KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

AN ENHANCED TRIPLE DATA ENCRYPTION STANDARD (TDES) ALGORITHM TO SECURE HEALTH LEVEL SEVEN (HL7) DATA TRANSFER

BY

ASARE MICHAEL TETTEH (PG2707714)

NOVEMBER 2016

KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

AN ENHANCED TRIPLE DATA ENCRYPTION STANDARD (TDES) ALGORITHM TO SECURE HEALTH LEVEL SEVEN (HL7) DATA TRANSFER

BY

ASARE MICHAEL TETTEH (PG2707714)

JUNE 2016

A THESIS SUBMITTED TO THE SCHOOL OF GRADUATE STUDIES, KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

DECLARATION

CANDIDATE'S DECLARATION

I hereby declare that this submission is my own work and that, to the best of my knowledge and beliefs, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma at Kwame Nkrumah University of Science and Technology, Kumasi, or any other educational institution except where due acknowledgement is made in the thesis.

_____ _____

Asare Michael Tetteh Date

SUPERVISOR'S DECLARATION

I hereby declare that I supervised this project work in accordance with the guidelines on the supervision of thesis as laid down by the Kwame Nkrumah University of Science and Technology

_____ _____

Dr Yaw Marfo Missah Date

HEAD OF DEPARTMENT

_____ _____

Dr J. B. Hayfron-Acquah Date

DEDICATION

This research is dedicated to my wife Mrs. Leticia Asare, and my daughter, Isabella Serwah Ayerki Asare.

ACKNOWLEDGEMENT

Though only my name appears on the cover of this dissertation, a great number of people have contributed to its production. I owe my gratitude to Lord Almighty for His love and support throughout this research and all the days I spent at school.

My sincere appreciation goes to all those people who have made this dissertation possible and because of whom my graduate experience has been one that I will cherish forever. Most importantly my supervisor, Dr Yaw Marfo Missah, you have been a great help and encouragement in this project. None of this would have been possible without the love and patience of my family. My immediate family, to whom this dissertation is dedicated to, has been a constant source of love, concern, support and strength all these years. I would like to express my heart-felt gratitude to my family. My extended family has aided and encouraged me throughout this endeavour.

I appreciate the financial support from the Valley View University for the funding for the years I spent in school. I am indebted to the following staff at Valley View University, for their various forms of support during my graduate study; Prof. Daniel Bediako – Vice Chancellor; Prof. OseiBonsu – Pro Vice Chancellor; Prof. Dr. Dr. Daniel Buor – Former Vice Chancellor; Mr. Emmanuel Osei Kuffuor – Assistant Finance Officer; Ebenezer Laryea – ITS Director; Mrs Susan Adjei-Mensah -- Lecturer, Kwadwo Debrah -- ITS, Miss Elizabeth Obeng -- PRO; Ezekiel Okoe, ITS; and Prince Opoku Boateng, ITS, just to mention a few. I would like to acknowledge Mr. Dominic Damoah – Dean, Faculty of Science, Valley View University, and Mr. Edward Danso Ansong – former Dean, Faculty of Sciences, also of Valley View University for their encouragement and practical advice.

Many friends have helped me stay focused through these difficult years. Their support and care helped me overcame setbacks and stayed focused on my graduate study. I greatly value their friendship and I deeply appreciate their faith in me, especially, Rebecca Amponsah. In my daily

work I have been blessed with a friendly and cheerful group of fellow students. And I am indebted to the many countless ones who contributed to where I am today.

And finally, I must express my very profound gratitude to my wife for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without all these people.

Thank you.

Table of Contents

KEYWORDS/ABBREVIATIONS

ACK – General Acknowledgement

ADT – Admit Discharge Transfer

Algorithm - a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer.

BAR – Add/change Billing Account

Cipher - a method of transforming a text in order to conceal its meaning.

Cryptography - is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Decipher - Convert coded text to readable form.

Decryption - The process of decoding a message into readable format.

DFT – Detailed Financial Transaction

Encryption - The process of encoding text so that it can be understood only by the recipient.

