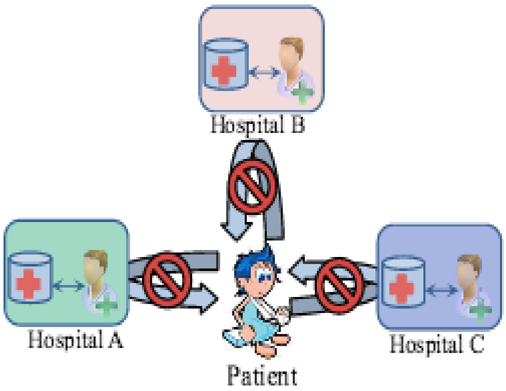


Figure 2.11: Health Records Stored in Local Systems in Different Healthcare Centers

2.6.2.1 How PHRs work

Each time a patient visits a new healthcare center, the patient may need to request for old health records from several previously visited healthcare centers, which is a time consuming and tedious job. If the patients can have full control over their own health records, they can share the appropriate part of their health records with appropriate caregivers when necessary. Thus, a patient-controlled health record (PCHR) system is necessary. The goal of a PCHR (Mandl et al, 2001) is to assemble the patient's complete health history and let the patient control whom to give access to this information and when.

2.6.2.2 P^3 HR System

The devised Privacy-aware Patient-controlled Personal Health Record (P^{3}HR) system is not meant to be an alternative to healthcare centers' usual local health records system. Instead, it is intended to provide a convenient, easy, secure and (Huda et al.2009). Privacy preserving is a way of making patient's personal health history available to any healthcare center at any time according to the patient's desire. Disclosure of some personal information to unauthorized parties doesn't necessarily mean privacy loss. If the unauthorized party cannot link or associate the disclosed information to the specific individual (to whom the private information belongs to) we do not say it is privacy loss (Huda, Kamioka, and Yamada. 2007). Based on this principle, P^{3}HR database is made anonymous by removing all quasi-identifier information. None, except the data subject (patient), can link a particular record of P^{3}HR database to the respective patient because the patient's unique ID (digital pseudonym) (Chaum, 1981) in a record that links the record with the specific patient and is known to the respective patient only. Figure 2.11 illustrates the simplified framework for P^{3}HR system. A patient can personalize/customize her privacy control policy through the web-based service from her home. The P^{3}HR site host's anonymous personal health records, provides mechanisms for personalizing privacy control policies and provides access control module for doctors and patients. A hospital is equipped with IC card readers for authentication and browsers for browsing patients' health records.

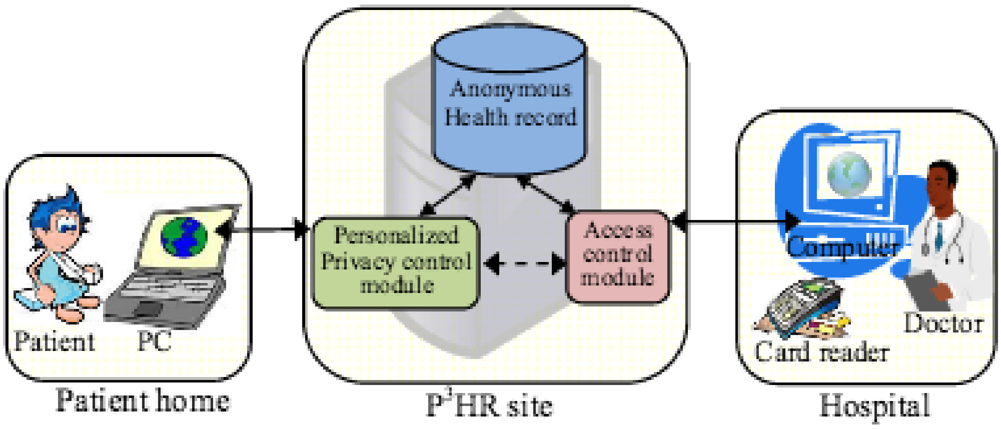


Figure 2.12: The Framework for Privacy-aware Patient-Controlled Personal Health Record (P3HR) System.

The P^{3}HR security system architecture consists of an anonymization module, an anonymous health record database, the patient's profile, access control modules for patients, access control modules for third parties, and a privacy control module as shown in Figure 2.13. The functionality and operation of each module of the architecture have been described in the following subsections.

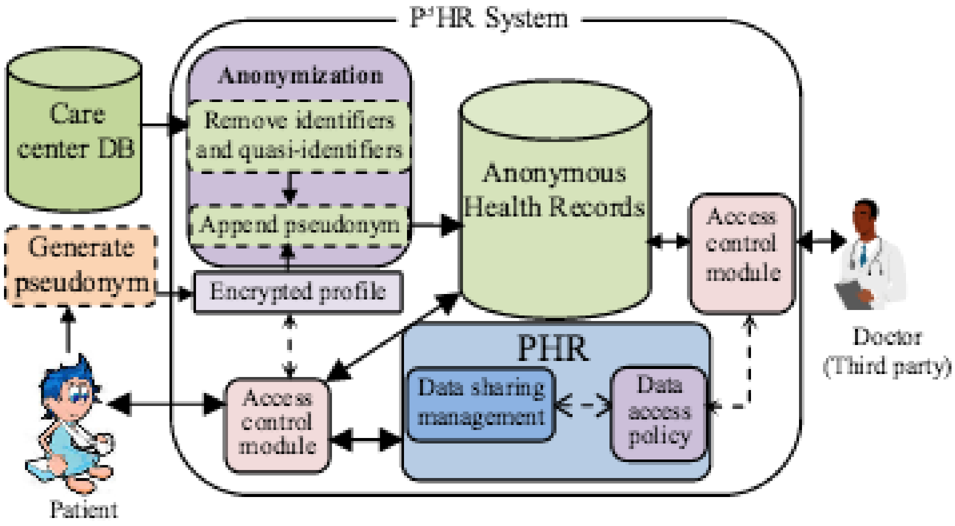


Figure 2.13: The P^3HR security system architecture

2.6.2.2.1 How Anonymization module works

To preserve patient's privacy from intruders, P^3HR system stores patient's health records in an anonymous form. Before storing health records from a care center database (or from patient's direct input) into the P^3HR database, the anonymization module removes all identifiers and quasi-identifiers (Ferrari and Thuraisingham, 2005) from the records so that a particular record cannot be associated with a specific identifiable individual. Thus, even if an intruder gets access to the P^3HR anonymous health database, he cannot determine which record or set of records belongs to a particular patient. To allow an authorized party (e.g., doctor) to access a set of records of a particular patient legitimately, the system needs to associate each record to the respective patient. To achieve these two conflicting goals of anonymization and keep each record associated with the respective patient, the patient creates her unique ID (known as digital pseudonym) using Unique User-generated Digital Pseudonyms mechanism (Schartner P; and Schaffer M. 2005). A patient can generate her pseudonym locally in her personal security environment, e.g. in her smart card or her personal digital assistant. There is no need for any information interchange between the patient and P^3HR system, except P^3HR supplies a unique identifier for each request (e.g., auto increment number). The digital ID is long enough and randomized so that one cannot guess it from the patient's background or personal information (e.g. name) obtained through other channels/sources. The patient also doesn't need to remember her digital ID. A patient's digital ID (pseudonym) is appended to all of her records during the record adding process. Thus, a record in the anonymous P^3HR database contains the respective patient's pseudonym along with her health information. No one can reveal the association of a pseudonym with its holder, unless the holder explicitly discloses it. Figure 2.14 shows the process of making an anonymous personal health record.

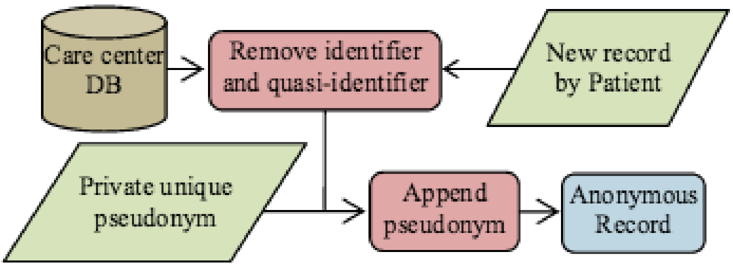


Figure 2.14: After Identifiable Information is removed; a Patient Appends Her Private Pseudonym with her Records.

A patient stores her pseudonym into her encrypted profile. The system accepts a new pseudonym that is not already in use by others. The patient needs to decrypt her pseudonym when she wants to add (or accept from an external source) a new health record. The system takes the decrypted pseudonym and appends with her new records. A pseudonym is created for the system use only and is visible to its holder only.

Security and privacy researchers have identified many items, which are used in different healthcare centers, as personally identifiable information (e.g., telephone numbers, fax numbers, e-mail addresses, social security numbers, health plan beneficiary numbers, vehicle identifiers and serial numbers etc. (Brook J.M.C.2008). Most of the personally identifiable information does not change frequently with time and they can make up a patient's profile. Patients sometime require personally identifiable information to be provided to the new healthcare centers that they visit for the first time. For providing general personal information conveniently to newly visited centers, P3HR system allows a patient to store her profile, consisting of general identifiable information, encrypted with a shared key. General

identifiable information includes the information that is usually stored in a paper based health card, such as name, address, and date of birth, phone number, and blood group. A patient can provide her shared key to the caregiver where she visits a care center for the first time. The care centers store needed general personal information into their secure local system. Some additional private information (e.g., patient's pseudonym), which is used for database anonymization, is also kept encrypted with the patient's public key. The extended profile is not shared with others. Figure 2.15 depicts the technological aspect of a patient's encrypted profile.

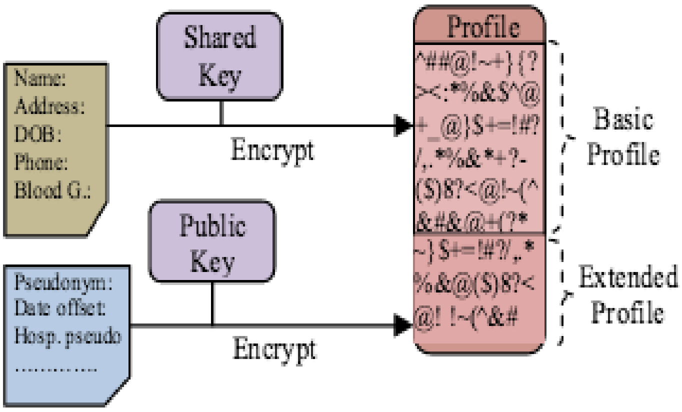


Figure 2.15: Personally Identifiable Information is kept Encrypted into Profile

2.6.2.2.1 Strength of P^{3}HR

In P^{3}HR system, the stored data is made anonymous so that an intruder cannot associate a record with a specific individual. We use patient created secret pseudonym that is known by the patient only to associate records with the respective patient. However, the relation between a physical patient and her pseudonym remains secret and does not need to be disclosed to anybody in order to use the system. The advantage of our system is that our stored database becomes most likely completely anonymous and it is highly unlikely that the data subject could be identified from the stored records. Thus, our system allows patients to have control over their health records, which in turn helps makes health care safer, cheaper, and more convenient

2.7 Conclusion

Due to resource limitation and the need to ensure maximum security the system operates on the lab LAN. There are 5 pcs that’s the server then the PC for receptionist/nurse then the other one is in the lab to capture and store the results print reports for client to take to their doctors and finally the one in the accounting department. The MDLS uses the familiar point-and-click interface of today's Web browser to bring your data to your desktop anytime. After a review of cryptography tools the researcher opted to use Advance encryption standard (AES) because of the following advantages: -

- AES is more secure (it is less susceptible to cryptanalysis than 3DES
- AES supports larger key sizes than DES's 112 or 168 bits.
- AES is faster in both hardware and software.
- The latest U.S. and international standard require AES

CHAPTER 3

METHODOLOGY

In this chapter, the researcher presents the methodology that was used in carrying out the research. It gives the research and system development methodologies, target population, and sampling procedures including the sampling techniques and sample size. It also gives data collection methodologies used namely document review, interview and questionnaires. In addition data analysis, system analysis and design, implementation and testing methodologies are also presented.

3.2 Research design

A User Centered Design (UCD) approach is adopted for this project, this means, that the users were placed at the center stage in the design phase of the system to be developed. The term 'user-centered design' originated in Donald Norman's research laboratory at the University of California San Diego (UCSD) in the 1980s and became widely used after the publication of a co-authored book entitled: User-Centered System Design: New Perspectives on Human-Computer Interaction (HCI) (Norman & Draper, 1986). Norman further built on the UCD concept in his seminal book titled The Psychology of Everyday Things (*POET*) (Norman, 1988). It is both a broad philosophy and variety of methods. There has been limited research and debates over the use of participatory techniques in developing countries. This compelled the researcher to attempt and test this method for this project. An Illustration to this research design is given figure 3.1 below.

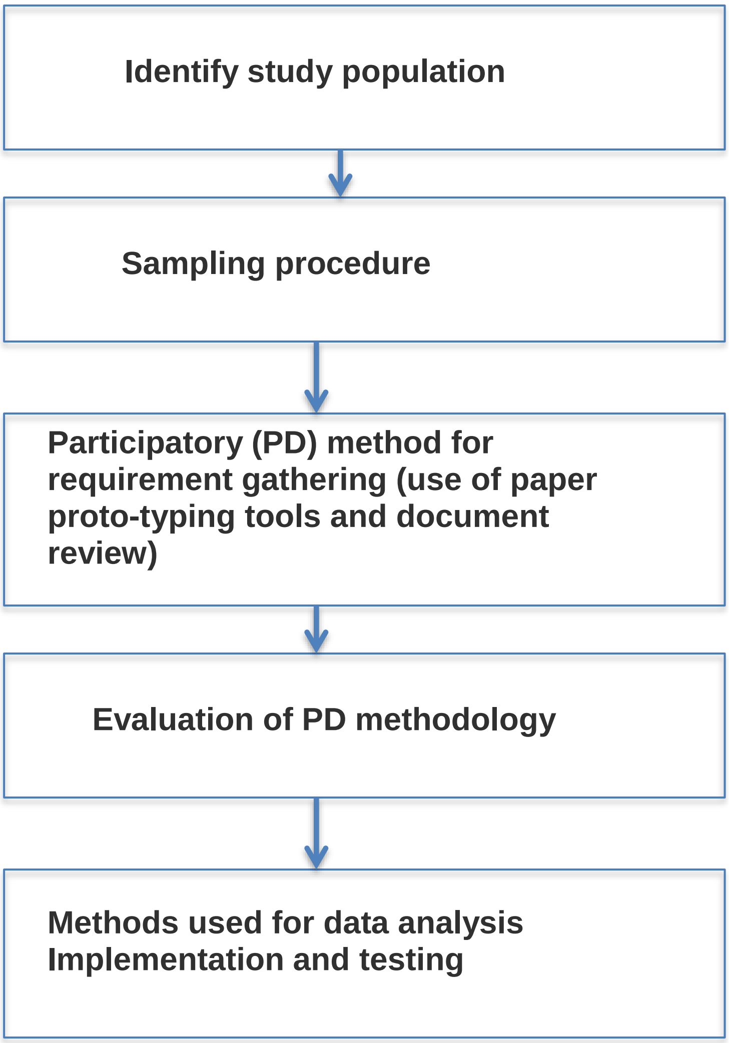

Identify study population
Sampling procedure
Participatory (PD) method for requirement gathering (use of paper proto-typing tools and document review)
Evaluation of PD methodology
Methods used for data analysis
Implementation and testing

Figure 3.1: Illustration of User Centered Design

3.2.1 Area of study

The researcher used the case study approach when collecting data with the aim of solving the broad-spectrum problem of poor data security management by medical facilities especially the lab management team. Focus was on Mbarara diagnostic lab with kin interest of lab management information security.

3.2.2 Systems study

This section explored the study of the current system; the problems associated with it and also bring out the need that guided the researcher to come up with this project.

3.2.2.1 Study population

This research was conducted with the intention of mainly enhancing information system security to patients' records at the center. The study populations in this case are staff that is receptionist, laboratory technicians and nurses and physicians who were able to directly participate in the systems design.

3.2.2.2 Sampling procedures

Sampling is involves selecting and inquiring from a fraction of the total population for purposes of making the conclusions about the population as a whole (Oxford, 2011).

3.2.2.2.1 Sampling technique

Purposive sampling was the chosen sampling technique. It is a non-probabilistic technique of sampling that gives the researcher freedom to select a sample based on judgment towards a specific purpose. This method was used by the researcher to identifying the key stakeholders who participated in the design of the system. This was made possible after a face-to-face interaction with the administrator in-charge of the lab' general manager.

This technique was selected to enable the researcher to acquire the right information for this project. Furthermore there was need to focus on the key actors that directly take part in the lab process. These are the lab technicians and doctors who interpret lab results. Also, this sampling technique provided for free interaction and willingness by the respondents who were selected to participate in the entire process.

Four participatory design sessions were conducted at the lab center on different days. Six participants were selected among the Administrative staff and 2 clients.

3.3 Data Collection Methods and Instruments

Various systematic ways was used to collect information during this project work. A chosen method was based on several considerations including a purpose of the technique, values, availability and cost (Bryman et al., 2007). Four methods that were used on the project are briefly explained below.

3.3.1 On Site observation

The researcher observed the procedures that were being used to register, store, retrieve and prepare reports for reviews and submission to physicians. Also, the flow of documents in the organization was observed. The research observed how the activities were being carried out at the lab center to gather information to boost understanding on the researched project and to be able to take action. This involved observing how clinicians handled patients, then how patients data was recorded kept and how patients where handled in case of an emergency. The research took kin interest in security of the records. That is the level of security of the patients' record and the availability of the records by patients and other medical staff.

Observation helped the researcher to obtain firsthand information about the events. It also allowed for verification of statements made in interviews and also to determine if procedures operate as specified in system documents.