HIS - Hospital Information System

HIV - Human Immunodeficiency Virus

HL7 - Health Level Seven

MDM – Medical Document Management

MFN – Master Files Notification

ORM – Order Pharmacy Treatment

ORU – Observation Result Unsolicited

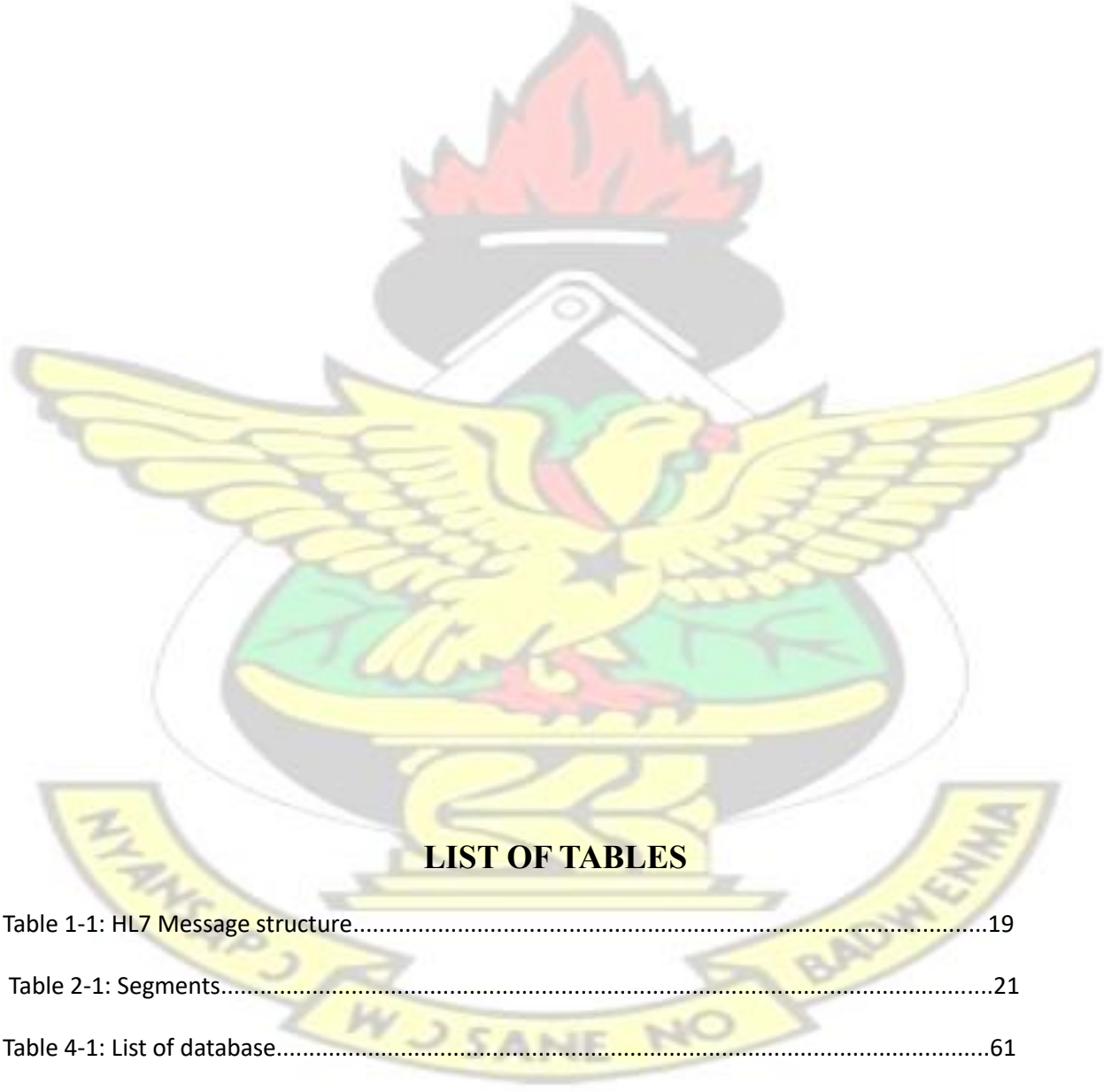
QRY – Query Original Mode

SIU – Scheduling Information Unsolicited

TDEA - Triple Data Encryption Algorithm
TDES - Triple Data Encryption Standard

VoIP - Voice Over Internet Protocol

WEP - Wired Equivalent Privacy



LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

ABSTRACT

The confidentiality of patient information is very important; this is because it contributes to the efficiency of healthcare delivery. The willingness of patients to disclose their information is based on the trust that their information is kept secret.

Data breaches on the other hand is on the increase, and data is no more safe whether at rest or on transit. Seventy percent (70%) of organizations reported of data breach within twelve (12) months in 2015, which is a very frightening statistics. Due to this, medical facilities in recent times have employed the use of Health Level Seven (HL7) Messaging standard to ensure seamless communication between Health Information Systems (HIS).

This study looked at a way to enhance Triple Data Encryption Algorithm (TDES/TDEA) to secure HL7 message or data on transit. The study looked at encrypting the encoded and validated HL7 message before transmission; the message was encoded and encrypted. Upon arrival at its destination, the message was decrypted and decoded thereby securing patients' data. The findings of the research show that, in order for any information sent through an HL7 Messaging System to be secured, to facilitate hospital–patient trust and confidentiality, there is the need for an Enhanced Triple Data Encryption Algorithm (A5AR3MY).

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND OF STUDY

Due to the increasing need to understand hospital-patient and even workers of health facilities status and behavioural patterns, hospitals amass a great deal of confidential information about their employees, patients, medical products, research and financial status. Most of these information are collected, processed, stored on computers, then transmitted across networks to other computers (Magaqa, 2012).

It has also been realized that, management of healthcare information in relation to time and cost is very important since human lives are at stake. A lot of clinical applications are now in existence that operates within individual healthcare institutions; there is the need for some kind of interoperability or common level of information system that manages healthcare information across the nation.

Though many of these institutions are aspiring to achieve this goal, it has been realized that, many of their systems are incompatible (Damoah, et al., 2014). Furthermore, securing data during transmission across networks is another major concern to be considered to ensure the realization of this kind of common platform in the nation.

According to Mweebo (2014), patients' privacy is paramount because any disclosure of personal health information such as the HIV status of the patient may result in stigmatization, unemployment, and denial of medical benefits. In addition, patients are likely to suffer financial

losses from illegal transfer of finances if billing information is accessed by unauthorised staff. Vithiatharan, (2014) indicated that, although attempts are being made to hide medical data, it does not guarantee its full protection.

In the case of Ghana, when a patient is being transferred from one hospital to the other, a transfer form will have to be completed by the medical officers initiating the transfer. This will include medical records like the patients history, current condition, drugs administered, observation made, just to mention a few. Since this is a human institution, the tendency to introduce error is very likely or high. This process will take a lot of time; if this is an emergency situation, casualties may be recorded. What if there is a system that allows the medical records of the patient to be pulled or accessed seamlessly, from the hospital information system of another hospital with the use of their health insurance number? In order to achieve this, Health Level Seven (HL7) will have to be implemented.

HL7 refers to a set of international standards for the transfer of administrative and clinical data between software/web applications used by a variety of hospitals and healthcare providers (HL7, HL7 International, 2011). It was founded in 1987 (HL7, HL7 International, 2011) and has a number of benefits:

- It facilitates the seamless exchange of data between health and medical institutions.
- Health providers can use HL7 interface engine to achieve the benefits that come with current legacy systems (Information Systems) without any major investment in new technologies; this lowers cost and extends the life and efficiencies of existing systems.
- There is also an opportunity to connect with systems outside the healthcare provider, which include providers of outsourced services like radiology (Orion, 2013).

However, there are few problems with the HL7. Although it makes it possible for seamless data exchange, data being transferred over a network is not safe and can easily be intercepted and read by anybody with little knowledge about HL7 standards (Zero, 2011)

1.2 MOTIVATION OF THE STUDY

According to Conn (2015), roughly eight (8) out of ten (10) leaders in health information technology who were recently surveyed indicated that their provider or insurance organizations suffered a cyber-attack that compromised their computer systems in the past two years. According to Department of Health and Human Services, records of more than 120 million patients have been compromised in more than 1,100 separate breaches at institutions in charge of protecting health data since 2009 (Peterson, 2015). Recently, about 3.9 million people have had their medical information exposed when Fort Wayne, Ind., medical software company's network was hacked (Press, 2015).

Based on the few incidents mentioned above, it is paramount that medical records must be secured during data transfer.

The proposed Enhanced Triple Data Encryption Standard Algorithm (A5AR3MY) is to secure HL7 data transfer in order to ensure patient's information confidentiality.

1.3 PROBLEM STATEMENT

Medical privacy is of great concern to every individual. Nobody would want their insurance company or employers to know about their health status. This is best known to an individual. An

attacker can easily intercept and modify any health details at the least opportunity given. This is likely to change any medical history thereby introducing new history.

Although HL7 has its own benefits and there is the transfer of data via unencrypted network, HL7 messages can be decoded easily with little technical expertise and, data not encrypted can be decoded easily when intercepted during transfer. This research therefore answers the question: How can data be transferred securely from one health information system to the other?

1.4 OBJECTIVES OF RESEARCH

This research studies existing security mechanism and presents an Enhanced TDES Algorithm to secure HL7 data transfer.