3.3.2 Individual interviews

The researcher conducted individual interviews from the lab attendants and clinicians about the safety of patients' records and how they avail access to the lab clients. The researcher also interviewed clients how easily are they availed with their medical results and confidential clause. How they also obtain their past records. This was done to verify actually whether there was a problem in the way clients medical records are handled and also accessed in case of a need to. Collecting data related to the needs and expectations of users evaluation of design alternatives, prototypes and the final artifact

3.3.3 Literature Review

The researcher reviewed literature about the international health systems standards, access control approaches, cryptography and patient centered access control models. The objective was to determine the acceptable standards for patients' electronic health records security and how access control approaches achieve them. The researcher examined how patient centered access control could be used to achieve the patient's electronic health records security and determined requirements for this approach in resource limited environments.

3.3.4 Paper prototyping

For the researcher to attain the objectives of user centered, paper prototyping was used as a methodology. This is because it involves working directly with the users to develop a system that will meet their needs. Paper prototyping is a widely used and validated technique for exploring, communicating, and evaluating early interface designs (Bailey et al, 2008).

During user-centered design, it is not everyone who is a stakeholder needs to be represented on a design team, but the effect of the artifact on them must be considered (Preece et. al, 2002). Prototypes were typically constructed using combinations of stock paper to represent main interface screens, overlays and sticky notes to represent results from user interaction, colored pens and pencils to sketch content, etc. Paper prototyping has many benefits during the design process. These benefits include allowing rapid externalization of design ideas with low investment and allowing numerous alternatives to be generated and tested early in the design cycle.

Participatory Design (PD) enables end users to become part of a design team as well as test the usability of systems (Snyder, C. 2003). Therefore, involving users in design facilitates the elicitation of requirements and early refinements. In this study, we used lab technicians because they were lead users of the systems

Paper prototyping was used because it provided a cost and time benefit since it involves the use of inexpensive material to create paper prototypes, minimum time and effort is required and technical skills are not required to create a paper prototype. Furthermore it improves interaction between the end users and the researcher will relieve the user of being bombarded with a product that they have to learn. It also improves user focus due to the early involvement of the users in the early stage of the development lifecycle such as the conceptual review stage. This will reduce user resistance in the future.

3.3.4.2 General Steps of the Paper Prototyping Method

This section describes the guidelines that were taken when using paper prototyping as a requirements gathering and elicitation tool.

a) Conducting an evaluation meeting

The meeting provided a platform to brief the stakeholders about the overall objectives of the sessions and the goals to be accomplished. Top management support is a critical success factor for the implementation of IS (Thong et al., 1996; Yap et al., 1992) and other organizational innovations (Damanpour, 1991). The procedures that guided the researcher together with the stakeholders are summarized as:

i) The purpose of the research, its specific objectives and their role in contributing to achieving the objectives of the research.
ii) An introductory briefing on the history of paper prototyping, its relevance and use in the industry and how it relates to participatory design.
iii) Provide participants with information about paper prototyping method as a research

tool. And the free mindedness expected from them emphasizing that there is no right or wrong answer and were free to explore their creative side.

iv) Evaluation of the current system and an earlier version or competitor system to identify usability problems and obtain measures of usability as an input to usability requirements, and review of necessary documentation.

v) Two groups are separately handled in developing the prototypes, which meant that, a number of requirements were elicited by the end of the session. All the members in each group collaboratively are tasked to develop the prototypes with the guide of the researcher.

vi) A briefing about the stationeries and materials used to develop paper prototypes. Samples of paper prototypes are provided in order to stimulate the stakeholders' design.

vii) A highlight of the benefits of the prototype in order to convince skeptics and to encourage the participants to give their full commitments.

viii) Use of questionnaires

b) Evaluation of paper prototypes

At this stage the goal of the researcher was to conduct an evaluation in order to get the users views and perception about the paper prototypes. This was conducted by using a table of performance measures that helped to tap the stakeholder's responses.

3.4 Analysis of findings

The desire to interpret the user's artifacts is necessary for purposes of system requirements acquisition, elicitation and implementation. This is done by selecting and going through the different paper prototypes and recommending the one with high precision. This exercise was conducted together with the stakeholders.

3.4.1 Data Analysis Techniques

This section explains the suitable technique that was used to analyze the data that was gathered form user participations.

3.4.2. Contextual and Narrative Analysis

Some time it is not possible to code all texts during analysis. But, contextual and narrative analysis was developed as an alternative to techniques such as coding. Instead of segmenting the data into discrete elements and re-sorting them into categories, these approaches to analysis seek to understand the relationships between elements in particular text, situation, or sequence of events (Kaplan and Dorsey, 1991). Liker scale attitude statements are utilized in order to analyze the user's satisfaction.

3.5 Limitations

With paper prototyping it was not possible to evaluate the details. It's was also difficult to measure object time. It's also required a lot of commitment and dedication from the modulator, which was tiresome and time consuming

3.8 Ethical considerations

Permission to conduct the research was gotten from the lab management since they need a system to ease their work and secure their clients records. Personal information like from interviewed clients was not to be disclosed. And staff member voluntarily participated in the interview and their responses were not disclosed to management. Providing a secure and reliable system was a requirement. User roles were identified and information to be disclosed to them was acquired too.

CHAPTER FOUR

SYSTEM ANALYSIS AND DESIGN

4.1 Introduction

This chapter presents findings from the data collected, analyses the results and presents the requirements gathered for the development of the Medical Laboratory System. An evaluation of the methods used, the system architectures and models were developed in this section that provided a comprehensive description of what the new system will require.

In order to implement a properly operational EHR system for the case that is Mbarara diagnostic laboratory, the researcher conducted a concurrent mixed study with selected key stakeholders using a purposive sampling method as explained in Chapter three. Five administrative members of staff were selected from the administrative staff and 45 clients were selected basing on gender. In order to automate the process, the researcher opted for an open approach in design and evaluation, instead of using hypothesis testing based methods to provoke inspirational responses. Consequently, four participatory design meetings with participants were conducted. In this case the researcher was the designer and facilitator. In particular, the work of (Retin, 1994) was used to develop low – to – high fidelity prototypes during the participatory design sessions.

4.2 Data Analysis and Presentation of Findings

After gathering the feedback from the target user groups, findings indicate that there is need for an automated system accessible to provide easy access to medical records. As revealed in the previous section, the current system is manual. Therefore, the decision of which features to include a secured system was largely influenced by the feedback gathered from intensively engaging the stakeholders using a participatory approach.

Table 4.1 below shows the different respondents who were engaged.

Table 4.1: Respondents' category

Category	Frequency	Percentages
Clients	45	90
Staff	5	10
Total	50	100

Table 4.1 above indicates respondents' categories, whereby clients are the majority with a representation of 45 (90%), followed by Laboratory staff whose representation was 5 (10%). The administrative staffs are few because the organization staff members are not that many in numbers. The information can be graphically presented as the figure below;-

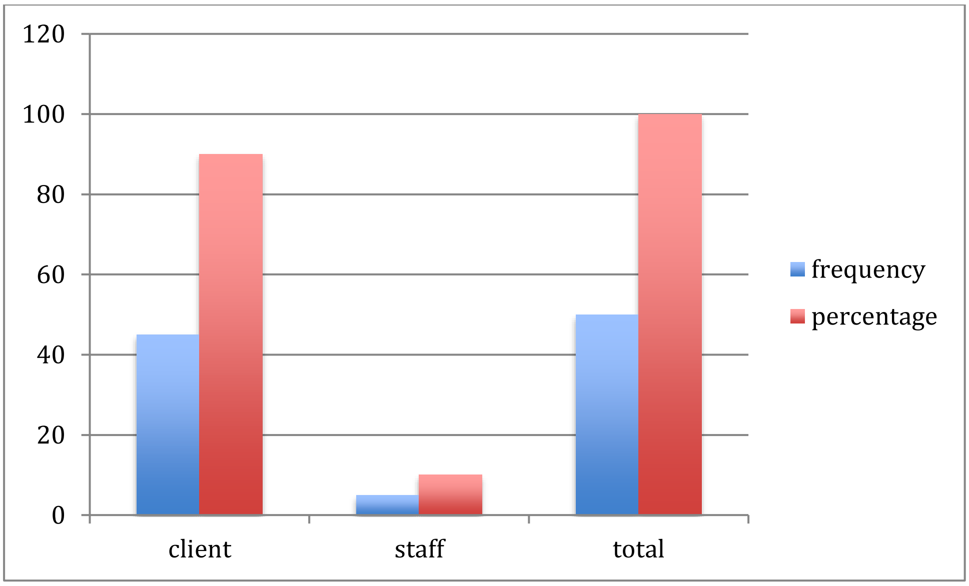


Figure 4.1: Graphical representation of respondents' category staff and clients

Table 4.2: Respondents by gender

Gender	**Frequency**	**Percentages** **%**
Males	29	58
Females	21	42
Totals	50	100

From Table 4.2 above, it can be seen that majority of the respondents targeted were male who made up a representation of 29 (58%) respondents. The female respondents only made up a representation of 21 (42%). Majority of these male were always visiting the medical center. The information can be graphically presented as the figure below;-

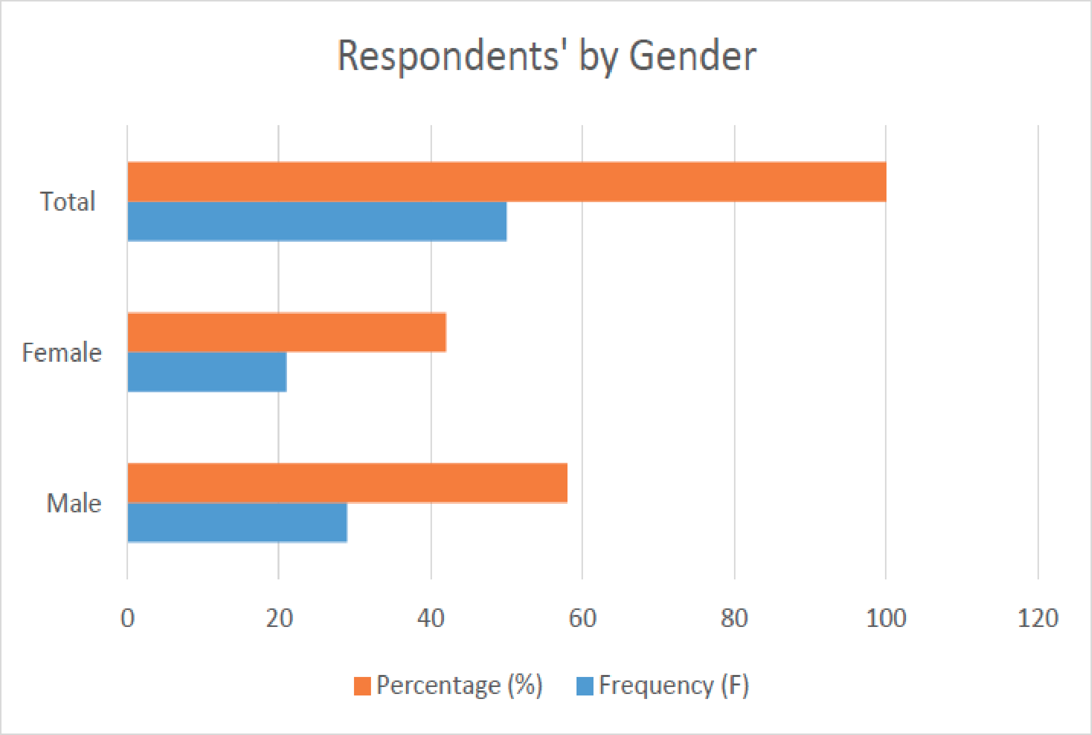


Figure 4.2: Graphical Representation of Respondents by Gender

Table 4.3 Table showing the age categories of respondents

Category	**Frequencies**	**Percentages**
5 – 15 Age	15	30
15 – 30 Age	15	30
30 – 45 Age	10	20
Above 50 Age	10	20
Totals	50	100

Table 4.3 above indicates majority of the respondents in selected from the different age groups, 5-15, a total of 15 (30%) respondents. The age groups in the range 15-30 had a total of 15 (30%) respondents. Those in the range 30-45 had a total of 10 (20%) respondents and the

age group above 50 years had a total of 10 (20%) respondents. The information can be graphically presented as the figure below;-

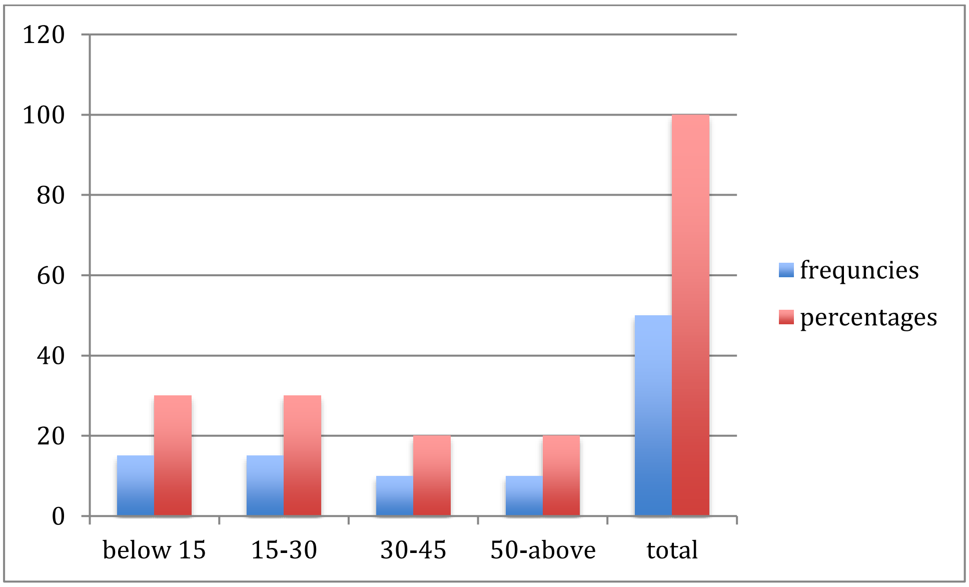
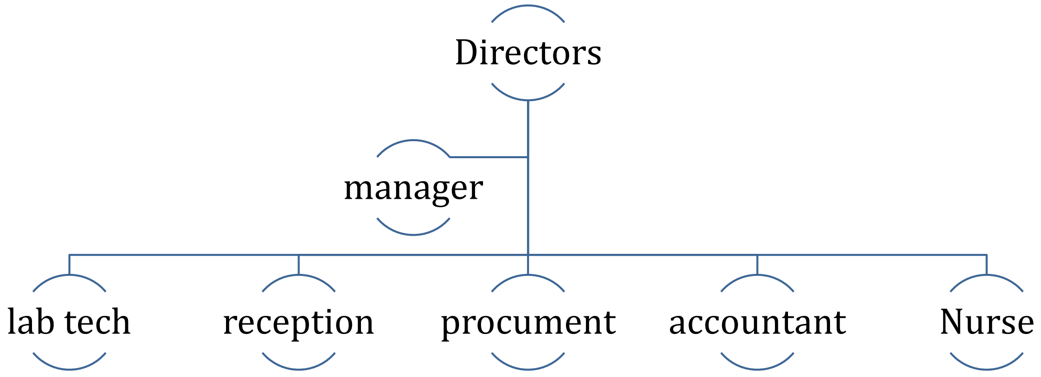


Figure 4.3: Represent respondents' basing on age groups

4.3 Current System

Mbarara diagnostic center is a privately owned medical laboratory located in the center of Mbarara town. The laboratory has director's at the top as heads and a manager who monitors and controls day to day activities and below him is other staff members include receptionists who receive and records patients then the lab technicians, an accountant, logistic officer and a physicians. Because of the modern lab equipment available at the center other privately owned clinics send their patients here to have they samples of tissues, blood and other bodily fluids checked and results sent to them. And the lab keeps a record of all the clients tests carried and the results

Figure 4.4: current organization structure



The following table shows the responsibilities of different staff at the facility.

Table 4.4: Roles of Staff at the Facility

Position	**Roles**
Receptionist/inquiries	Receives and records clients and gives them directions where to go next
Lab technicians	These ones carry out testes of the Specimen
Nurse	Handle patients on treatment
Procurement /account	Responsible for purchase of supplies, payment of staff and keeping books of accounts
Physician	Diagnoses patients

Table 4.5: The analysis of the current System at Mbarara Diagnostic Center

Questions	**Analysis**	**Conclusion**
Current Software	- Manual System (Paper based)	Need an Electronic System

Database		
Type of database	- None	Need a centralized database to store encrypted patient information
Operating system	- None (Since computers are not used)	Need an Open-source system
Application programs	- None	Outdated
Documentation	- Manual records/paper based	Electronic documentation
Security on Data	- None, accessible by anyone, locked in overhead cabinets - No restricted limitation of access to the box files	Include strong security features in the stored data by encrypting all the records
Backup of database	- None	Need a centralized database and back of electronic data in the cloud and other servers
	-	
Data validation	- None	Be included in New LMIS (Laboratory Management Information System)
Linkage to other databases	- Admission number is the link though manually	Be included in New LMIS
Ability to export data	- No export feature	Export/import feature needed
No of potential system users	- 5 users; Doctors, Nurses, Reception Clerks, Laboratory personnel, Pharmacists	Be trained in New LMIS

Other important features to be included	- Enabling of all the patient data while include prescribed medicine, diagnosis carried out and laboratory results.	Be included in New LMIS

Table 4.6: Analysis on Current Hardware and Reporting Needs

Major Area	Requirement	Conclusion
Current Hardware and Network infrastructure	- No servers, no network only one portable modem - 4 standalone computers for clerical work and 2 printers	Need established IT infrastructure
Laboratory results	- Results still manually tracked and there is no security at all which minimizes confidentiality of patient data	Need to include the weighting criteria in LMIS
Reporting mechanism	- Manually done	Automate reports
Reporting frequency	- Weekly, monthly, quarterly and annually	Be automated
Reporting format	- Typed on standalone computer - Backup typewriter	Provide for reporting

4.3.1 The Business process

When a patient arrives at the laboratory, the receptionist captures their details and then the patient is sent to the physician for consultation. On the other hand, if the patient was sent from another clinic they present their physician’s recommendation to the receptionists, which are then recorded. These patients then make payments from the accounts section after which they are sent to the laboratory where blood samples or bodily tissues or fluids are taken from the client depending on the type of test to be carried out. The lab technician records the results and prints them and issues a hard copy to the patient to take to the doctor. Usually, a copy of their test results is retained in the system including client details.