The objectives are;

- To evaluate TDES algorithm
- To propose an enhanced TDES Algorithm to secure HL7 data transfer To implement the enhanced algorithm

1.5 RESEARCH QUESTION

The research questions are as follows:

- What are the features of TDES algorithm?
- Can TDES Algorithm be improved to secure HL7 data transfer?
- Can the implementation of the proposed enhanced TDES Algorithm Secure HL7 data transfer?

1.6 STUDY JUSTIFICATION

According to Staggers, et al., (2008) the need for a computerized system for the health sector is on the rise, every medical facility will like to have a Health Information System (HIS) to automate their manual processes. This speeds up the delivery of healthcare to patients. The storage and retrieval of these medical records are made simple with the help of these HISs. On the other hand, medical institutions will like to exchange data seamlessly without a lot of paper work. This will improve the transfer process of patients from one medical facility to the other. Since this is possible, how then can exchange of data be secured? No matter how secure your network is, data can still be intercepted on the network with the help of tools such as;

Aircrack-ng: This is a tool that includes 802.11 WEP and WPA-PSK key cracking programs. It can be used to capture wireless packets and recover keys as soon as enough information has been captured. (Howe, 2011)

Airjack: It is an 802.11 packet injection tool. It was first used as a development tool to capture and inject or replay packets. Airjack can also be used to inject forged de-authentication packets, a basic technique employed in many distributed denial-of-service (DDos) and Man-in-theMiddle attacks. It constantly injects de-authentication packets into a network wreaks havoc on the connections between wireless clients and access points (Howe, 2011).

AirSnort: It is wireless LAN (CLAN) tool which recovers WEP encryption keys. AirSnort works by passively monitoring transmissions, and then computing the encryption key when enough packets have been gathered. After that point, all data sent over the network can be decrypted into plain text using the cracked WEP key (Howe, 2011).

Cain & Able: This is a multi-purpose tool that can intercept network traffic, using information contained in those packets to crack encrypted passwords using dictionary, brute-force and

cryptanalysis attack methods. It also records VoIP conversations, recover wireless network keys, and analyze routing protocols (Howe, 2011).

These tools can easily be found on the internet and are all threats that can compromise the privacy of patients, hence the need for a secured HL7 data transfer.

1.7 OVERVIEW OF RESEARCH METHODOLOGY

In order to achieve the goals of the research, the following activities would be undertaken to secure HL7 data transfer.

- Implement HL7 data transfer between HISs
- Develop an enhanced TDES Algorithm to secure the data transfer.
- Implement the enhanced TDES Algorithm to secure HL7 data transfer.

1.8 SCOPE AND LIMITATION OF THE RESEARCH WORK

The base of the research under study is in the area of Computer Security and specifically Encryption techniques. From a range of security measures available to today's Information Technology (IT) professional, the research will focus on Encryption techniques. Findings of this research will be implemented in HL7 data transfer.

1.9 ORGANIZATION OF THE RESEARCH

The thesis is organized into five (5) chapters;

Chapter one (1) entails the general introduction concerning the background of the study, statement of the problem, research objectives, and significance of the study, scope and limitations of the study, definition of terms and organization of the thesis.

Chapter two (2) consists of the review of related work. Works on previous secure data transfer and techniques are discussed. The chapter also discusses the objectives of different encryption techniques, and an overview of which technique is efficient in HL7 data transfer.

Chapter three (3) describes the methodological approach adopted, elaborating on prevention techniques. It also features on the design of the encryption algorithm.

Chapter four (4) is the implementation of the algorithm.

Chapter five (5) is the final chapter. It offers a summary of the major findings of the study, outlines a number of recommendations and future work on the secure HL7 data transfer.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

The purpose of this literature review is to discuss previous works done on secure data transfer and TDES algorithm, in a variety of contexts. The objective of this review is to lay a solid foundation for the study outlined in this chapter.

2.2 DATA TRANSFER

Data transfer refers to the process of moving analogue or digital data in the form of bits over communication medium between one or more computing network, communication or electronic devices. It enables the transfer and communication of devices in a point-to-point, point-tomultipoint and multipoint-to-multipoint environment (Thakur, 2013). There are 3 different modes of transfer based on the direction of the exchanges: simplex, half-duplex and full-duplex connections (Kioskea, 2014).

2.3 DATA SECURITY

According to Mahan et al. (2011) data travelling on a network that is not under the direct control of an organization will require a strong encryption Algorithm like the Advanced Encryption Standard (AES) to encrypt traffic. Weiss, (1993) argued that the weakest link available in most computer security systems, is the reliance on improper methods for identifying and authenticating users who are authorized and excluding all others. The introduction of a token will augement passwords or biometric, and will ensure a two-factor authentication.

2.3.1 Theories Backing Data/Information Security

According to (Petri, 2006), most organizations typically focus on technical and procedural security measures when implementing their information security solutions. However, from the point of view of Information Systems (IS), that is not enough: in order to ensure effective information security, it is required that users are aware of and use the security measure made available and described by their organizations information security policies and instructions. He concluded that, "Only a few of the existing studies on IS security awareness are theoretically grounded" (Petri, 2006).

Hong, (2003) argued that, information security is amongst the most important assets of an organization, and should be protected appropriately. In order to ensure security, an organization needs to combine systems, operations and procedures.

Current trends of designing security systems include piecemeal designs and patchwork systems made up of multiple point solutions. Methods for keeping up security requirements are being strained as increase in the complexity of business driven systems arise (Petri, 2006).

2.3.2 Areas of Data Security

There are three (3) main areas of data security: Confidentiality, Integrity, Availability (CIA) (Hayaati & Mohd, 2012). Confidentiality is when you ensure that information is protected from unauthorized user (Jung, Han, & Lee, 2001). The factors that affect confidentiality include: hackers, unauthorised users, masqueraders, Trojan horses and unprotected downloaded files (Hayaati & Mohd, 2012).

Integrity gives you the assurance that the information is complete and authentic. The integrity of data does not only depend on how 'correct' it is but whether its reliable and can be trusted. Integrity indicates the reliability and acuracy of information (Jung, Han, & Lee, 2001).

Availability guarantees that the computer system can be accesed by authorised users whenever the need arises (Hayaati & Mohd, 2012).

Recently, organizations of different sizes rely heavily on the internet and other network connections to provide support for their businesses. Network and Information security have increasingly become an important aspect of these businesses. Meanwhile, it has become a herculean task to provide an adequate level of security to protect a business because; information security is a complex undertaking. In order to achieve a successful information security program, a business will have to embark on continues improvement project which involves people, processes, and technology in a uniformed manner (Bray, 2011).

According to Li, (2015), ensuring security online is a major component of information security. It seeks to protect information-related assets of operators and users of a website during transactions through the use of technologies, policies, and procedures. The operator or owner will have to guard against security threats like hacking, phishing, and identity theft in order to achieve this objective. Online security continues to be an integral aspect of a business because any breach in security may result in damage of reputation and subsequently cause financial loss due to litigation and disruption of business.

Burkett, (2012) indicated that Information security is an essential aspect of an organizational success propelled by the need to protect information assets. In the public and private sectors, the need to protect and secure information is increasingly becoming a struggle due to the continues evolution of internal and external threats. This is due to the narrow focus on on operational security.

Kim, (2013) argued that, although technology has advanced to protect users from cyber threats, that alone cannot protect end users' information and systems effectively. Users need to learn security concept and controls to maintain a safe environment.

2.3.3 Effects of Unsecured Data

Unsecured data characterizes an organization's failure to mitigate risk. The cost for an average data breach costs an organization, $5.5 million and this does not only include penalties but forensic investigation, monitoring of credit for customers, lost sales, damaged brand, and litigation (Townsend, 2013)

Once content is uploaded online, it's sure to be there forever, no matter how hard one tries to get rid of it. It can be made public with ease if your data is breached (Author, 2011). Unsecured data can lead to vandalism where a hacking group gets access to your data, and modifies it to tanish the image and reputation of the organization. Unsecured data makes it easy for hackers to steal sensitive data or clasified documents. It will also lead to loss of revenue since your system may experience some down time (Author, 2011)

While identity theft can be incredibly bad, intellectual property theft can be just as damaging to an organization. Blueprints, ideas, and plans could be stolen by hackers, and this will make it extremely difficult to implement new products or designs: this will prevent the business from expanding (Author, 2011).

In order to address these security breaches, a security mechanism such as data encryption is required to curtail these challenges.

2.4 ENCRYPTION

Encryption is a technique used in preventing unauthorized users from making meaning out of message content. Encryption does not prevent interception, the message being sent can easily be intercepted, but the interceptor cannot make meaning of the message content until the encrypted message has been decrypted. The decryption will require a private key in order to make this possible. Encryption is technically changing or converting plain text to cipher text (Beal, 2001)

2.4.1 Types of encryption

According to Behrens, (2014) there are three main types of encryption: Symmetric Encryption, Asymmetric Encryption, and Hashing.

The symmetric encryption takes plain text and scrambles it into an unreadable format before stored on a disk or transmitted over a network. It uses the same key to encrypt and decrypt. Asymmetric encryption converts plain text to cipher text, and then decipher it again at the receiver's end. It uses a public key to cipher and a private key to decipher. The public key as the name suggests, is kept in the public domain whilst the private key is kept secret for deciphering (Behrens, 2014). Hashing is a technique used to encrypts data like paswords. It creats a hash out data. The same data will always produce the same hash; it is not possible to reverse the hash (Behrens, 2014).

2.4.2 Triple Data Encryption Standard Algorithm

Triple DES in cryptography is refered to as Symetric Block Cipher, It applies Data Encryption Standard Cipher Algorithm three times to each block of data (Tutorialspoint, 2015). The TDES process is made up of the following steps: the user generates and distributes a 3TDES key K, which

is made up of three different DES keys K1, K2 and K3. This implies that the actual 3TDES key has length 3×56 = 168 bits (Tutorialspoint, 2015). The encryption scheme is shown belows:

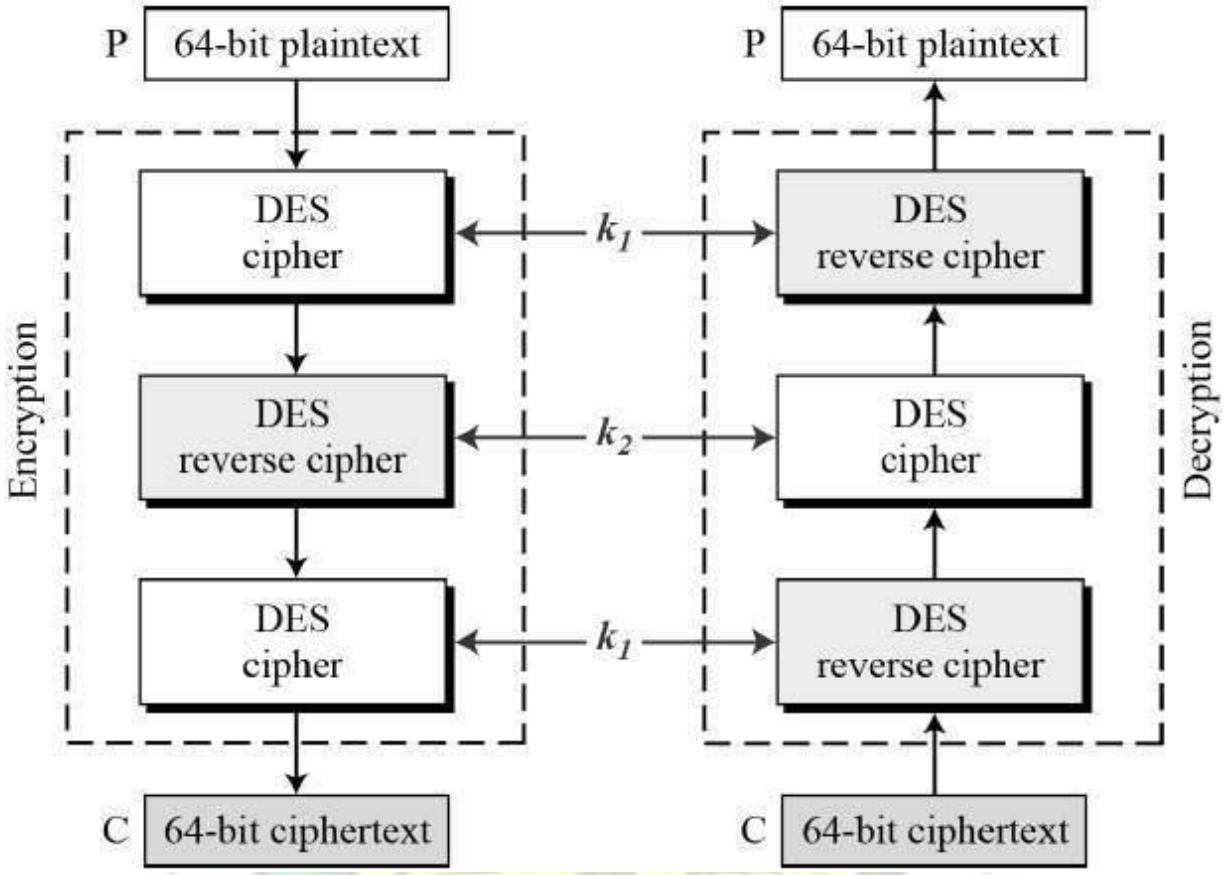


Figure 2-1 Encryption and decryption process of TDES

Given a plaintext message, the first key is employed to encrypt the plaintext; The second key is also employed to decrypt the encrypted message. Since the second key is not the right key but in a new form, this decryption just scrambles the data further. The twice-scrambled message is then encrypted again with the first key to yield the final ciphertext (Grabbe, 2011).