4.3.2 Challenges of the Current System

Mbarara diagnostic center current laboratory processes are paper based where all the records are documented on paper. Registration of patients is also done on a piece of paper form. The logistics management department uses MS excel to track its records of purchase and other lab expenses.

The following are the challenges of the existing system:

i) The time taken by staff in recording patients’ records is not optimal. This result into long queues at the facility as patients is registered and makes payments. Also the turnaround time taken by staff in managing and auditing books of accounts is not optimal.

ii) Generation of reports using the current system is difficult. This makes making business decisions difficult.

iii) Ensuring security of patients’ medical records and test results is almost impossible. This is because almost all staff have access to the store where records are kept. Also when the paper files accumulate, they are often burnt to create space. This implies that records are often lost. Since in the current business world security is a must as by HIPPA there is a bleached here. Also, some clients retreat from accessing the facility for fear of what will happen if people get to know of their condition especially if media finds out that one has renown killer disease like HIV/AIDS

4.4 Requirements for the Proposed System

To derive the system requirements for the proposed system user centered design and the users of the system used paper prototyping methodologies to derive the system requirements.

4.4.1 Hardware Requirements

The new system requires minimum hardware requirements as listed below;

i) Processor: pentium4- 2.4 GHz (Core Duo Intel processor) or higher
ii) Memory: 1GB of RAM or higher
iii) Hard Drive 160GB or higher
iv) Monitor: 15inch and above
v) Backup devices: External hard drive, USB flash drive

4.4.2 Software requirements

The MLRS requires minimum software requirements as listed below;

i) Operating system: Windows xp and newer versions
ii) Databases: MySQL
iii) PHP
iv) Servers: MySQL server Browsers: Internet explorer, Mozilla Firefox, Google chrome, Opera, Safari and others.

4.4.3 Functional Requirements

This MLRS (medical laboratory record system) is developed to address security as the major objective. However, it is desirable to maintain a core set of functions in each EMR system in order to support similar workflows and encourage best practices in clinical care. This section details the functional requirements for EMR systems, including required and recommended capabilities The Use Cases section offers specific scenarios to demonstrate the applicability and use of these capabilities. The functional requirements defined in this section can be categorized into6 key functional areas that are critical to the definition of an EMR: (i) basic demographic and clinical health information ;(ii) clinical decision support; (iii) order entry and prescribing; (iv) health information and reporting; (v) security and confidentiality, and; (vi) exchange of electronic information.

Standards Referenced

This section references the following standards:

i) ISO /TR 20514: Health Informatics – Electronic Health Record – Definition, scope and context
ii) ISO/TS 22220: Health Informatics Identification of Subjects of health care
iii) HL7 Electronic Health Record – System Functional Model, Release 1 February 2007
iv) ISO/TS 18303: Health informatics — Requirements for an electronic health record architecture

v) CCHIT Certified 2009 EMR Certification Criteria

This section draws heavily on ISO 18303 specifications and the HL7 Reference Information Model (RIM); reference is also made to ISO TS 22220 in defining the identification of subjects of care (including the demographic details specifications). The section also reflects EMR requirements set forth by the Certification Commission for Health Information Technology (CCHIT), which are used in the United States in determining eligibility for federal funding. The list consists of functionality, interoperability, and security requirements that ensure EMR systems exchange data effectively, maintain confidentiality and provide necessary functionality. The defined functionalities may be used to develop a similar certification process to encourage standardization of EMR systems. Below are the functional requirements of the system. The system will:

i) Allow only authorized users to log in
ii) Capture processes and store patient information,
iii) Permit the querying of patient records by authorized users,
iv) Encrypt patient's records and will only be decrypted by authorized persons,
v) Allow users to view patient information as needed,
vi) Capture all data pertaining patient. This ranges from the registration details, the screening details, the patient‘s health treatment processes,
vii) Keep track of each client and the services provided to them,
viii) Check and eliminate duplicates so as to ensure data integrity and
ix) Register its users (staff of the laboratory).

4.4.5 Non-functional requirements

Non-functional requirements were also sought and this was aligned with intended users' responses. These requirements are described below.

i) The system should be easy to use with intuitive interfaces that prompt users.
ii) The system should be secure and password protected and the administrator can set criteria for users to access the system.
iii) The system should be able to run in the current window OS environment.
iv) The system should be able to handle multiple end-users thus web-based.

4.5 System Design

In this section, the researcher discusses how MLRS was designed from a basic paper prototype to the functional prototype. As discussed in the first section of this chapter, this part of the design process required the researcher to design an interactive system that enables staff members execute their roles. Therefore, a participatory design approach was used, in conjunction with paper prototypes. The next section, describes the process and results obtained after using this approach.

4.5.1 Procedure

PD sessions were conducted with the three different groups as discussed in the previous section. The participants were briefed about the overall objectives of the sessions and the goals to be accomplished. Then they were introduced to the paper prototyping technique in which the following aspects were highlighted as presented by (Snyder, 2003).

A meeting was scheduled with participants and stakeholders discussed how the project was going to be conducted. The concept of PD was also introduced and explained to the participants.

Participants were also informed that they were learning paper prototyping. They were further told that there is no right or wrong answer and were free to explore their creative side. The participants were briefed about the stationeries and materials used to develop paper prototypes. They were shown samples of paper prototypes in order to stimulate their design. The benefits and the positive aspects of paper prototyping were highlighted throughout the briefing, to convince skeptics and to encourage the participants to give their full commitments. Different group were required to come up with prototypes, where by end of the sessions, a number of requirements were elicited. All the members in each group collaboratively developed the prototypes

In the second step, the concept of user goals was explained to the participants. They were also reminded that they were the users and that they were developing a lab system. Thus since they are the users they know the lab activates and processes. They were asked to identify their needs for the system requirements.

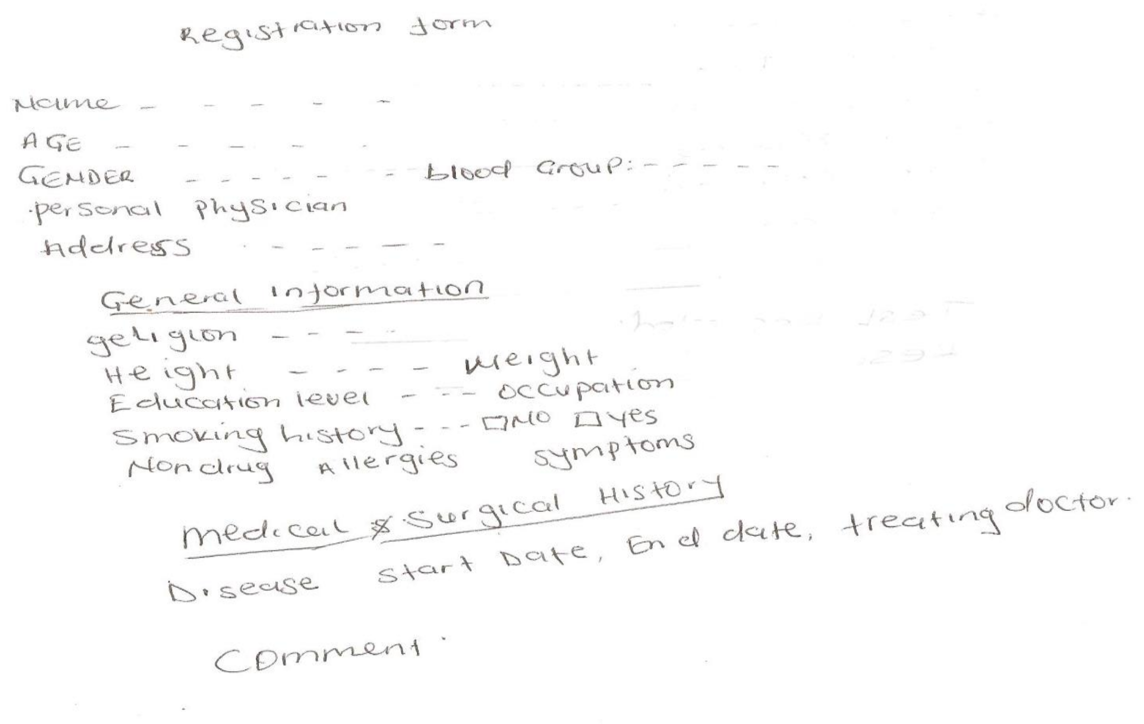
Next, they were asked to list a set of questions regarding the functionality, navigation and terminologies to be used in the prototype. They were also asked to prioritize activities although they all validated the idea that all activities were of equal importance. The researcher then guided the groups with sample prototypes showing activities (that simulate the requirements a lab system) in order to stimulate them to think about the system. They were required to practice basing on what they were provided. After each session, a walkthrough was done in order to identify any issues and for the participants to justify their choices. The groups then started developing the prototypes with the assistance of the researcher.

The facilitator presented the participants with storyboards showing activities (that simulate the production of a lab activities) in order to stimulate them to think in line with activity at hand. They were required to re-arrange them starting with the first activity to the last. After each session, a walkthrough (which is a rehearsal in which any problems can be detected and corrections made) was done in order to identify any issues and for the participants to justify their choices. The groups then started developing the prototypes with the assistance of the facilitator. This is the moment where they could explore their creative side to design the tool. Because they are busy and we only had 2 – 3 hours for each of the sessions, paper prototyping during the sessions helped in eliciting user goals and identifying requirements for our tool.

4.5.2 Paper prototype

At this stage the main goal was not to come up with a complete tool as each participant only afforded to draft two or three incomplete screens. Therefore, this study does not undertake PD in the strictest sense (as that would require longer multiple sessions working towards a final agreed design) but facilitates opening up of the design space and uncovering a number of crucial requirements Figure 4.5 below illustrates an example of the prototype elements that were created by the participants.

4.5.1 paper moving to requirement design



Registration form

Name - - - - -

AGE - - - - -

GENDER - - - - - - - blood Group:- - - - -

·personal physician

Address - - - - -

General information

geligion - - - -

Height - - - - Weight

Education level - -- occupation

Smoking history - - - □NO □yes

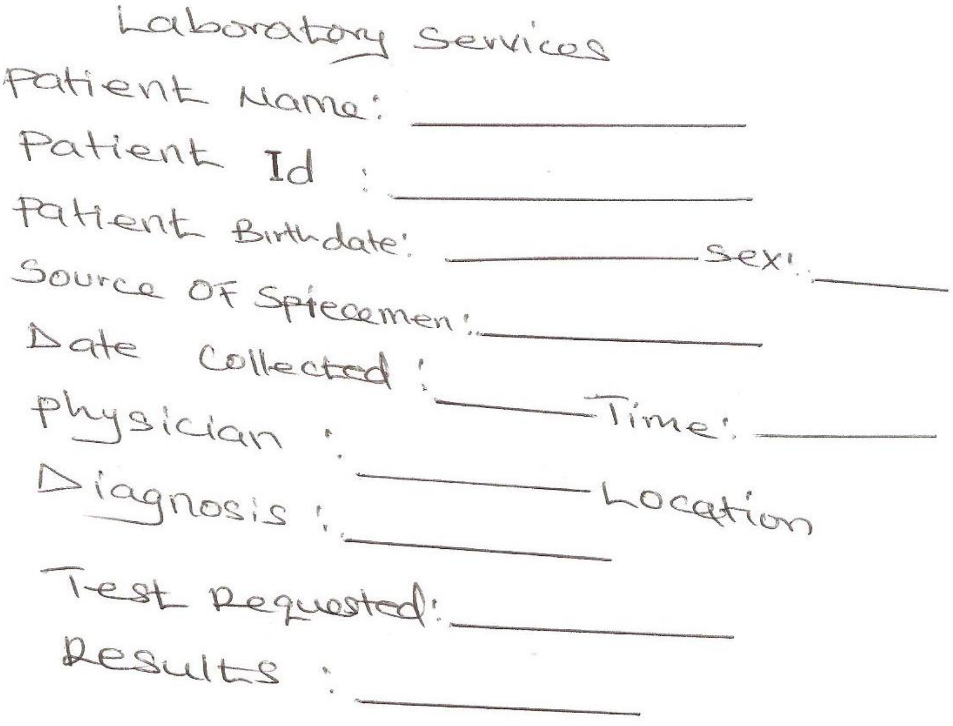
Nondrug Allergies symptoms

Medical & Surgical History

Disease start Date, End date, treating doctor.

Comment·

Figure 4.5: prototypes for patients registration



Laboratory Services

Patient Name: ____________

Patient Id : ____________

Patient Birthdate: ________ sex: ______

Source Of Spiecemen: ____________

Date Collected : ______ Time: ______

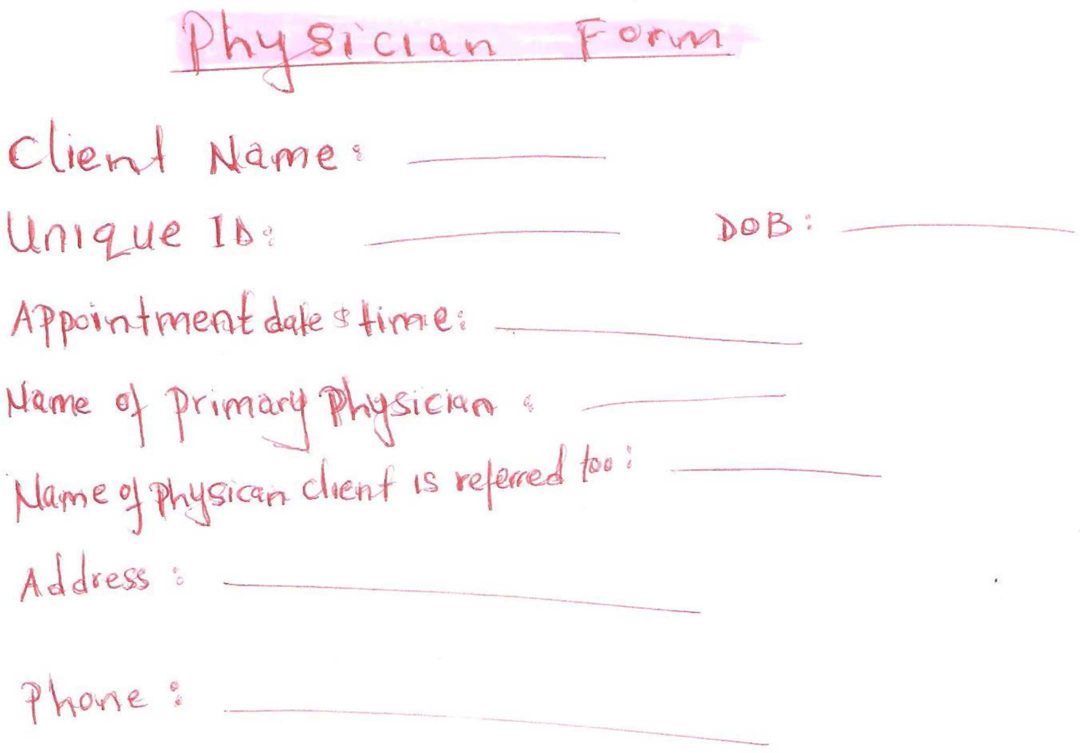
physician : ________ Location

Diagnosis : ________

Test Requested: ____________

Results : ____________

Figure 4.6 Prototype for laboratory services



Physician Form

Client Name: ____________

Unique ID: ____________ DOB: ____________

Appointment date & time: ____________

Name of Primary Physician: ____________

Name of Physican client is referred too: ____________

Address: ____________

Phone: ____________

Figure 4.7: Prototype for physician form

4.5.3 Results of the Design Session

As a result, several issues were identified with the prototypes including incomplete interfaces, missing links, failure to generate tasks and the reluctance from one of the participants to sketch solutions. The screen designs produced during the design activity revealed a trend towards simplicity. There was a need to strike a balance between functionality and the number of steps to accomplish the task. The researcher verified the assumptions about what users minimally expected on the tool record, capture screen shot, preview, edit, publish and modify settings.

In this light, the participants raised a lot of wary of the security, authenticity and user friendliness of the system. This guided the researcher on the methods to choose to implement the system. In the next section system models using UML are presented. The systems architecture and implementation is also performed. This is obtained from the findings provided in this section.

4.6 System models

This section presents the system models that where derived as a result of the functional and nonfunctional requirement. Unified Modeling Language (UML) was used as presented in the sections that follow.

4.6.1 Use Case Diagram

Use case diagram illustrates a unit of functionality provided by the system. The main purpose of the use-case diagram is to help the researcher visualize the functional requirements of a system including the relationship of actors (people who will interact with the system) to essential processes as well as the relationships among different use cases. To show a use case on a use case diagram, an oval is drawn in the middle of the diagram and the name of the use case put in the center of or below the oval. To draw an actor indicating a system user on a user case diagram, a stick person is drawn to the left or right of your diagram.