According to Alanazi et al, (2010), There has always been a suspicion of Triple DES because of how it works, since the original Algorithm (DES) was not designed to work this way; but no serious flaws have been uncovered in its design.

2.4.3 Theories backing Encryption

A message in transit or Storage may be protected by encryption (Fig. 2-2). *M* being the input represents plaintext. The cipher text $C = f(K, M)$, an incomprehensible form of the original plaintext, is computed as a function and a finite secret cipher key *K*. By applying an inverse transformation $M = f^{-1}(K, C)$, the plaintext may be recovered by the valid receiver from the cipher text. The sender and receiver will both share a secret key *K* that should be made available only to the two parties using a secured means (Dömstedt & Jansson, 2001).

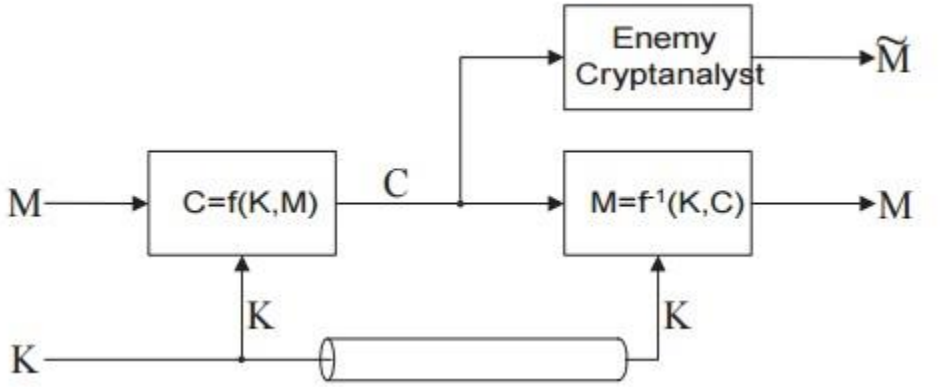


Figure 2-2, *source :* (Dömstedt & Jansson, 2001)

Some ciphers are implemented in software, others in Smart-Cards, FPGAs etc. and requires different implementation techniques. A mismatch between the application area, selected cipher, and target technology may decrease the technical efficiency obtained. It is obvious that no matter how efficient and flexible a cipher may be, it will not be optimal enough to meet these challenges. Therefore, a cryptographer will have to implement a cipher that includes general computational process with all construction parameters kept secret; this will make it difficult for a cryptanalyst to solve (Dömstedt & Jansson, 2001)

The most basic method of attack for any cipher is brute force; where each key is tried until the right one is found. The key length is the determinant of possible number of keys which makes this kind of attack feasible. The strength of an encryption is tied directly to the size of key. Unfortunately, the more the size the more resources required for computation.

Chapple, (2010) argued that, encryption is a data-centric security control; it does not protect your physical device but rather prevents unauthorized users from gaining access to your information. Encryption cannot prevent someone from hacking into your system with an inappropriately configured firewall. It will, however, prevent the hacker who gains access to a device from stealing sensitive data.

2.5 IMPORTANCE OF HEALTH RECORDS

According to Marinič, (2015), a proper health record database of patients helps in the treatment of patients. Proper monitoring of the health, planning and treatment is the resultant proof of consistent recording by doctors, nurses and other clinical staff. The growth of digital medical records databases ensure that, healthcare becomes more cost-effective and result in improved patient outcomes. Data-driven medical records will place medical professionals on the cutting edge of providing patient care; these tools aid them catch human error, monitor effectiveness of treatments, track therapies, and make predictions about outcomes (Reina, 2014).

2.5.1 Health Level Seven (HL7)

It is a not-for-profit, ANSI-accredited standards developing organization that provides a comprehensive framework and related standards for the exchange, integration, sharing, and

retrieval of electronic health information to supports clinical practice and the management, delivery and evaluation of health services (HL7 A. , 2010)

HL7 interface engines are software which functions as a link between different systems. They monitor different types of communication points and interfaces, and perform actions based on rules set by an organization (Orion, 2013)

2.5.2 HL7 Standards

HL7 works with numerous standards (Messaging Standards Conceptual Standards, Application Standards, and Document Standards).

Messaging standards describe how information is put together and transmitted from one system to the other.

Conceptual standards: ensures that, information is transmitted between systems without any loss of meaning or context.

Application standards allow the interaction of software systems by determining the implementation of business rules.

Document standards indicate the location of the information, and the type of information included in a document (Care, 2013).

2.5.3 HL7 Architecture

HL7 messages transmit data between different systems. An HL7 message is made up of a collection of segments in a classified sequence, with these fragments or segments being voluntary, required

or repeatable (Microsoft, 2015). The HL7 message type defines the rationale for the message being sent, and exists in each HL7 message. The types of messages are recognized using a three-character code, and they are collectively used with a trigger event. An HL7 trigger event can be described as a real-world event which facilitates communication and the relaying of messages, and presented as a subset of the message type. The trigger event and message type are both present in the MSH-9 field within the message (Microsoft, 2015). A typical example of the MSH-9 field is likely to contain the value ADT-A01. This implies that, the HL7 message type is ADT, and the trigger even is A01. In the HL7 Standard, "patients admit" message is referred to as ADT-A01 message. Every trigger event and message type within an exact HL7 version has a distinct format. There exist some triggers and message types that came with the exact format, like ADT-A01, ADT-A04, ADT-A05 and ADT-A08. In most cases, their formats vary extensively.

When receiving or sending messages, it is paramount that the correct trigger and message type is chosen for use when putting together the message processing. When a different trigger format and message type is received than the expected, data can be misinterpreted and/or lost.

The most widely used HL7 message types are:

- ACK – General acknowledgement
- ADT – Admit discharge transfer
- BAR – Add/change billing account
- DFT – Detailed financial transaction
- MDM – Medical document management
- MFN – Master files notification
- ORM – Order (Pharmacy/treatment)

- ORU – Observation result (Unsolicited)
- QRY – Query, original mode
- RAS – Pharmacy/treatment administration
- RDE – Pharmacy/treatment encoded order
- RGV – Pharmacy/treatment give
- SIU – Scheduling information unsolicited

HL7 is normally associated with a trigger event and has a hierarchical structure. The trigger event of the HL7 standard is defined as "an event in the real world of health care (that) creates the need for data to flow among systems", (Microsoft, 2015). There is a relationship between each trigger event and an abstract message. This sets up the type of data needed by the message to back the trigger event. An abstract message is made up of segments, and contains the rules of repetition and addition for those segments. The table below depicts an example abstract message that is associated with the trigger event A04 – Register Patient (Microsoft, 2015).

Trigger event	Abstract message
ADT^A04^ADT_A01	Admissions, Discharge, and Transfer
MSH	Message Header
EVN	Event Type
PID	Patient Identification
[PD1]	Additional Demographics
[{ ROL }]	Role
[{ NK1 }]	Next of Kin / Associated Parties
PV1	Patient Visit
[PV2]	Patient Visit - Additional Information
[{ ROL }]	Role
[{ DB1 }]	Disability Information
[{ OBX }]	Observation/Result
[{ AL1 }]	Allergy Information
[{ DG1 }]	Diagnosis Information
[DRG]	Diagnosis Related Group
[{	
PR1	Procedures

[{ ROL }]	Role

Table 1-1, HL7 Message structure

}]	
[{ GT1 }]	Guarantor
[{	
IN1	Insurance
[IN2]	Insurance Additional Information
[{ IN3 }]	Insurance Additional Information - Cert.
[{ ROL }]	Role
}]	
[ACC]	Accident Information
[UB1]	Universal Bill Information
[UB2]	Universal Bill 92 Information
[PDA]	Patient Death and Autopsy

The square brackets in table 1-1 "[", "]" show that one segment or group of segments is optional, whereas braces "{", "}" show one segment or group of segments are repeated.

A segment is described as a group of fields where each matches to a particular data type. The fields can have a complex or simple structure consisting of components based on the rules set up in their data-type definition. Some components will be made up of subcomponents in order to maintain complex data types (Microsoft, 2015).

2.5.4 HL7 Message Parts

An HL7 message is made up of the following parts: components, data fields, and segments optionally subcomponents. The hierarchical structure of the HL7 message is:

I. Segment

II. Data Field

III. Component

IV. Subcomponent (optional)

2.5.5 HL7 Segments

The segments are known as the logical grouping of data fields. They are at the highest level (depth 1) of the (Message) hierarchy. Every segment is with a name made up of a three-character literal value. The table below depicts segment names within the ADT message types.

Table 2-1: Segments

Segment code	**Description**
MSH	Message Header
EVN	Event Type
PID	Patient Information

The HL7 messages are made up of a message header and body. The MSH segments describe the message header and all other types of segments which form the body of the message.

2.5.6 Data Fields

A data field is a string of characters that take place at depth two (2) of the message hierarchy. Data types define data fields both simple and complex.

2.5.7 Components and Subcomponents

Components and subcomponents also have the data within data fields. Components and subcomponents can or may repeat within the same field.

2.5.8 HL7 Security

HL7 employs a number of security mechanisms to secure patient data both at rest and during transit; these include:

Secure Socket Layer (SSL): is the standard security technology for establishing an encrypted connection between a web server and a browser. The connection ensures that all data transmitted between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers (Com, 2015).

Virtual Private Network (VPN): A VPN is a technique used to add security and privacy to public and private networks, like the Internet and WiFi Hotspots. They are most often used by organizations to protect sensitive data (Gilbert, 2015).

Internet Protocol Security (IPSec): is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session (IPsec, 2016).

HIPAA Encryption: is a solution for protecting medical data at rest. HIPAA encrypts data and drives in order to prevent unauthorised access (Sookasa, 2015)

2.5.9 Shortfalls in HL7 Security

According to Encryption (2007), encryption of data in transit require a lot of technical overhead and management in order to allow for secure creation of keys, transmission of those keys and PKI infrastructure management just to mention a few. They stressed that encryption is not currently a concern of the HL7 protocol, but should, rather be addressed by a separate protocol such as SSL (HTTPS). Meanwhile, HL7 data is not transmitted via HTTPS but rather transmitted directly using TCP/IP.

HL7 recommends the use of VPN. Unfortunately, the design and security implementation for a virtual private network can be cumbersome. This implies that, there is the need for a professional with a high level of skills and understanding for the best type of VPN configuration and some of the security issues that can occur when using a VPN (Blog, 2015).

The reliability of a VPN can become a factor depending upon the internet service provider (ISP). If the VPN makes use of the Internet, it is essential to work with a provider that can guarantee minimal downtime (Blog, 2015).

VPN is noted for incompatibility issues when it comes to scalability and changing of vendors. When the need arises to expand, an organization using VPN will face challenges doing that. The use of mobile devices on a wireless network to establish connectivity to a virtual private network can create security problems (Blog, 2015). The HIPAA encryption that is used to secure HL7 data

is only applicable to data at rest. Data on transit is not protected by HIPAA; this makes data vulnerable since it is decrypted before transmission.

The security options recommended by HL7 cannot really guarantee the security of patient data during transit. If an organization fails to implement any of these security mechanisms, patient data will be compromised during transit.

This research is proposing a solution that will be part of the HL7 encoding and decoding process; where patient data will be encoded using HL7 standard then, encrypted with A5AR3MY Algorithm before transmission. When the encrypted data gets to its destination, it will be decrypted with A5AR3MY Algorithm and subsequently decoded, thereby ensuring data security during transit.

2.6 RELATED WORK

Weerasinghe et al., (2008) proposed a protocol that provides security and privacy services such as user anonymity, message confidentiality, message privacy, user authorization, user authentication, and message replay attacks. The patient is validated with the proposed protocol at the healthcare service to make sure they are registered patient. The identity and medical records of the patient is made anonymous and linked in a single report. The real identity of the patient can be securely reverse tracked: Thus using the temporal identity of the patient to determine his or her real identity.

Chao, Twu, & Shu, (2005) proposed a patient-identity security system, that comes with an identity cipher and decipher, and a user-authentication protocol, that will ensure the authentication and confidentiality of patients' electronic medical records (EMRs) at rest and during transit. To sustain the EMR confidentiality, three logical-based functions and a datahiding function is used by the identity cipher/decipher to encrypt/decrypt a patient's identifying data and medical details in an

EMR. The scrambled text of the patient's identifying data is patient-EMR related, whereas that of medical details is healthcare agent-EMR related. The userauthentication protocol which is based on a public key infrastructure (PKI) uses certificates and dynamic cookies for identification/verification in order to support the authentication of an EMR. Anderson, (2006) focused on the move by UK government to centralise patient records whilst putting the security of medical records at risk and will in turn jeopardise patient confidentiality. There are claims that privacy issues will be curtailed by mechanisms in place in the centralized system by way of role based access controls which are expected to limit patient record access by clinicians who claim to have a relationship with patients. This will be done by a page popping up asking the clinician whether they have the consent of the patient to view their medical records. It is very tempting for the clinical staff to click yes in order to view the medical records.