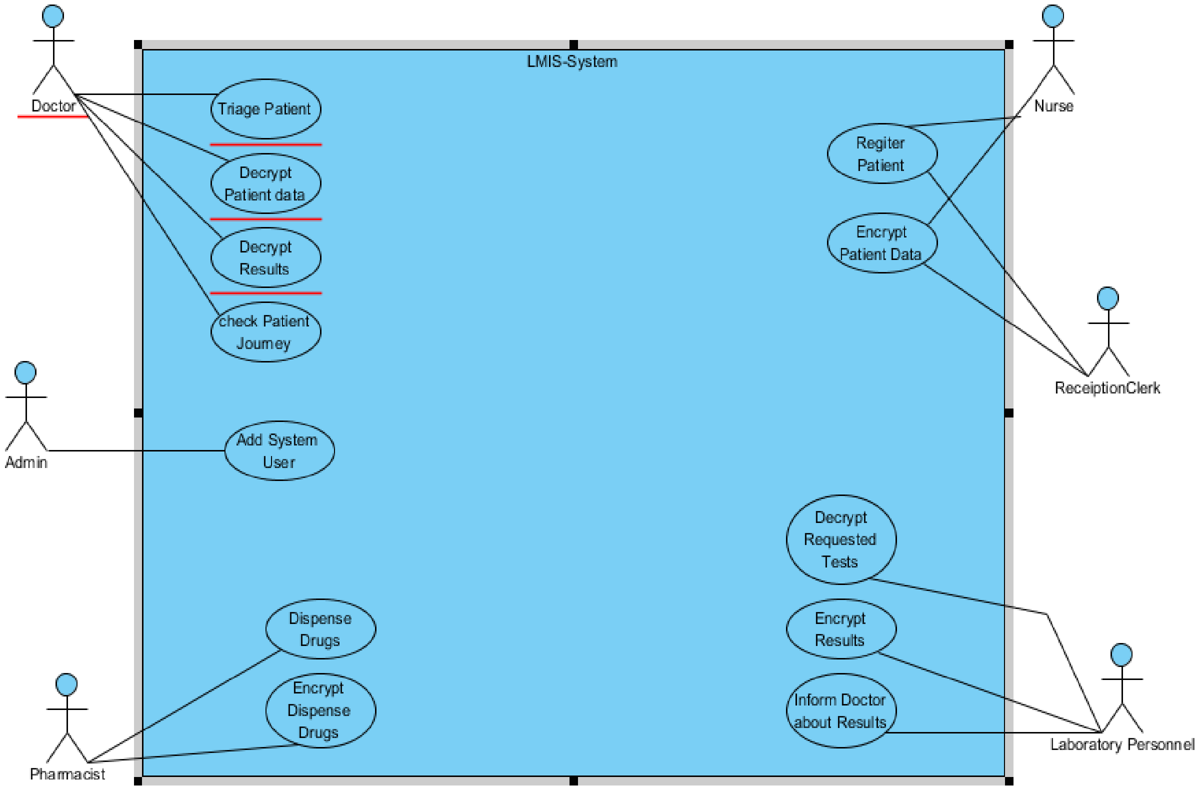


Figure 4.7: Use Case Diagram

4.6.2 Systems Architecture

The implementation runs on a three-tier architecture. Three tiers simply means there is enforcement of separation between the following three parts. These are Client Tier, Middle Tier business logic and the Data Storage Tier.

4.6.2.1 The Client tier

At the client/browser side there are two kinds of users, the administrator and the authorized users. The administrator is responsible for adding critical data to the system, the type of data is like the user' and their roles, username and password for any other Administrators, viewing of the clients medical results. The application is web based and can be accessed by the administrator through the web browser. But, both the system users access the application through the web application hence share the same database. The second user is the organization administrator. The role of this person is to be able to login in order to be eligible to use the system. The privilege to access the system is given by the Administrator. The interface accessed by the users in a web form.

4.6.2.2 Middle Tier

The middle tier will contain the core parts of the MLRS application, i.e., the web server and business logic. The web server will handle all requests coming from the client machines. The requests are different with its type, for example; request for data insertion, request for report generation and others. It is also the web server, which manages the responses that is forwarded to the client machines. The business logic part will hold the process and core functions that will be implemented in the system. When the data is submitted from the client machines, first it will be handled by the functions of the web server and then transferred to the business logic for processing. Again, the business logic processes the data and sends it either to the database or back to the web server, this is determined by the type of service required.

4.6.2.3 Data Tier

The system uses one single database. The database stores information about Voters. This database is not part of the system; it is referred from an external system. It stores patients' information like patient number, which is a unique number that is used for identifying patients in the system. The application can also benefit from this for identifying voters uniquely.

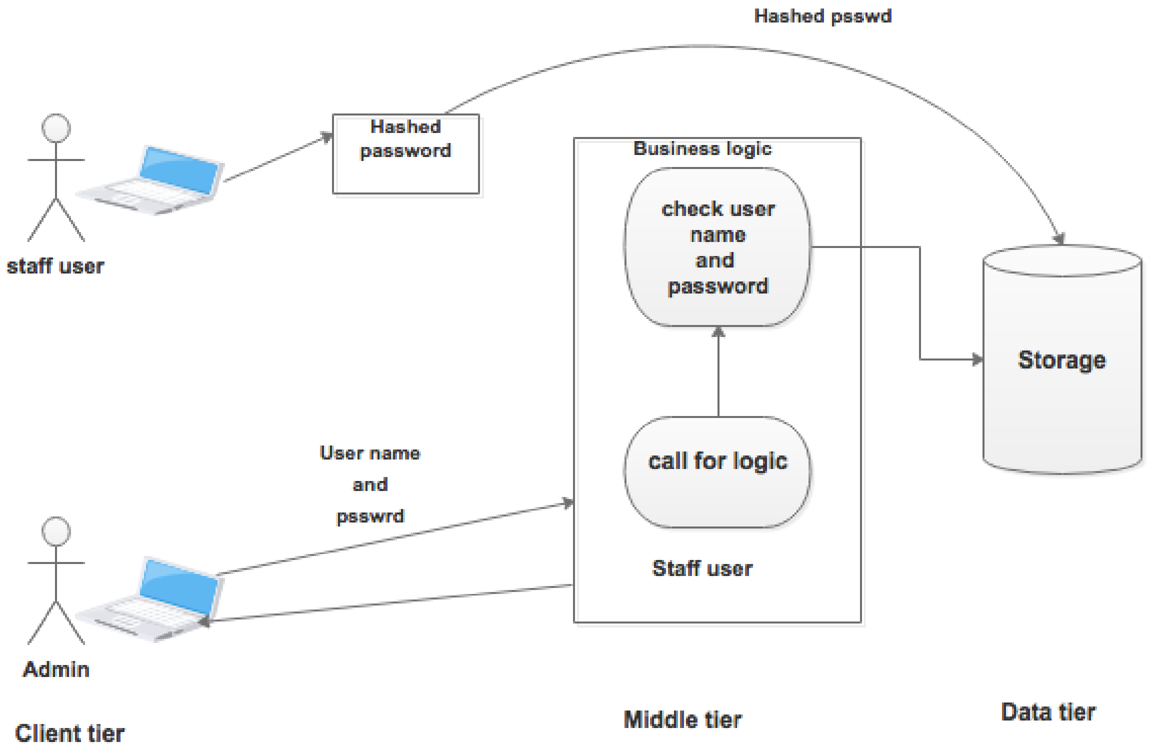


Figure 4.8: Client Server Architecture Pictorial

4.6.3 Activity diagrams

Activity diagrams were used to show how activities of the flow in the system. The figure 4.5 below shows the registration process and figure 4.6 shows the lab activity.

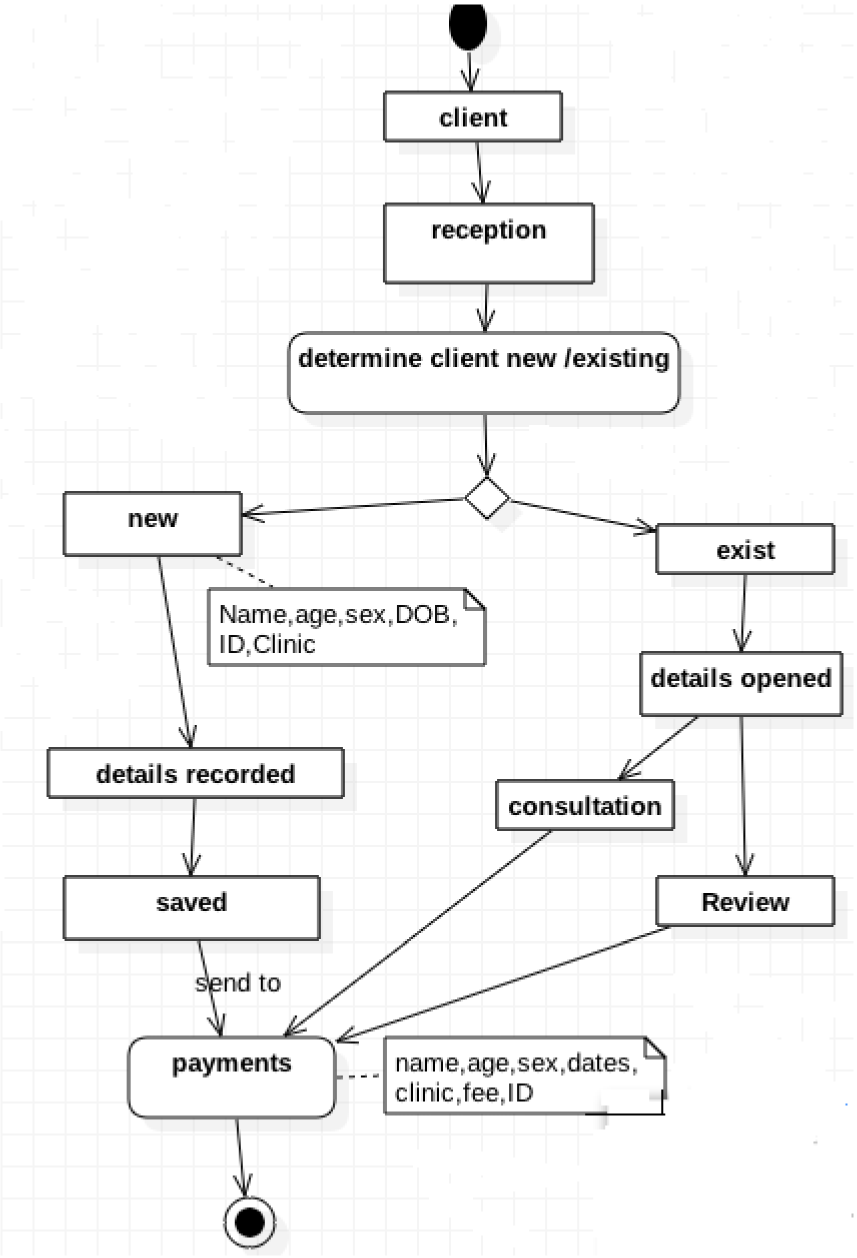


Figure 4.9: Activity Diagram for Registration

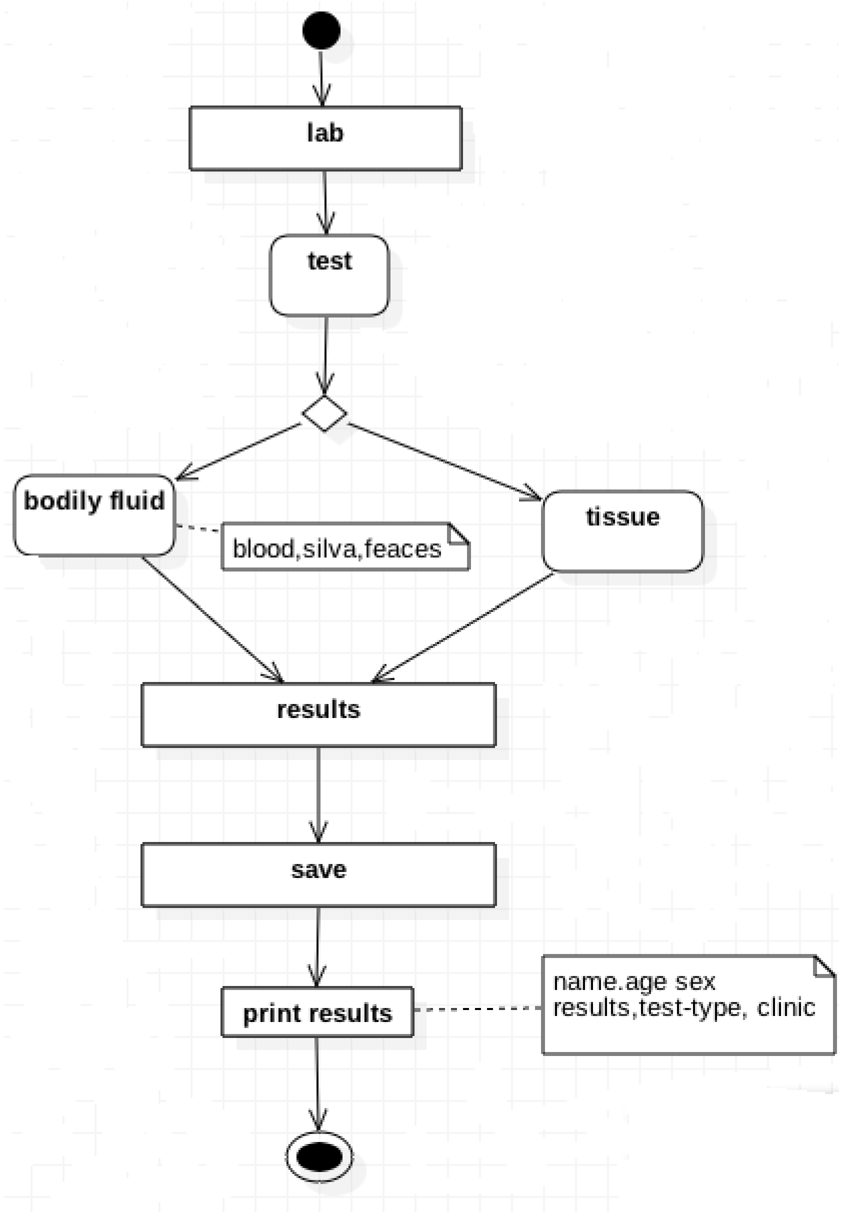


Figure 4.10: Activity Diagram for lab activity

4.7 Database Design

The database consists of several tables. The tables are used for storing the attributes of actors as illustrated by use case and clients' particulars.

4.7.1 Entity Relationship Diagram

The ER diagram represents all the entities that make up the system it highlights all entities, attributes and their associations. Its gives critical analysis of the database to avoid redundancy and build a data model that will result in a database that is flexible and can be extended.

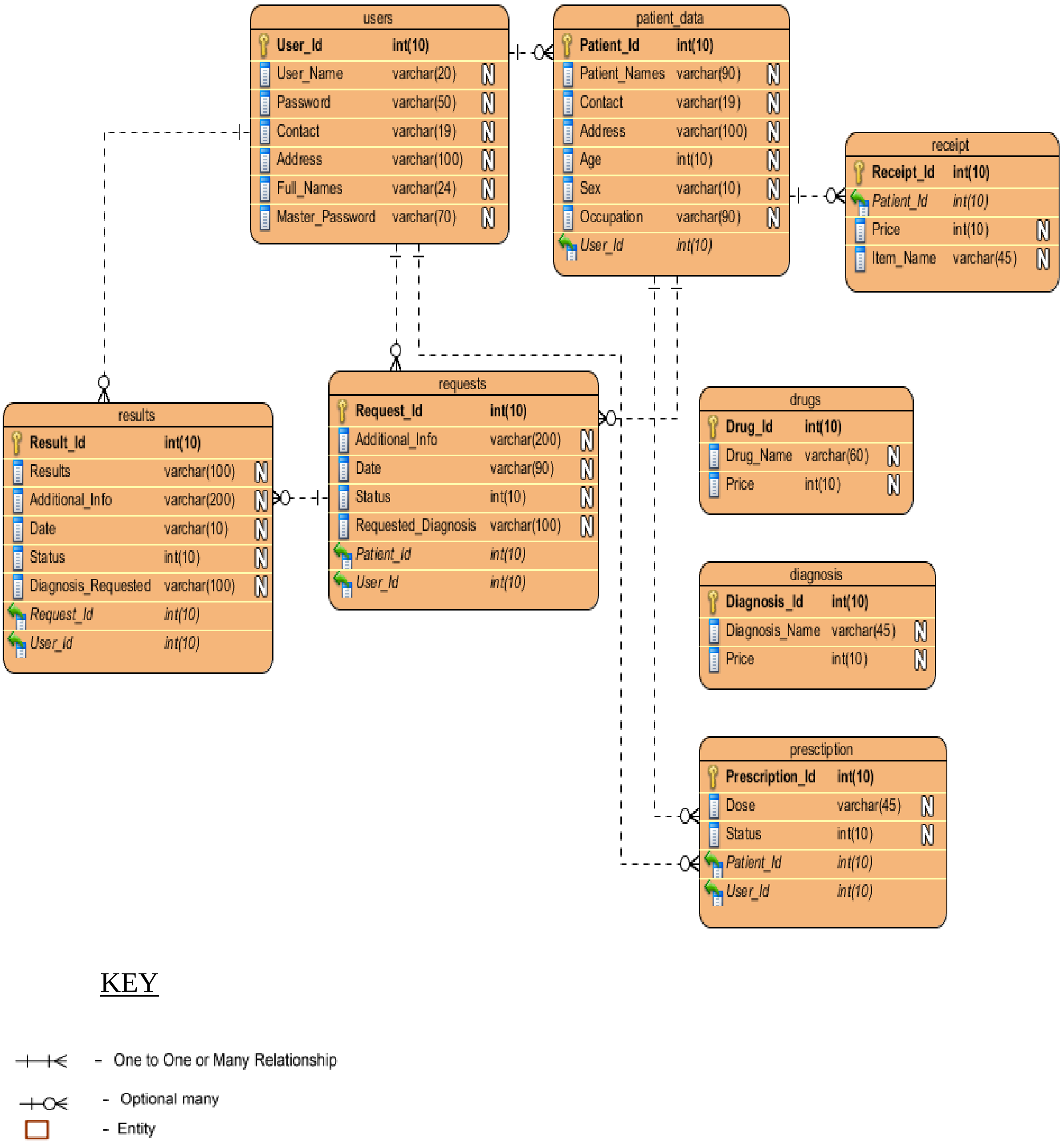


Figure 4.11: Entity Relationship Diagram for the System

4.7.2 Physical Database Design

This involved the actual design of that database according to the requirements that were established during logical modelling. It involves transforming the logical design into database schemas.