He further explained that they will make use of 'Sealed Envelops'. This is a feature that will allow sensitive date of patients to be sealed; this is to prevent ordinary clinicians from having access to that sensitive data. If a clinician outsides the care group access the data, an alert is sent to the privacy officer of the care group. There is a further option of the record to be 'sealed and locked so that clinicians outside the care group will not even know of its existence. They hope to build patient's confidence by deploying this feature. However, other systems that communicate with the centralised system will have access to the sealed and lock data. Medical records will also be made available upon demand by the law. The data will be 'anonymised' just by merely replacing the name and address with the postcode, date of birth and NHS number. This is a clear indication that the level of confidentiality here is minimal.

(Anderson, 2006) proposed the facilitation of the secondary record access where sealing will be accomplished by marking data with HL7 codes which is created for that purpose rather than encrypting the data and keeping the private key on the same patient card.

A critical look at (Anderson, 2006) proposal indicates that it is a laudable idea. This is because HL7 facilitates seamless communication between two hospital management systems at the same time making patient records difficult to understand. On the other hand there is a disadvantage with just using the HL7 for data transfer. What happens when a user who is very familiar with the HL7 codes chances upon these sensitive data of a patient? They can easily make meaning out of the HL7 codes. In this case using only HL7 for systems communication is not enough. There should be a way to further make the sensitive data difficult to understand even when you are able to access it.

Benyoucef et al., (2011) investigate the suitability of web service orchestration and choreography, two closely related but fundamentally different methodologies for modelling web service-based healthcare processes. The study showed that Hospital Management systems will have to interact with each other in order to exchange data. Data which is the lifeblood of healthcare is very paramount in the healthcare industry implying that it will have to be available for the right task at the right time. This can be achieved by use of protocols or communication channels such as HL7 (Morad, Craig, Amir, & Ali, 2011).

Security was one of the important factors they indicated must be considered for healthcare systems development. This is because models are the blue print of systems; they should represent security features as well.

They also talked about privacy which is currently an issue and requires a lot of attention. They therefore proposed embedding privacy features in modelling languages. Privacy is vital in

healthcare as most processes involving interactions with other organizations such as insurance companies, police departments, external laboratories, and other healthcare enterprises, carry private patients' data as well as private implementation details about internal processes.

The recommendations given above are essential, however, the limitation to the recommendations is the fact that they failed to add a precise solution on how to achieve security and privacy in patient data access and exchange. This is a growing concern to every individual who patronises health services in a way or the other.

Ronan, James, & Manfred, (2011) identify the gap that currently exists between enterprise and consumer-focused mash-up tools in terms of personalized, trusted collaboration. They describe how Sqwelch, a semantically enabled mash-up maker, addresses this gap during the design of mash-ups and in their execution. They proposed the enabling of data privacy by using Sqwelch to execute trusted collaboration by placing control of data in the hands of owners. This will allow them specify who sees what. The Sqwelch environment requires the passing of messages between components of Telehealth applications; HL7 was the protocol that they chose.

They proposed the control of access to sensitive data by the owner of that data. However, they were of the opinion that the introduction of security elements has the potential to make the platform more difficult to use. Hence, their solution to that problem was Role Based Access Control (RBAC) (Ronan, James, & Manfred, 2011). This solution works only when the system is within an organization. The question to ask is, will this same solution protect data whilst on the network? What happens during the exchange of messages via different systems? How secure is the data being transferred? There is a chasm in the solution provided above.

Konstantinos, (2013) looks at the critical success factors of Service-Oriented architecture in healthcare. Due to the nature of healthcare systems, there is a need to increase SOA adoption

success rates as the non-integrated nature of healthcare systems is responsible for medical errors that cause the loss of tens of thousands of patients per year.

SOA will help healthcare institutions to comply with the new laws/regulations. As medical data and services are progressively more exposed among healthcare partners and patients, conformity with current and commonly revised laws and compulsory standards are set by governments to insure safety and security of the exchange process. HL7 is one of such Standards.

One will agree that, the compliance of compulsory standards set by government is not enough to ensure patient confidentiality or data security. More will have to be done to ensure these features in the health care sector (Konstantinos, Marinos, Paulo, & Da, 2013).

Themistocleous (2015), identified that data security and patients' confidentiality are clearly significant challenges to healthcare, and beyond the boundaries organizational structures and roles, specific testing, standards, policies and best practices are needed.

Although the challenges have been identified, there are no solutions to address these challenges. It is apparent that, a lot of researchers are concentrating on how to secure data and by so doing ensure patient confidentiality. It is an established fact that, there is nothing like hundred percent (100%) security. It is difficult to hide data that is accessed every now and then. How do you hide data that is being transferred on a network, or messages that are exchanged by systems? Messages travelling on a network can easily be intercepted by any user on the network. When the data is being transferred using HL7, it becomes quite obfuscated but not completely secure.

This is because anybody with the requisite skills in the HL7 codes can make meaning of the intercepted HL7 message. Hence HL7 alone is not the solution to ensuring patient privacy and data security.

To ensure that data intercepted on the network is not used by the wrong person, A5AR3MY Algorithm will have to be implemented. The system sending the HL7 encoded messages will have to encrypt the message at the sending stage. In this case, if any unauthorised user intercepts this message, they cannot make meaning out of the message. They will require a private key to be able to decrypt the encrypted message which is already encoded using HL7 standard. When the message gets to its destination, it will then be decrypted using the private key of the encryption algorithm. A strong encryption Algorithm will require that it is fully open to public scrutiny and comment to ensure a comprehensive, transparent analysis of the design (Rouse, 2014).

The main reason why this study is required, is because patient's data is confidential and must be secured. HL7 messages traversing a network will have to be secure from unauthorised users to ensure data integrity.

CHAPTER 3

METHODOLOGY

3.1 INTRODUCTION

This chapter explains the research methodology that was used to develop the system. This study adopted the design science research methodology in developing a system to meet its objectives. The study explored detailed steps and processes used in the subsequent sections.

3.2 DESIGN SCIENCE METHODOLOGY

According to Peffers & co. (2007), whilst natural sciences and social sciences seek to understand reality, design science seeks to produce objects that serve the purposes of humanity. Wieringa, (2013) also argues that, natural science and social science are problem oriented whereas design science is solution oriented. In the computer science and engineering domains, there have been the realizations of lots of benefits from practical application of design science research (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007). For this reason, it was appropriate to adopt this approach purposely for this study. Each of the steps involved in this methodology has been elaborated below to suit the purpose of this study.