4.7.2.1 Data Dictionary

This section gives detailed information on the various tables that were used to develop the database, including the fields, data types and any other constraints on the fields.

Table 4.7: Data Dictionary

<table>
<tr><th>Table Name</th><th>Description</th><th>Column Details</th></tr>
<tr><td><b>Users</b></td><td>This table contains information about the users of the system. It contains information about the staff in the labaratory.</td><td>
<table>
<tr><th>Name</th><th>DataType</th><th>Constraints</th><th>Nullable</th><th>Documentation</th></tr>
<tr><td>User_Id</td><td>int(10)</td><td>PK</td><td>No</td><td></td></tr>
<tr><td>User_Name</td><td>varchar(20)</td><td></td><td>Yes</td><td></td></tr>
<tr><td>Password</td><td>varchar(50)</td><td></td><td>Yes</td><td></td></tr>
<tr><td>Contact</td><td>varchar(19)</td><td></td><td>Yes</td><td></td></tr>
<tr><td>Address</td><td>varchar(100)</td><td></td><td>Yes</td><td></td></tr>
<tr><td>Full_Names</td><td>varchar(24)</td><td></td><td>Yes</td><td></td></tr>
<tr><td>Master_Password</td><td>varchar(70)</td><td></td><td>Yes</td><td></td></tr>
</table>
</td></tr>
<tr><td><b>Patient data</b></td><td>This table contains information registered about the patients.</td><td>
<table>
<tr><th>Name</th><th>DataType</th><th>Constraints</th><th>Nullable</th><th>Documentation</th></tr>
<tr><td>Patient_Id</td><td>int(10)</td><td>PK</td><td>No</td><td></td></tr>
<tr><td>Patient_Names</td><td>varchar(90)</td><td></td><td>Yes</td><td></td></tr>
<tr><td>Contact</td><td>varchar(19)</td><td></td><td>Yes</td><td></td></tr>
</table>
</td></tr>
</table>

Table Name	**Description**	**Column Details**				
		Address	varchar(100)		Yes	
		Age	int(10)		Yes	
		Sex	varchar(10)		Yes	
		Occupation	varchar(90)		Yes	
		User_Id	int(10)	FK (users. User_Id)	No	
Receipt	This table contains information about payments made by the patients.	**Name**	**DataType**	**Constraints**	**Nullable**	**Documentation**
		Receipt_Id	int(10)	PK	No	
		Patient_Id	int(10)	FK (patient_data.Patient_Id)	No	
		Price	int(10)		Yes	
		Item_Name	varchar(45)		Yes	

<table>
<tr><th>Table Name</th><th>Description</th><th>Column Details</th></tr>
<tr><td><b>Results</b></td><td>This table contains results of tests carried out.</td><td>
<table>
<tr><th>Name</th><th>DataType</th><th>Constraints</th><th>Nullable</th><th>Documentation</th></tr>
<tr><td>Result_Id</td><td>int(10)</td><td>PK</td><td>No</td><td></td></tr>
<tr><td>Results</td><td>varchar(100)</td><td></td><td>Yes</td><td></td></tr>
<tr><td>Additional_Info</td><td>varchar(200)</td><td></td><td>Yes</td><td></td></tr>
<tr><td>Date</td><td>varchar(10)</td><td></td><td>Yes</td><td></td></tr>
<tr><td>Status</td><td>int(10)</td><td></td><td>Yes</td><td></td></tr>
<tr><td>Diagnosis_Requested</td><td>varchar(100)</td><td></td><td>Yes</td><td></td></tr>
<tr><td>Request_Id</td><td>int(10)</td><td>FK (requests.Request_Id)</td><td>No</td><td></td></tr>
<tr><td>User_Id</td><td>int(10)</td><td>FK (users.User_Id)</td><td>No</td><td></td></tr>
</table>
</td></tr>
<tr><td><b>Requests</b></td><td>This table holds information about requests for laboratory</td><td>
<table>
<tr><th>Name</th><th>DataType</th><th>Constraints</th><th>Nullable</th><th>Documentation</th></tr>
<tr><td>Request_Id</td><td>int(10)</td><td>PK</td><td>No</td><td></td></tr>
</table>
</td></tr>
</table>

Table Name	**Description**	**Column Details**				
	tests including the patient ID of the patient on whom the tests are conducted.	Additional_Info	varchar(200)		Yes	
		Date	varchar(90)		Yes	
		Status	int(10)		Yes	
		Requested_Diagnosis	varchar(100)		Yes	
		Patient_Id	int(10)	FK (patient_data.Patient_Id)	No	
		User_Id	int(10)	FK (users.User_Id)	No	
Drugs	This gives the details of available drugs	**Name**	**DataType**	**Constraints**	**Nullable**	**Documentation**
		Drug_Id	int(10)	PK	No	
		Drug_Name	varchar(60)		Yes	
		Price	int(10)		Yes	

4.8 Networks and System Architecture

On a client/server network, every computer has a distinct role: that of either a client or **a** server. A server is designed to share its resources among the client computers on the network. Typically, server is located in secured areas, such as locked closets or data centers (server rooms), because it holds an organization's most valuable data and do not have to be accessed by operators on a continuous basis. The rest of the computers on the network are clients.

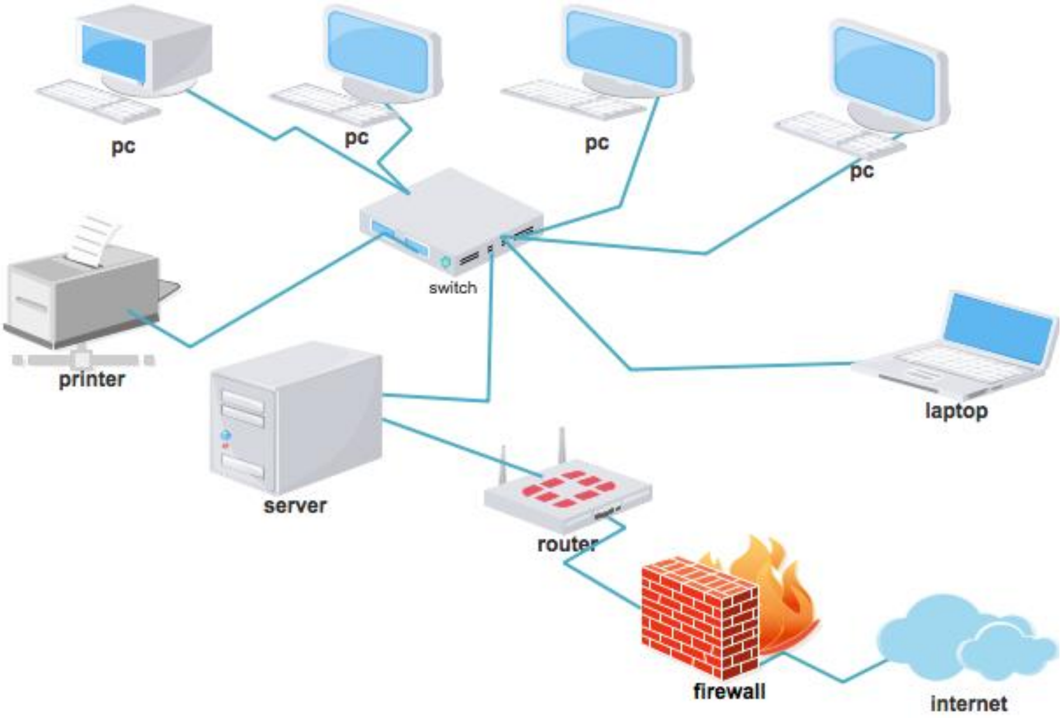


Figure 4.14: System/Network Architecture

A dedicated server computer has faster processors, more memory, and more storage space than a client because it might have to service different users at the same time. High-performance servers typically use from two processors (and that's not counting multi-core CPUs), have many gigabytes of memory installed, and have one or more server-optimized network interface cards (NICs**)**, RAID (Redundant Array of Independent Drives) storage consisting of multiple drives, and redundant power supplies. Servers often run a special network operating system (OS) Windows Server that is designed solely to facilitate the sharing of its resources. These resources reside on a single server. A client computer typically communicates only with servers, not with other clients. A client system is a standard PC that is running OS (windows Eights). Current operating systems contain client software that enables the client computers to access the resources that servers share. Older OS's, such as Windows 3.x and DOS, required add-on network client software to join a network.

The Internet plays a vital role of files sharing that are on the networks. These files can be accessed by doctors online from the different location can remotely logon to the systems via their user accounts consult on the patients medical records and recommend the treatment. The Internet in this case has its dangers associated with it and that's why in this system the researcher recommends encryption to protect the records from illegal access. The system has to be protected by the firewall to filter traffic.

Conclusion

In this chapter findings from the data collected was analyzed and presented. A discussion on the current system considering the data inputs and data outputs was also discussed. Current business processes, project designing presented with context data flow diagrams, paper prototyping and use case. Still under this chapter, a discussion of the ERD and Data structure, current system problems, and system requirements was also presented. In the following chapter, we shall discuss the proposed system design.

CHAPTER FIVE

SYSTEM IMPLEMENTATION

5.1 Introduction

This chapter entails the implementation of the designs to realize the physical database and the system. This section describes about the implementation of the product in two sections. The first section explains about the development tool, and the second section describes the system developed.

5.2 Development tools

The development tools used in this section are described in two categories; the first section describes about the development and programming tools and the second part specifically describes about the security tools.

5.2.1 Development environment

The programming language used to run this program is Php verson 5.2.5. Php is a server side scripting language hence provides for a thin client. Php is open source hence cross platform. PHP 5 has got new features such as improved support for object-oriented programing, the PHP Data Objects (PDO) extension (which defines a lightweight and consistent interface for accessing databases.

5.2.2 The application server

WAMP server 2.0 was selected for this project because it was readily available and since it implements in a windows platform, which is the most commonly used by most computers. However, the system can be accessed by different operating systems such as MAC Systems and Linux i.e it is open source and cross platform. Another consideration was based on a fact that databases and applications developed using WAMP can always be upgraded to newer versions with minimal changes. WAMP is an integrated development environment comes packaged with MYSQL and Apache server and a PHP preprocessor. MySQL has some better qualities which makes it preferable compared to the others relational database management systems. It is multithreaded, multi-user database management system, supports all known platforms including Windows-based platforms, requires less hardware resource for storage as well as for execution, much faster, supports Unicode character storage and more than that, it has free version product.

5.2.3 Data Base Implementation

The database management system used was MySQL. WAMP server interface was used to create the database and all tables. All tables have primary keys and where necessary, there are foreign keys to ensure data integrity. Below is a screen shot of the lab_db in PHP MyAdmin showing the database and its tables.

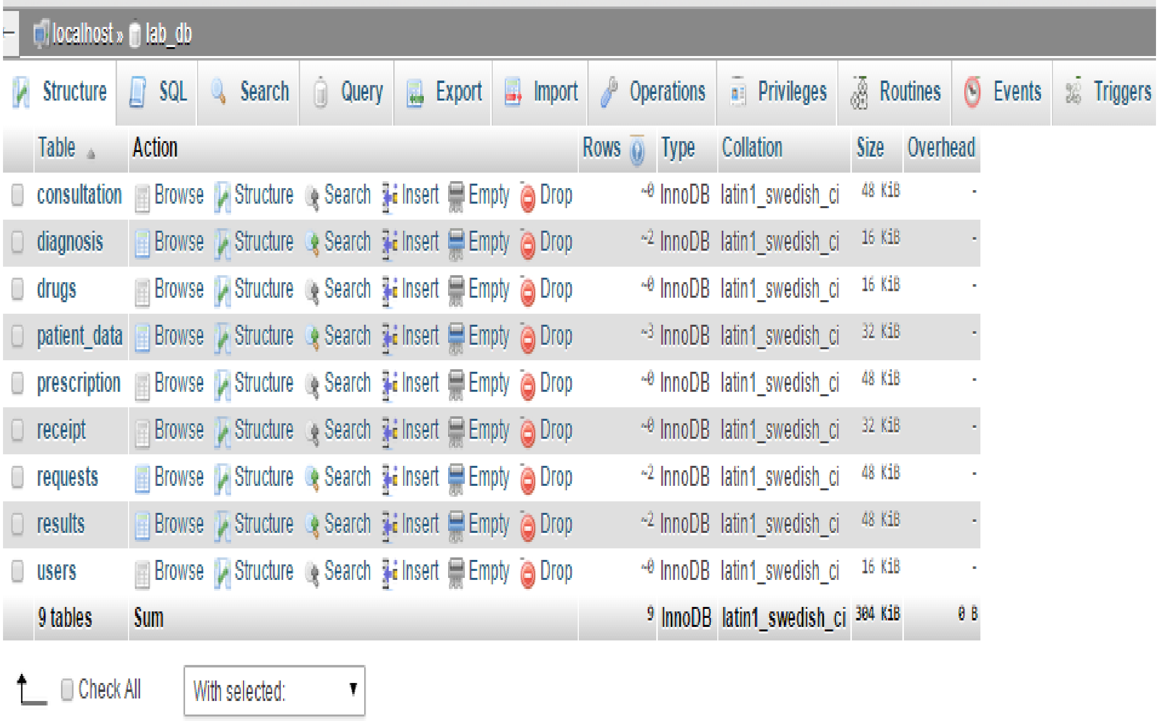


Table	Action						Rows	Type	Collation	Size	Overhead
□ consultation	Browse	Structure	Search	Insert	Empty	Drop	~0	InnoDB	latin1_swedish_ci	48 KiB	-
□ diagnosis	Browse	Structure	Search	Insert	Empty	Drop	~2	InnoDB	latin1_swedish_ci	16 KiB	-
□ drugs	Browse	Structure	Search	Insert	Empty	Drop	~0	InnoDB	latin1_swedish_ci	16 KiB	-
□ patient_data	Browse	Structure	Search	Insert	Empty	Drop	~3	InnoDB	latin1_swedish_ci	32 KiB	-
□ prescription	Browse	Structure	Search	Insert	Empty	Drop	~0	InnoDB	latin1_swedish_ci	48 KiB	-
□ receipt	Browse	Structure	Search	Insert	Empty	Drop	~0	InnoDB	latin1_swedish_ci	32 KiB	-
□ requests	Browse	Structure	Search	Insert	Empty	Drop	~2	InnoDB	latin1_swedish_ci	48 KiB	-
□ results	Browse	Structure	Search	Insert	Empty	Drop	~2	InnoDB	latin1_swedish_ci	48 KiB	-
□ users	Browse	Structure	Search	Insert	Empty	Drop	~0	InnoDB	latin1_swedish_ci	16 KiB	-
9 tables	Sum						9	InnoDB	latin1_swedish_ci	304 KiB	0 B

□ Check All   With selected: ▾

Figure 5.1: Structure of lab_db in PHP MyAdmin

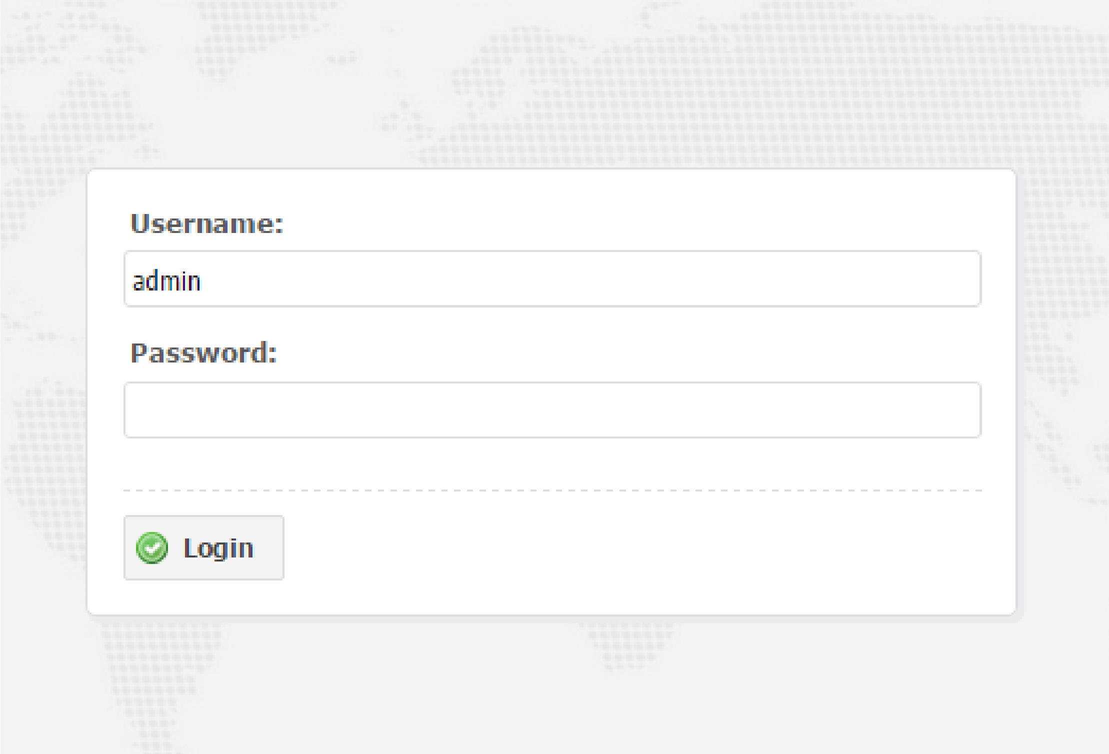
MySQL DBMS was used to create the lab database. To ensure reduction in redundancy and improve data integrity, tables were normalized by use of ―Primary keys to uniquely identify each entry in the database and the ―foreign key to show the relationships by linking different tables. In order to test the integrity of the database design, attempts were made to enter erroneous data into the database to ensure that the correct data types were recognized. Below is a sample of how the data appears at the backend of the database.

5.3 User Interface and System Reporting

For the user interfaces/front end and business logic, PHP CSS, java scripts and Ajax were used as the programming language embedded in HTML. Sample forms developed discussed and shown in the subsections that follow.

5.3.1 Admin login form

The administrator has all rights to change users password and user names its. And it’s the admin responsible for registering system users. The administrator login form is shown below



Username: admin

Password:

Figure 5.2: The Log in Form

Access to the system will only be to members registered on the system. They will have to login using the same login form; which queries for the username and password of the user. Below is a sample design of the login form.

5.3.2 User Registration Form

The systems administrator must register all system users before they can use the system. The users are also assigned roles by indicating the user type as shown in the figure below. In the user registration form

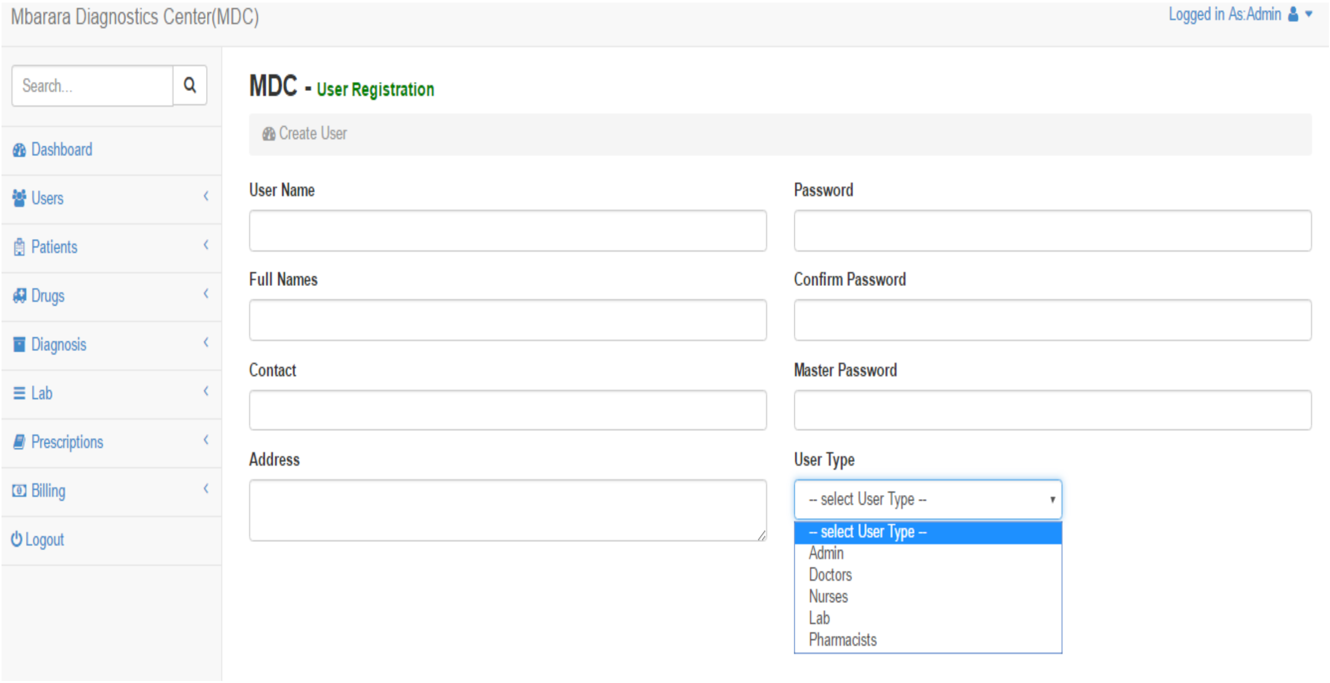


Figure 5.3: User Registration Form

5.3.3 Patient Registration Form

This is used to capture patient details into the system the first time they visit the clinic. It helps in putting data into the database. Below is the patient registration form

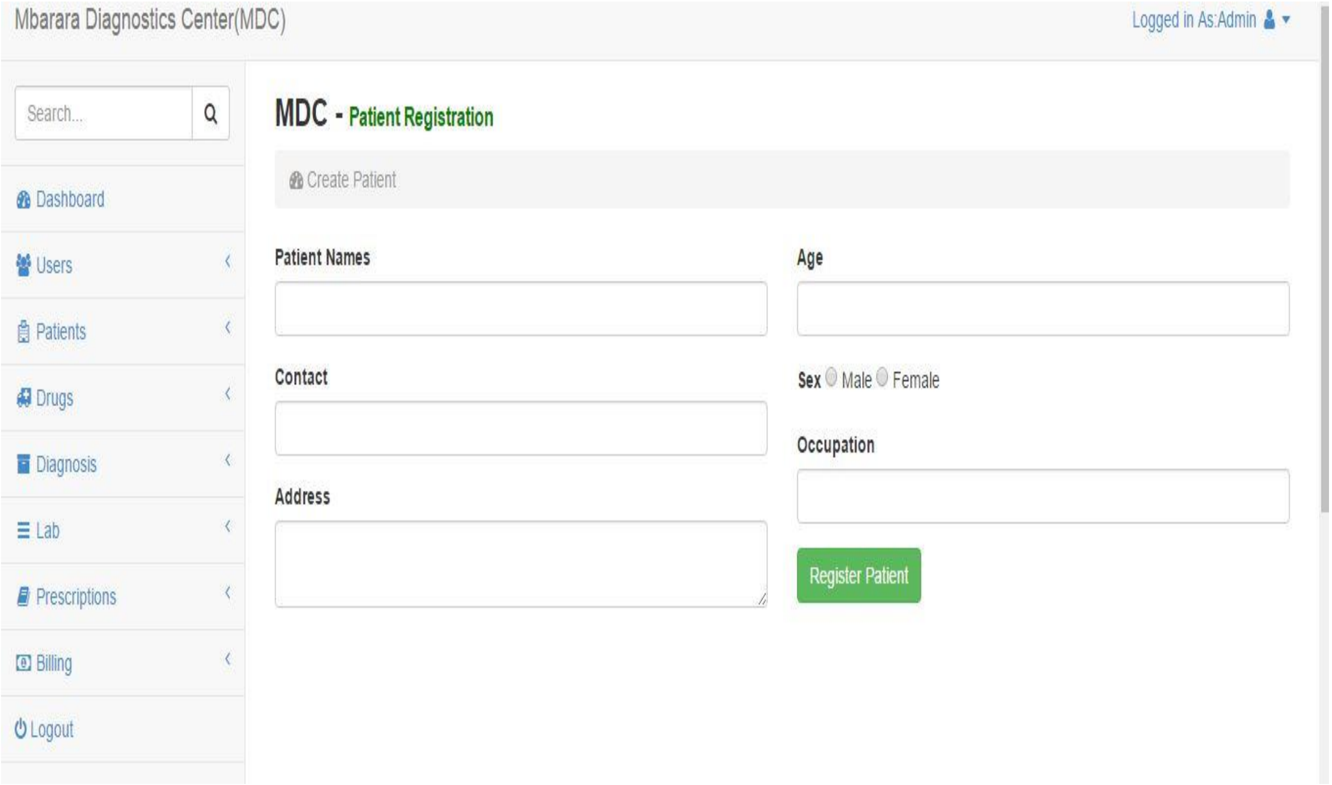


Figure 5.4: Patient Registration Form

5.3.4 Request for Diagnosis

This form is used to for request diagnosis. It indicates the tests that are supposed to be carried out on a particular patient.

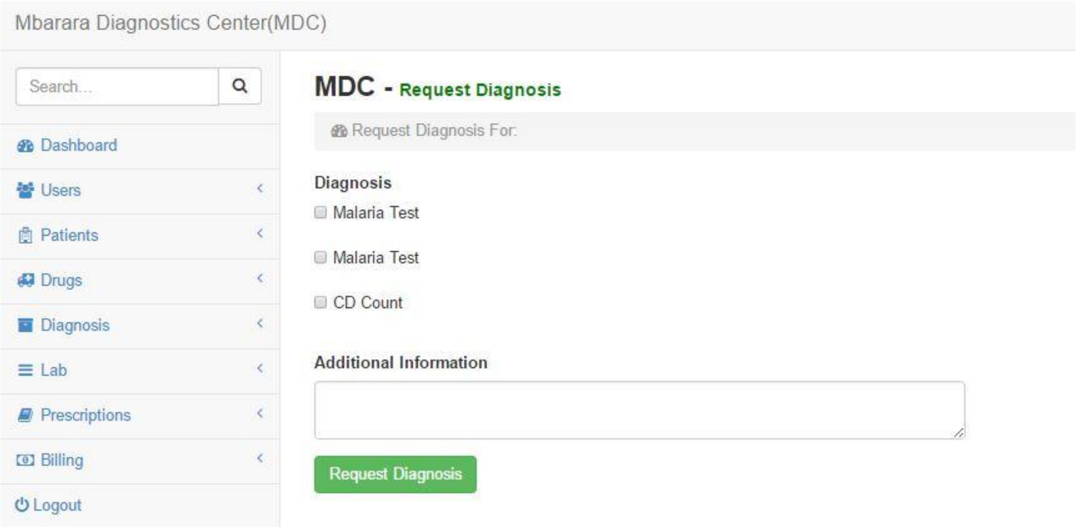
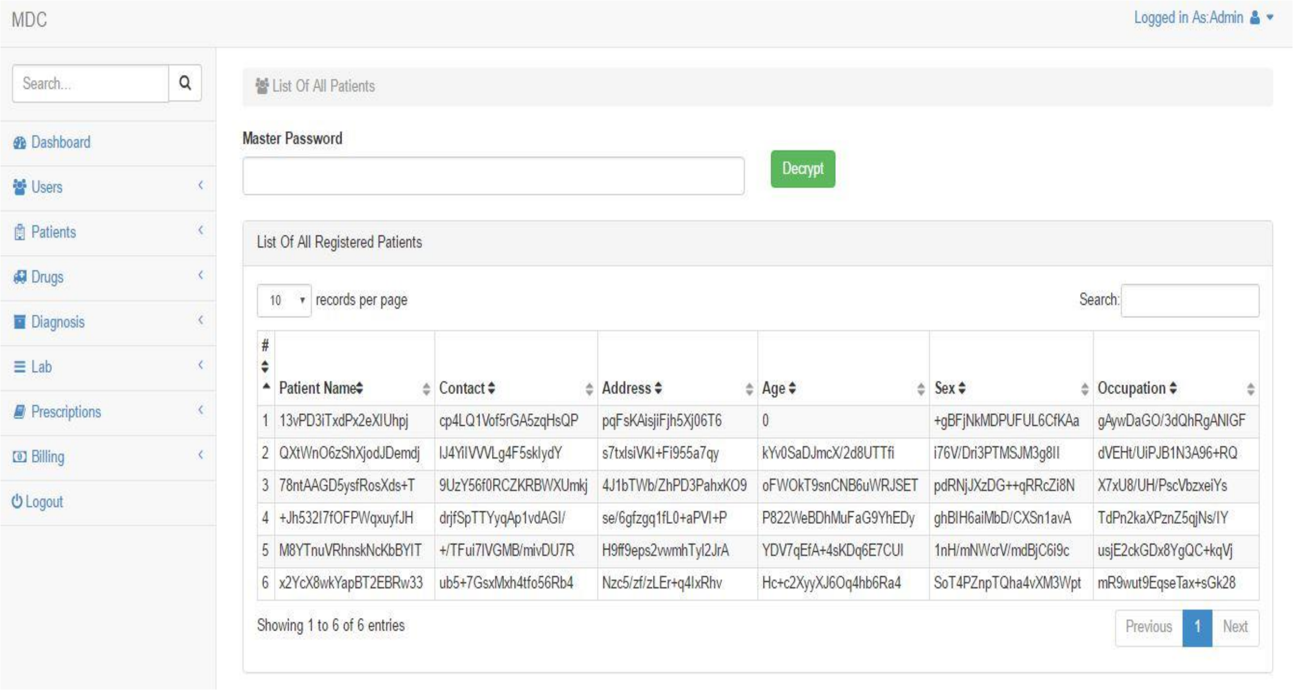


Figure 5.5: Form for Diagnosis Request

5.3.5 Patient Report with encrypted data

When a user request for patient information, it is presented in an encrypted format.



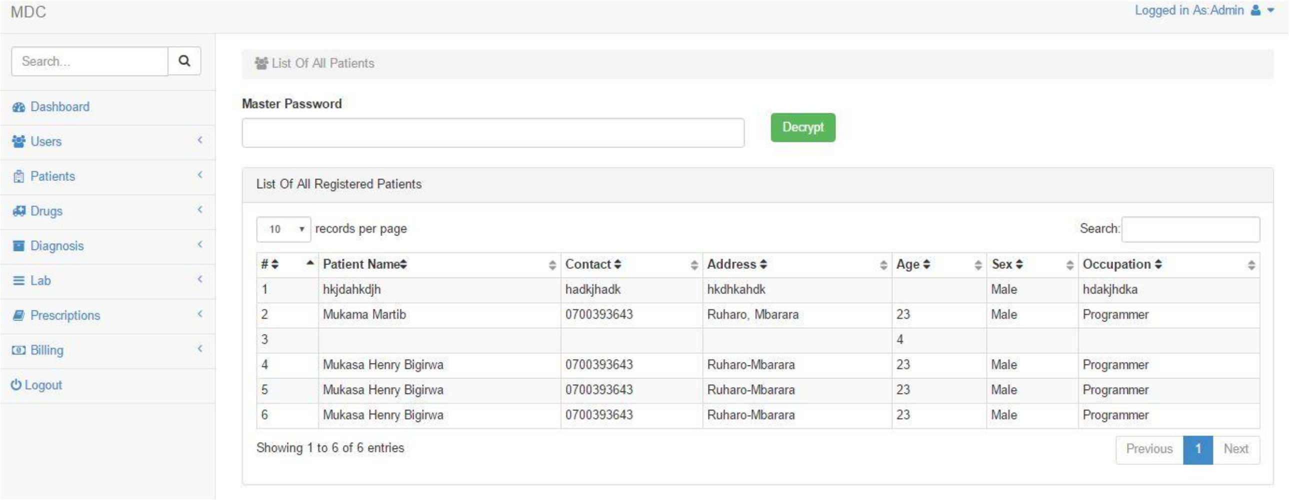
#	Patient Name	Contact	Address	Age	Sex	Occupation
1	13vPD3iTxdPx2eXIUhpj	cp4LQ1Vof5rGA5zqHsQP	pqFsKAisjiFjh5Xj06T6	0	+gBFjNkMDPUFUL6CfKAa	gAywDaGO/3dQhRgANIGF
2	QXtWnO6zShXjodJDemdj	lJ4YiIVVVLg4F5skIydY	s7txlsiVKI+Fi955a7qy	kYv0SaDJmcX/2d8UTTfi	i76V/Dri3PTMSJM3g8Il	dVEHt/UiPJB1N3A96+RQ
3	78ntAAGD5ysfRosXds+T	9UzY56f0RCZKRBWXUmkj	4J1bTWb/ZhPD3PahxKO9	oFWOkT9snCNB6uWRJSET	pdRNjJXzDG++qRRcZi8N	X7xU8/UH/PscVbzxeiYs
4	+Jh532I7fOFPWqxuyfJH	drjfSpTTYyqAp1vdAGI/	se/6gfzgq1fL0+aPVI+P	P822WeBDhMuFaG9YhEDy	ghBIH6aiMbD/CXSn1avA	TdPn2kaXPznZ5qjNs/IY
5	M8YTnuVRhnskNcKbBYIT	+/TFui7IVGMB/mivDU7R	H9ff9eps2vwmhTyl2JrA	YDV7qEfA+4sKDq6E7CUI	1nH/mNWcrV/mdBjC6i9c	usjE2ckGDx8YgQC+kqVj
6	x2YcX8wkYapBT2EBRw33	ub5+7GsxMxh4tfo56Rb4	Nzc5/zf/zLEr+q4IxRhv	Hc+c2XyyXJ6Oq4hb6Ra4	SoT4PZnpTQha4vXM3Wpt	mR9wut9EqseTax+sGk28

Showing 1 to 6 of 6 entries

Figure 5.6: List of registered Patient in encrypted Format

5.3.6 Patient Information report after decryption

In order to view the patient information in an understandable format, the user should provide the master password to decrypt the information. The figure below shows the patients details after decryption.



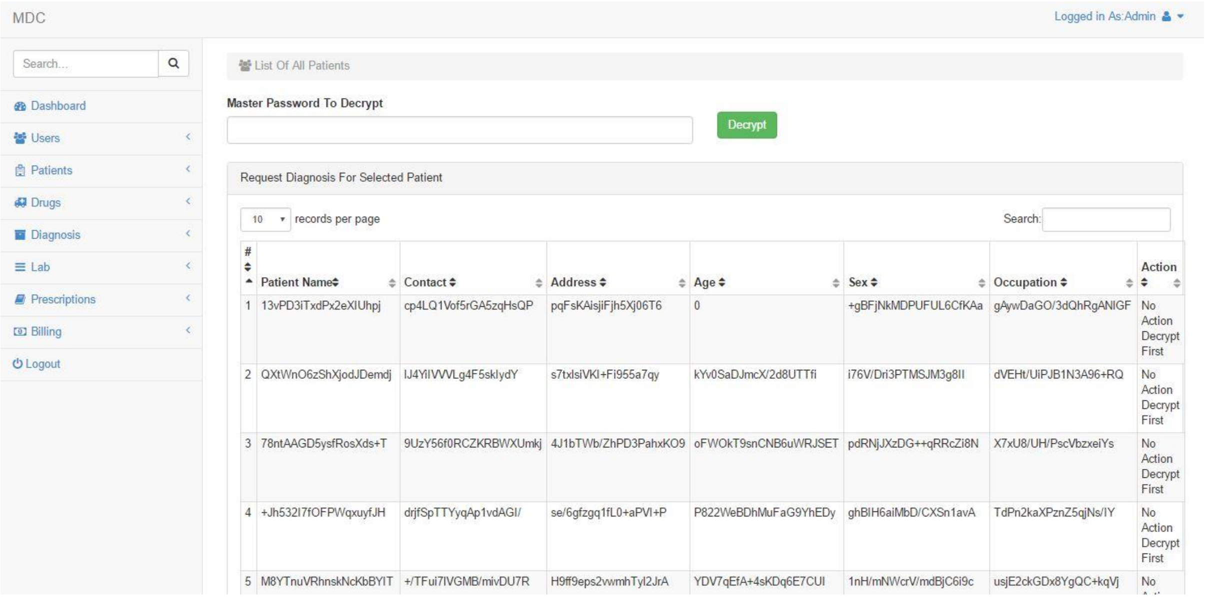
#	Patient Name	Contact	Address	Age	Sex	Occupation
1	hkjdahkdjh	hadkjhadk	hkdhkahdk		Male	hdakjhdka
2	Mukama Martib	0700393643	Ruharo, Mbarara	23	Male	Programmer
3				4		
4	Mukasa Henry Bigirwa	0700393643	Ruharo-Mbarara	23	Male	Programmer
5	Mukasa Henry Bigirwa	0700393643	Ruharo-Mbarara	23	Male	Programmer
6	Mukasa Henry Bigirwa	0700393643	Ruharo-Mbarara	23	Male	Programmer

Showing 1 to 6 of 6 entries

Figure 5.7: Results after decryption

5.3.7 Requesting for results of a particular patient

In order to view test results of a particular patient, the user is required to provide a master password to decrypt the data otherwise the data will be presented in an **encrypted** format as shown in the figure below.



Master Password To Decrypt

Request Diagnosis For Selected Patient

10 records per page

Search:

#	Patient Name	Contact	Address	Age	Sex	Occupation	Action
1	13vPD3iTxdPx2eXIUhpj	cp4LQ1Vof5rGA5zqHsQP	pqFsKAisjiFjh5Xj06T6	0	+gBFjNkMDPUFUL6CfKAa	gAywDaGO/3dQhRgANIGF	No Action Decrypt First
2	QXtWnO6zShXjodJDemdj	lJ4YiIVVVLg4F5sklydY	s7txlsiVKI+Fi955a7qy	kYv0SaDJmcX/2d8UTTfi	i76V/Dri3PTMSJM3g8II	dVEHt/UiPJB1N3A96+RQ	No Action Decrypt First
3	78ntAAGD5ysfRosXds+T	9UzY56f0RCZKRBWXUmkj	4J1bTWb/ZhPD3PahxKO9	oFWOkT9snCNB6uWRJSET	pdRNjJXzDG++qRRcZi8N	X7xU8/UH/PscVbzxeiYs	No Action Decrypt First
4	+Jh532I7fOFPWqxuyfJH	drjfSpTTYyqAp1vdAGI/	se/6gfzgq1fL0+aPVI+P	P822WeBDhMuFaG9YhEDy	ghBIH6aiMbD/CXSn1avA	TdPn2kaXPznZ5qjNs/IY	No Action Decrypt First
5	M8YTnuVRhnskNcKbBYIT	+/TFui7IVGMB/mivDU7R	H9ff9eps2vwmhTyl2JrA	YDV7qEfA+4sKDq6E7CUI	1nH/mNWcrV/mdBjC6i9c	usjE2ckGDx8YgQC+kqVj	No

Figure 5.8: Requesting test results

5.4 Security Issues

The system will always request for login details in order to prevent illegal access to it. The user of the system must either be working with the organization or an administrator or staff authorized to use it. To view stored records especially lab results the data is encrypted one will need a decrypted to have them in readable form. Also the system programmed to always logout when idle to prompt the user to re-enter password and user name in order to have access. Un-Interruptible Power Supply (UPS) need to be in place against any power shortages and cuts. The hardware should be handled with care and protected from damages like fire, water and others. There is also need to put in place a stabilizer to regulate power flows into the related accessories. Finally, restriction of physical access to the system environment shall be put in place so as to protect the system from unauthorized use.

Constant monitoring of the lab system (hardware, network, application, OS and security) is critical. An effective monitoring solution will predict and fix problems before they adversely affect the end users of the application. An effective monitoring system will be implemented and operated by the support team.

Employ virus protection

An anti-virus updates should be consistently installed and kept running on the LMS server and configured to perform daily scans and full scans on weekly basis. It should be configured to automatically trigger alerts to support users in the event of virus detection.

5.5 Formative Evaluation

The primary goal of formative evaluation is to collect information about the perceptions on learning effectiveness, users' satisfaction and identify any usability issues early in design. In order to achieve this, the researcher used three groups of two making a total of four staff and two clients. The participants were given an introductory briefing about the high-fidelity prototype, user goals and requirements derived from the PD sessions.

The participants were then given a debriefing questionnaire in order to capture their experiences with the interface. A number of issues were highlighted as revealed in the subsections that follow. In order to collect information about the perceptions on learning effectiveness, users' satisfaction and identify any usability issues early in design, we utilize Likert scale attitude statements as illustrated below:

5.5.1 Learning Effectiveness

The evaluation of perceived learning effectiveness of lab system gives satisfactory results. The first four questions posed sought to measure how easy it is to learn, ease of navigation, enjoy-ability and ease of use after training. The results in table 5.1 below confirm that users found the high fidelity prototype easy to learn, navigate, enjoyable and easy to learn after training.

Table 5.1: Prototype learning effectiveness

Learning Effectiveness	**SD**	**D**	**A**	**SA**
The lab System is not easy to learn.		4	2	
Navigating the Lab system is difficult	1	4	1	
the lab system is secure			4	2
Using the lab system is enjoyable			5	1

Learning Effectiveness	**SD**	**D**	**A**	**SA**
The lab system is easy to learn after training			6	

SD – Strongly Disagree, **D** – Disagree, **A** – Agree and **SA** – Strongly Agree

5.5.2 Perceived Benefits

In order to evaluate the perceived benefit of the prototype, the users were asked whether they thought the tool may help improve security of clinical records, whether the prototype functions facilitate ease of use and whether the prototype features are easy to understand. The majority of our participants revealed positive results for the three questions as shown in the table below.

Table 5.2: Prototype Perceived benefits

Perceived Benefits	**SD**	**D**	**A**	**SA**
The system may improve security of records			5	1
The system functions facilitate the ease with which content can be accessed.		2	4	
It is easy to understand the features provided by lab system		1	5	

SD – Strongly Disagree, **D** – Disagree, **A** – Agree and **SA** – Strongly Agree

5.2.3 User Satisfaction

In order to evaluate the perceived users' satisfaction of the prototype, they were asked four questions. More precisely, the users were asked to answer questions that focused on measuring aspects related to the their reaction to the interaction with the interface, the user's opinion about the navigation, how the functions are structured, the sequence of screens and whether the prototype could be explored using trial and error. Results from table 5.3 reveal that all the 6 respondents thought the interface was intuitive, only 1 said it was confusing to navigate, 5 said the functions were not structured suitably, 4 said the sequence of screens were not confusing and that 4 said you could explore the prototype features using trial and error.

Table 5.3: Prototype's Users' Satisfaction

Users' Satisfaction	**SD**	**D**	**A**	**SA**
The Lab System interface is intuitive (i.e. It can be used without thinking)			6	
The system is confusing to navigate		4	1	
System functions are not structured suitably		6		
The Sequence of screens is confusing		4		
You can explore system features using trial and error		1	4	

The data analysis points out that the prototype has been fairly appreciated. The tables 5.1, 5.2 and 5.3 show the representation of the different usability aspects measured.

CHAPTER SIX

DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

This project aimed at developing a basis of Electronic health record system for medical laboratory. Through the Design and Development of a secured system for resource-constrained environment. This started with the evaluation of the current systems; establishment of users. By using paper prototyping and user centered design the system requirements and functionalities were identified. This was so helpful since the researcher used the actual users ideas to design the system. Users felt appreciated and satisfied with the results since they participated in requirement collection and design.

6.1 Report summary

This sub-section presents a summary of the study that was carried out at the Center. It presents the aim of the study, objectives, and how these were achieved, the challenges and successes as shown below. The study aimed at developing a secure lab system in a resource-constrained environment. To achieve the study set out with objectives to evaluate the existing lab systems in view of business processes and technologies to establish weaknesses in relation to the lab unit; review methodologies to come up with the best approach and methods for executing the project; design a prototype solution and implement the solution (Chapter one). The study reviewed literature on related works to determine the gap (Chapter two) and established a secure lab system. Evaluated the healthy policy standards. Business processes on the supply side through use of data collection techniques and tools user centered design and paper pro-typing (explained in chapter three). Findings revealed Investigators constantly faced challenges of retrieving files and updating the existing ones and unauthorized access to medical results files. Management reports were delayed and sometimes inaccurate as a result of relying on inaccurate information to generate these reports. In response, a secure lab system was development and implementation was planned, user and system requirements determined; models designed solution implemented. Basing on the project objectives and requirements prior determined. Chapter five clearly shows that the MLRS system designed for resource constrained environment project was successful in implementing the objectives as stated in the previous chapters of this report. The use of this MLRS saves time, the system also operators on low hardware thus saving cost. And records security is guaranteed.

6.2 Recommendations

It’s the government duty to provide good health services to its people. At the rate on which the population is increasing the available government facilities cannot accommodated meet the standards of all the people and also provide quick and efficient health services. Therefore there a need for the government to think of increasing funds in health and ICT ministry to developed a centralized EHR (electronic health records). This will soften/quicken and eliminate long queues especially in government hospitals thus reducing work of health practitioners and enhance smooth communication and better relationships between client and medical workers

As an effect of the ageing of the population in general, the number of citizens with chronic diseases is increasing, especially among elderly people throughout the country. This is a great challenge for both the well being of the citizens and the public health care systems. Health care solutions provided by information and communication technology (ICT), also known as eHealth, offer one solution to this problem. The tools and services that contribute to eHealth provide better and more efficient health care services for all. E-Health technologies empower patients to take more responsibility for their own health and quality of life, and they lead to better cost-efficiency in the health sector. The use of eHealth technologies allows a mutually beneficial collaboration and involvement of patients and medical professionals in the prevention and treatment of chronic diseases. Overall, ICT can be used to ensure the top-quality health care of citizens

6.3 Discussion

Despite the potential of EHR systems to address the challenges facing health systems in developing countries, the majority of EHR systems designed for developed countries cannot be adapted for implementation in developing countries. The failure of adoption is attributed to many factors including: 1) Online Access Control: The majority of EHR systems require online access control decision. When the server/database is unavailable, for example due to frequent power outages that is common in developing countries, access control decisions cannot be made, making health records unreachable; 2) Users’ Context: The majority of EHR systems designed for developed countries were developed with the user contexts in the developed World and therefore do not represent the needs of the patients and medical practitioners in the developing countries. We therefore feel that in order for EHR systems to satisfy the intended users specifically in developing countries, existing systems needs to be extended on mobile phones such that records can be made available when hospital servers are offline. Akinyele et al. (2011) affirmed that mobile phones (also called small handheld computers) could be used to provide health records without the need for a single server.

6.4 Conclusion

The Internet enhances information and communication among individual work-stations and on a large scale between medical information systems. However, the Internet is a public environment with high-risk security threats. When medical information systems, instruments, workstations and mobile devices are connected to the Internet significant protection is required. All medical personnel should have a basic understanding of Internet security threats and should be in compliance with their organization's policies and procedures to avert them. Security is key factor in EHR system since it helps to improve quality of health care being provided any attempt to alter records can be of great risk to an individual. So help providers should make sure individual records are protected and accessed granted to only authorize personnel and services available all the time. As the researcher AES encryption that is implemented in the developed system in the research will help to provide security for the medical records.

REFERENCES

Andriole, K.P. 2014. Security of electronic medical information and patient Privacy: what you need to know. *Journal of the American College of Radiology*, 11(2).

Annas G. J. (2003). HIPAA Regulation - A New Era of Medical Record Privacy. *The New England Journal of Medicine*. Vol 48, pp. 1486-1490

Annas G. J. 2003. HIPAA Regulation - A New Era of Medical Record Privacy. *The New England Journal of Medicine* 348:1486-1490

Bailey .B .P, Biehl .J .T, Cook .D .J, and Metcalf .H .E (2008). Adapting paper prototyping for designing user interfaces for multiple display environments. *Personal Ubiquitous Comput.* 12, 3, pp 269-277.

Bailey .B .P, Biehl .J .T, Cook .D .J, and Metcalf .H .E (2008). Adapting paper prototyping for designing user interfaces for multiple display environments. Personal Ubiquitous Comput. 12, 3, pp 269-277.

Baker, D.B. and Masys, D.R. 1999. PCASSO: A Design for Secure Communication of Personal Health Information via the Internet. *International Journal of Medical Informatics*. 54:97-104

Baker, M. 2005. Keeping a Secret. *Technology Review*, 108(1), 82-83.

Bell, D.D. and La Padula L.J.1974. Secure Computer System: Unified Exposition and Multics Interpretation

Bhargav-Spantzel, A., Camenisch, J., Gross, T., & Sommer, D. 2007. User centricity: A taxonomy and open issues. *Journal of Computer Security*, 15(5), 493-527.

Bourka, A.; Kaliontzoglou, A. and Polemi, D. 2003. PKI-based Security of Electronic Healthcare Documents. *Proc SSGRR.*

Brook J.M.C. 2008. Pseudonymization methodologies: personal liberty vs. the greater good. *The Last HOPE Conference*, New York.

Chaum D.L. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, Vol. 24(2), 84 – 90.

Choi, Y.B., Capitan, K.E., Krause, J.S., and Streeper, M.M. (2006) ―Challenges Associated with Privacy in Healthcare Industry: Implementation of HIPAA and Security Rules, *Journal of Medical Systems*, vol. 30, no. 1, pp57–64

Cooley, J.A. and Smith, S. W. 2010. "Dr. Jekyll or Mr. Hyde: Information Security in the Ecosystem of Healthcare. http: //www. ists.dartmouth.edu/library/474.pdf. [Viewed 24-06-2016]

Etzioni, A. 1999.*The Limits of Privacy,* Basic Books, New York

Ferrari E.; and Thuraisingham B. 2005. Analysis of information security objects under attacks and processed by methods of compression, IRM Press.

Fisher, F. and Madge B.(1996). Data Security and Patient Confidentiality: The Manager's Role. *The International Journal of Bio-Medical Computing*. Vol 43, pp.115 - 119

Gasser, M. 1998. *Building a Secure Computer System.* New York, Van Nostrand Reinhold.

Greenhalgh, T., Stramer, K., Bratan, T., Russell, J., and Potts, H. 2010. Adoption and nonadoption of a shared electronic summary record in England: A mixed-method case study. *British Medical Journal, 340.* doi: 10.1136/bmj.c3111.

Gunter, T and Terry, N. 2005. The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions. *Journal of Medical Internet Research*, 7(1):3.

Hillestad R., Bigelow J., Bower A., Girosi F., Meili R., Scoville R., and Taylor R., 2005. Can electronic medical record systems transform health care? Potential health benefits, savings, and costs, Health Affairs, Vol.24(5), 1103-1117.

http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1496871/

http://www.radiologyinfo.org/en/info.cfm?pg=article-patient-privacy

Huda M.N, Kamioka E, and Yamada S. 2007. An efficient and privacyaware meeting scheduling scheme using common computational space. *IEICE - Transactions on Information and Systems,* Vol. E90-D(3), 656-667.

Huda, N.M.D et al. 2009. A Privacy Management Architecture For Patient-Controlled Personal Health Record System. *Journal of Engineering Science and Technology*. Vol. 4, No. 2 154 – 170

ISO(2015).http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=54960[Viewed 01-06-2015]

Johnson, M., et al. 2009. Laissez-Faire File Sharing: Access Control Designed for Individuals at the Endpoints. *New Security Paradigms Workshop, September 2009*

Kalogriopoulos, N. A., Baran, J., Nimunkar, A. J. and Webster, J. G. 2009. Electronic medical record systems for developing countries: review. *Conference Proceedings of the IEEE Engineering in Medicine and Biology Society,* September 2009; 1730–3.

Kamadjeu, R. M., Tapang, E. M. and Moluh, R. N. 2005. Designing and implementing an electronic health record system in primary care practice in sub-Saharan Africa: a case study from Cameroon. *Inform Prim Care (*Jan 2005*),* 13(3):179-186.

Kim M. I. and Johnson K. B. (2002). Personal health records: evaluation of functionality and utility. *Journal of the American Medical Informatics Association,* Vol. 9(2), 171–180.

Knapp, K.J., and Boulton, W.R. 2006.Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments, *Information Systems Management*, vol.23, no.2, pp 76-87

Kulynych, J. and Korn, D. 2003. The New HIPAA (Health Insurance Portability and Accountability Act of 1996) Medical Privacy Rule. *Circulation.* **108**:912-914.

Levy, S. (2001). Crypto: How the code rebels beat the Government - Saving privacy in the digital age. New York: Viking Penguin Publishing.

Li, M., Poovendran, R., and Narayanan, S.2005. Protecting Patient Privacy against Unauthorized Release of Medical Images in a Group Communication Environment. *Computerized Medical Imaging and Graphics.*Vol 29, pp. 367-383

Malin, B., and Airoldi, E. 2007.Confidentiality Preserving Audits of Electronic Medical Record Access,‖ *Proceedings of the 12th World Congress on Health (Medical) Informatics - MedInfo*, Brisbane, Australia

Mandl, K.D., Szolovits P. and Kohane, I.S.2001. Public Standards and Patients' Control: How to Keep Electronic Media Records Accessible but Private. *BJM*. 322:283-287

Mavridis, I., Georgiadis, C., Pangalos, G and Khair, M. 2001. Access Control Based on Attribute Certificates for Medical Intranet Applications. JMIR3 (1):e9.

McGinn, C. A., Grenier, S., Duplantie, J., Shaw, N., Sicotte, C., Mathieu, L… Gagnon., M. P. 2011. Comparison of user groups' perspectives of barriers and facilitators to implementing electronic health records: A systematic review. *BMC Medicine, 9*doi:10.1186/1741-7015-9-46.

McIntyre, D. 2007. *Learning from experience: Health care financing in low and Middle-income countries*, Global Forum for Health Research, Geneva.

Mercuri, R.T. 2004. The HIPAA-potamus in Health Care Data Security. *Communications of the ACM*, vol.47, no.7

Mitamura, Y., Yamamoto, A., Hayashi, H., Namioka, T., Tsuduki, Y., Shimono, T., Hirokawa, H., Yamakami, H. and Yoshida, A. 2005. A peer-to-peer-based medical information sharing system. CCECE/CCGEI, Saskatoon.

MOH(2015)..http://www.hhs.gov/ocr/privacy[Viewed 01-06-2015]

Mohit, M., AjeevBedi, Amritpal, S., and Tejinder S.2009. "Comparative Analysis of Cryptographic Algorithms", *International Journal of Advanced Engineering Technology*

NRC National Research Council .1997.For the Record: Protecting Electronic Health Information

Omary, Z., Lupiana, D., Mtenzi, F. and Wu, B. 2009. Challenges to E-Healthcare adoption in developing countries: A case study of Tanzania. *Networked Digital Technologies*, 2009.

Oppliger, R. 1996. *Authentication System for Secure Networks*, Artech House, Boston, MA.

Personal Health Information Protection Act, *(*PHIPA 2004*).*

Rindfleisch, T.C. 1997. Privacy, Information Technology, and Health Care, *Communications of the ACM*,, vol.40, no.8, pp 93 – 100

Rindfleisch, T.C. 1997.Privacy, Information Technology, and Health Care,‖ Communications of the ACM,, vol.40, no.8, pp 93 – 100

Robinson, S. 2008. Safe and secure: data encryption for embedded systems.*EDN Europe*, 53(6), 24-33

Sanders, C., Rogers, A., Bowen, R., Bower, P. Newman, S. P. 2012. Exploring barriers to participation and adoption of telehealth and telecare within the Whole System Demonstrator trial: a qualitative study. *BMC Health Services Research*, doi: 10.1186/1472-6963-12-220.

Sandhu, R., Ferraiolo, D. and Kuhn, R. 2001. The NIST Model for Role-Based Access Control: Towards a Unified Standard. *ACM Transactions on Information and System Security (TISSEC).*

Schartner P; and Schaffer M. 2005. Unique user-generated digital pseudonyms. *Springer LNC* ,Vol. 3685, 194-205.

Schneier, B. 2004. The Nonsecurity of Secrecy. *Communications of the ACM*, 47(10), 120-120.

Sinclair, S. and Smith, S. "What's Wrong with Access Control in the Real World?", IEEE Security and Privacy, vol. 8, no. 4, pp. 74-77, July/Aug. 2010, doi:10.1109/MSP.2010.139

Sittig, D.F. and Singh, H. 2011. Legal, Ethical, and Financial Dilemmas in Electronic Health Record Adoption and Use. *Pediatrics*. 127(4)

Smith, B., Austin, A., Brown, M., King, J. T., Lankford, J., Meneely, A., and Williams, L. 2010. Challenges for protecting the privacy of health information: required certification can leave common vulnerabilities undetected. *Proceedings of the second annual workshop on Security and privacy in medical and home-care systems* (pp. 1-12).

Snyder, C. 2003. Paper prototyping: the fast and easy way to design and refine user interfaces. Morgan Kauffman Publishers, San Francisco, USA.

Snyder, C. 2003. Paper prototyping: the fast and easy way to design and refine user interfaces. Morgan Kauffman Publishers, San Francisco, USA.

Storbrauck, L. 2015. Mobile Device Use: Increasing Privacy and Security Awareness for Nurse Practitioners. *Economic Crime Forensics Capstones*. Vol 7

Sundelin, L. T. 2003. Surrogate Trust System: Solving Authentication and Authorization Issues in Dynamic Mobile Networks. Unpublished Masters' thesis, BrighamYoung University, USA.

Tierney, W.M., Beck, E.J., Gardner, R.M.; et al. 2006. Viewpoint: A Pramatic Approach to Constructing a Minimum Data Set for Care of Patients with HIV in Developing Countries. *Journal of the American Medical Informatics Association.* 13:253-260.

Tuyikeze, T. 2005. *A model for information security management and regulatory compliance in the South African health sector.* MSc thesis. Nelson Mandela Metropolitan University. http://www.nmmu.ac.za/documents/theses/Thesis_TITE.pdf. Accessed 01/08/2012.

Tuyikeze, T. and Pottas, D. 2005. Information Security Management and Regulatory Compliance in the South African Health Sector.

US Congress (2007a) ―Health Information Privacy and Security Act, S.1814

US Congress (2007b) ―National Health Information Technology and Privacy Advancement Act of 2007, S.1455,

US Congress (2008) ―Technologies for Restoring User‗s Security and Trust in health Information Act of 2008,‖ H.R.5442

Vawdrey, D.K.; Sundelin, T.L.; Seamons K.E.and Knutson C.D.2003. Trust Negotiation for Authentication and Authorization in Healthcare Information Systems. *Proc Annual International Conference of IEEE.***2**:1406-1409

WHO World Health Organization. 2006. Electronic Health Records: Manual for Developing Countries. WHO Library Cataloguing in Publication Data

Willey V.J. and Daniel G.W. (2006). Healthcare: an economic evaluation of use of a payer-based electronic health record within an emergency department, http://event.on24.com/event/35/62/1/rt/1/images/player_docanchr_5/study.pdf.

Win, K.T., Susilo, W., and Mu, Y. (2006) ―Personal Health Record Systems and Their Privacy Protection, *Journal of Medical Systems*, vol.30, pp 309 – 315

Preece, J., Rogers, Y., & Sharp, H. (2002). Interaction design: Beyond human-computer interaction. New York, NY: John Wiley & Sons.

Damanpour, F. and Gopalakrishnan, S. (2001) ‘The Dynamics of the Adoption of Product and Process Innovations in Organizations’, The Journal of Management Studies 38(1):45–65.

Thong, J. and Yap, C. (1996) ‘Information Technology Adoption by Small Business:

Kaplan, B., & Dorsey, P. (1991). Requirements Analysis interviewing: alternative perspectives. Technical Report 91-021. Washington, D.C.: The American University, Department of Computer Science and Information Systems

Sanbar SS. American College of Legal Medicine Textbook Committee. Legal Medicine. 6th ed. St. Louis: Mosby; 2004. Medical records: Paper and electronic.

Appendix

The data base is called lab_db

The SQL code for creating the database
was; CREATE DATABASE
lab_db USE lab_db

Source Code for encryption:

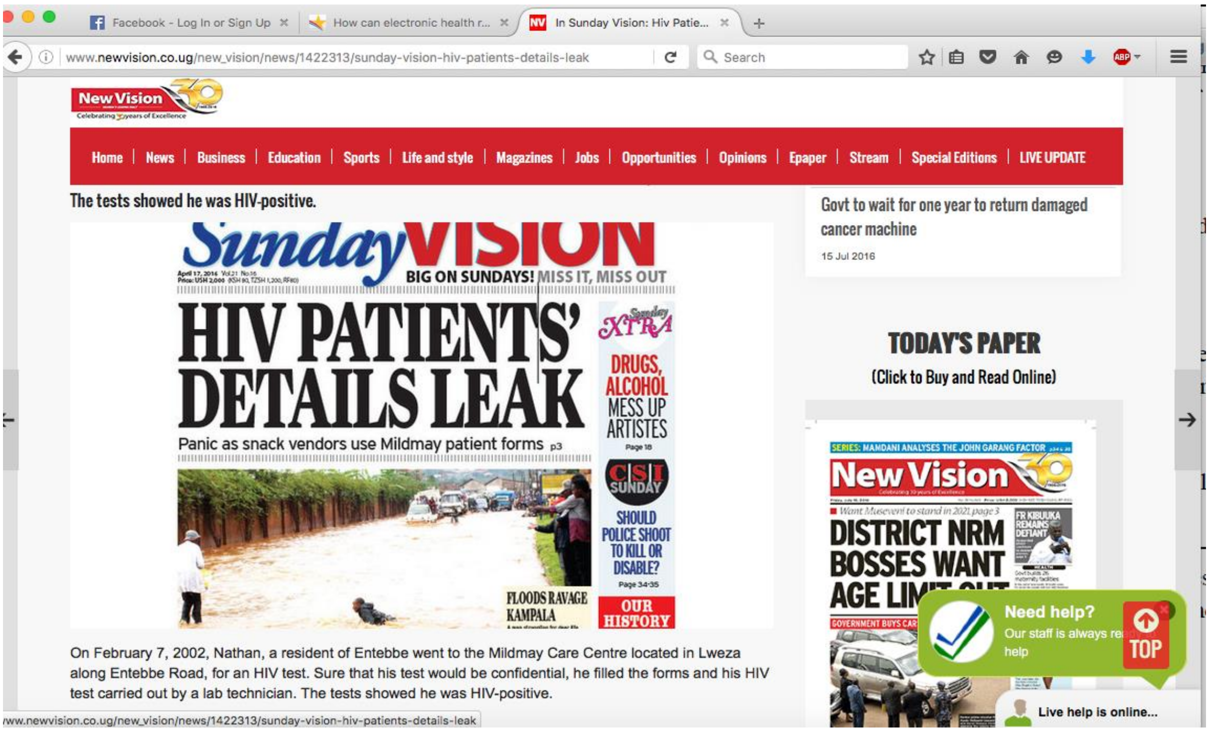
```
//encrypt function

function mc_encrypt($encrypt, $key){

   $encrypt = serialize($encrypt);

   $iv = mcrypt_create_iv(mcrypt_get_iv_size(MCRYPT_RIJNDAEL_256,
MCRYPT_MODE_CBC), MCRYPT_DEV_URANDOM);

   $key = pack('H*', $key);

   $mac = hash_hmac('sha256', $encrypt, substr(bin2hex($key), -32));

   $passcrypt = mcrypt_encrypt(MCRYPT_RIJNDAEL_256, $key, $encrypt.$mac,
MCRYPT_MODE_CBC, $iv);
```

```
    $encoded = base64_encode($passcrypt).'|'.base64_encode($iv);
    return $encoded;
}
// Decrypt Function
function mc_decrypt($decrypt, $key){
    $decrypt = explode('|', $decrypt.'|');
    $decoded = base64_decode($decrypt[0]);
    $iv = base64_decode($decrypt[1]);
    if(strlen($iv)!==mcrypt_get_iv_size(MCRYPT_RIJNDAEL_256,
MCRYPT_MODE_CBC)){ return false; }
    $key = pack('H*', $key);
    $decrypted = trim(mcrypt_decrypt(MCRYPT_RIJNDAEL_256, $key, $decoded,
MCRYPT_MODE_CBC, $iv));
    $mac = substr($decrypted, -64);
    $decrypted = substr($decrypted, 0, -64);
    $calcmac = hash_hmac('sha256', $decrypted, substr(bin2hex($key), -32));
    if($calcmac!==$mac){ return false; }
    $decrypted = unserialize($decrypted);
    return $decrypted;
}


//function for inserting a new record in the database
function DB_Inserter($table_name, $form_data) {
    // retrieve the keys of the array (column titles)
    // print_r($form_data);
    $db=  Database::getInstance();
    $mysqli=$db->getConnection();
    $fields = array_keys($form_data);
    //echo 'Names';
    // building the query
    $sql = "INSERT INTO " . $table_name . "
    (`" . implode('`,`', $fields) . "`)
    VALUES('" . implode("','", $form_data) . "')";

    $myQuery = $mysqli->query($sql);
    if ($myQuery) {
        $result = 'Record Saved';
    } else {
        $result = 'Record Not Saved' . $mysqli->error;
    }
    return $result;
}
//code for deleting database records
function db_row_delete($table_name, $where_clause) {
    // check for optional where clause
            //$where_clause=" WHERE ID='$idValue'";
    $whereSQL = '';
    if (!empty($where_clause)) {
        // check to see if the 'where' keyword exists
        if (substr(strtoupper(trim($where_clause)), 0, 5) != 'WHERE') {
            // not found, add keyword
            $whereSQL = " WHERE " . $where_clause;
        } else {
            $whereSQL = " " . trim($where_clause);
        }
    }
    // building the query
    $sql = "DELETE FROM " . $table_name . $whereSQL;

    // run and return the query result resource
    return mysql_query($sql);
}
//code for updated database records
function db_row_update($table_name, $form_data, $where_clause) {
            $db=  Database::getInstance();
    $mysqli=$db->getConnection();
    // checking for optional where clause
    $whereSQL = '';
    if (!empty($where_clause)) {
        // check to see if the 'where' keyword exists
        if (substr(strtoupper(trim($where_clause)), 0, 5) != 'WHERE') {
            // not found, add key word
            $whereSQL = " WHERE " . $where_clause;
        } else {
            $whereSQL = " " . trim($where_clause);
        }
    }
    // start the actual SQL statement
    $sql = "UPDATE " . $table_name . " SET ";
    // loop and build the column /
    $sets = array();
    foreach ($form_data as $column => $value) {
        $sets[] = "`" . $column . "` = '" . $value . "'";
    }
    $sql .= implode(', ', $sets);

    // append the where statement
    $sql .= $whereSQL;

    // run and return the query result
    return $mysqli->query($sql);
}
```

//**code that encrypts patient data while saving it**

```
<?php
                        if (isset($_POST['Register'])) {
                            $p = mc_encrypt($_POST['names'], ENCRYPTION_KEY);
                            $c = mc_encrypt($_POST['contacts'], ENCRYPTION_KEY);
                            $ad = mc_encrypt($_POST['address'], ENCRYPTION_KEY);
                            $ag = mc_encrypt($_POST['age'], ENCRYPTION_KEY);
                            $sx = mc_encrypt($_POST['sex'], ENCRYPTION_KEY);
                            $occ = mc_encrypt($_POST['occupation'], ENCRYPTION_KEY);
                            $user = $_SESSION['user_id'];
```

```
          $reg_patient = array('Patient_Names' => $p, 'Contact' => $c, 'Address' =>
$ad,
            'Age' => $ag, 'Sex' => $sx, 'Occupation' => $occ, 'User_Id' => $user);
          $registered = DB_Inserter('patient_data', $reg_patient);
          if ($registered) {
            _sucMsg("Patient Successfully Registered");
            //_refresh("patients_register.php");
          }
        } else {
          echo "Enter new patient's details below";
        }
        ?>
```


Facebook - Log In or Sign Up
How can electronic health r...
In Sunday Vision: Hiv Patie...
www.newvision.co.ug/new_vision/news/1422313/sunday-vision-hiv-patients-details-leak
Search
New Vision
Home | News | Business | Education | Sports | Life and style | Magazines | Jobs | Opportunities | Opinions | Epaper | Stream | Special Editions | LIVE UPDATE
Sunday Vision
BIG ON SUNDAYS! MISS IT, MISS OUT
HIV PATIENTS' DETAILS LEAK
Panic as snack vendors use Mildmay patient forms p3
DRUGS, ALCOHOL MESS UP ARTISTES
CSI SUNDAY
SHOULD POLICE SHOOT TO KILL OR DISABLE?
FLOODS RAVAGE KAMPALA
OUR HISTORY
TODAY'S PAPER
(Click to Buy and Read Online)
DISTRICT NRM BOSSES WANT AGE LIMIT OUT
Need help?
Our staff is always re
help
TOP
Live help is online...

The tests showed he was HIV-positive.

Govt to wait for one year to return damaged cancer machine

15 Jul 2016

On February 7, 2002, Nathan, a resident of Entebbe went to the Mildmay Care Centre located in Lweza along Entebbe Road, for an HIV test. Sure that his test would be confidential, he filled the forms and his HIV test carried out by a lab technician. The tests showed he was HIV-positive.

APPENDICES

Appendix A: interview Questions.

MIS finalist's student of Uganda Martyrs Nkozi university student is conducting this interview guide. This data collection tool is for study purposes only and any data collected will be used for academic reasons only.

1. How do you store your records?

   ……………………………………………………………………………………………
   ………….

2. How do you perform the record retrieval process?

   ……………………………………………………………………………………………
   …………..

3. How many computers do you have?

   …………………………………………………………………………………

4. Who are the computer users?

   ………………………………………………………………………………..

5. How has access to lab records?

…………………………………………………………………………….

6. Security management of electronic health record is important to me?

   …………………………………………………………………………….

7. What measures are used to protect the data from loss, theft, and hacking
8.

Appendix II Debriefing Questions

Secure lab management system.

The objective of this study is to get the learning effectiveness of the staff about the newly developed system. This data collection tool is for study purposes only and any data collected will be used for academic reasons only. The Questionnaires targets the staff from the office of the system users i.e. lab tech receptionist and physician in order to get their opinion about the lab system

How do you find the lab management system usability?

……………………………………………………………………………..

How has the new system impacted your performance?

………………………………………………………………………………

The lab management system is enjoyable to use?

……………………………………………………………………………….

The lab management system is easy to learn after training?

………………………………………………………………………………..