3.2.1 Problem Identification and Motivation

Based on the fact that patient confidentiality is amongst the core responsibilities of medical practice, health care providers are required to keep personal health information of patients private unless the patient provides consent to release the information (Bord, 2013).

According to Cod (2013), a confidential relationship between physician and patient is crucial for the free flow of information required for good medical care. Trust in the physician-patient relationship is likely to diminish if the confidentiality of this information is not protected. Patients' privacy is paramount because any disclosure of personal health information such as the HIV status of the patient may result in stigmatization, unemployment, and denial of medical benefits. In

addition, patients are likely to suffer financial losses from illegal transfer of finances if billing information is accessed by unauthorised staff (Mweebo, 2014).

There has been an evolution of health records keeping from pen and paper to the adoption and implementation of electronic health records and health information systems. This can be attributed to the many benefits that come with digital information. Medical records at rest can be secured by encryption techniques, but data on transit is quite difficult to secure. Not all medical records use SSL/TLS during data transmission thereby exposing patient data to attackers (Manes, 2014).

With the inception of disparate health information systems, it has become necessary to enable a common means of communicating patient information between health facilities, protecting information between these facilities is key. This can be achieved through the implementation of an enhanced encryption algorithm.

3.2.2 Suggested Solutions

With the challenges indicated in chapter II, the study sought to develop an Enhanced TDES Algorithm. The suggested solution took into consideration an investigation of securing data during transit. It also considered seamless data exchanged using HL7 messaging standard.

It was evident most health facilities use HL7 for data exchange without securing the data being transmitted. If the A5AR3MY Algorithm was part of the HL7 message standard, it made security a default feature.

3.2.3 Design and Development

The proposed Algorithm aimed at ensuring patient data is protected during transit. To ensure this, the application was segmented into five parts.

First was to provide a platform for various health facilities to configure their settings. Using the available segment fields provided by the messaging standard, various facilities were used to specify or map their local database fields to the segmented fields, to ease the retrieval and generation of HL7 messages, as well as capturing the data from the message to a local database. Also, an interface was made available to the facilities, to specify an IP address and a port number through which HL7 encoded messages was transmitted.

The second part considered providing a portal for setting the necessary parameters to generate the desired message. After the message was generated, it was parsed for conformance to the standards. The next stage dealt with hashing a private key and using it to encrypt the HL7 message that was transmitted. This made sure it was secured over the network. The next stage considered identifying the facility to receive the encrypted message by selecting the socket which included the IP address and port number specified of the destination facility, and then sending the message to that facility, an acknowledgement in the form of message is received.

The final stage dealt with keeping a log of data in the various segmented fields in the local database to enable the destination facility make good use of the data.

3.2.4 Tools Used

The proposed System was developed based on asp.net C# and made use of Triple Data Encryption Standard (TDES) and MD5CryptoServiceProvider classes of C#, and NHapi a C#.nET version of the HL7 API (Hapi). For the transmission of the HL7 messages, the study adopted the TCP/IP protocol and MSSQL database management systems. The study adopted the software development life cycle methodology in the development of these features.

3.2.5 Evaluation

The performance of the proposed system is assessed based on conformity, performance and consistency of the various modules. Since healthcare data is assumed to be sensitive, it is necessary to uphold a criterion that ensures efficiency. For this reason, the proposed system was evaluated as follows:

3.2.6 Conformance

According to Shackleford (2014), most of today's standards and compliance regulations are mainly concerned with the protection of private data at rest, during transactions, and while traversing network connections. Encryption can be employed for all of them by determining what data you are required to protect, locating the data at rest and in transit and implementing the appropriate encryption technologies. The study implemented an encryption Algorithm that secured data in transit. The private key which is the backbone of this security mechanism is hashed to prevent any reverse engineering.

Since the data to be exchanged is based on a specific messaging standard or protocol, it was necessary to ensure a good level of conformity of generated messages to the implemented standard. To ensure this, two main components (libraries and message parsing function) was evaluated. In assessing the libraries or API, it was necessary to obtain the recent stable version. As mentioned in the previous section, the library implemented in the proposed system was the NHapi, a C#.Net version of the HL7 API (Hapi) which originally is based on java.

Just like Hapi, Nhapi is one of the highly used libraries for the development of applications related to HL7 messages. It contains about eighty eight (88) HL7 datatypes, six hundred and sixty two (662) message groupings, two hundred (200) different message types and one hundred and fifty two (152) message segments. It also contains necessary methods which make it easy to facilitate

the development of applications with the libraries; as part of these methods is the message parser. Taking into account that there are different HL7 standards, the parser is required to validate the messages to ensure conformance to the standard as well as the denoted version.

3.2.7 Consistency

From the CIA (Confidentiality, Integrity and Availability) point of view, availability is ensuring timely and reliable access to and use of information. In the context of this study, in dealing with healthcare data, a lack of availability of access to client databases will be detrimental. It is therefore necessary to ensure availability of patient data. This would ensure timely and efficient retrieval of data. (Stallings, 2011)

Aside the availability of the client side database, it was also important to ensure consistency in patient data. As indicated earlier, a key feature of this study was to ensure safe transmission of patient data. This was meant to ensure facilitation of consistency in patient data. Data integrity is also key. An attacker can intercept data in transit, modify and resend to its destination and this will affect the consistency and integrity of the data. Hence, security during transit will have to be ensured.

3.2.8 Performance

Aside conformance and consistency of the system, it is also necessary to ensure the optimized performance of the system. In ensuring secure data transmission, throughput was measured to determine the efficiency of the system. Throughput is known to measure the number of messages that are successfully delivered per unit time (Network performance, 2016).

CHAPTER 4

OUTLINE OF THE SYSTEM – DATA ANALYSIS

4.1 INTRODUCTION

This chapter contains a range of diagrams which give an outline of the proposed system and its functional requirement. It consists of flow charts, the data flow, context level diagrams and UML diagrams. For the purpose of the study, three main roles were identified to interact with the proposed system. These are the physician, local administrator and system administrator.

The study aimed at coming up with an enhanced TDES Algorithm (A5AR3MY) to secure HL7 data transfer of patient data between Health Information Systems. The data sent was first encoded in the HL7 format, after which the encryption Algorithm was applied to it. It was then sent to the destination address. Upon arrival, it was decrypted and subsequently decoded to make meaning.

This protected the patient information from unauthorised users who will be tempted to intercept and make meaning out of the data.

4.2 FLOWCHART OF THE PROPOSED SYSTEM

According to Radatz and Co. (1990), a flowchart is a control flow diagram in which geometrical figures are linked with arrows which are used to represent operations, data, or equipment to indicate sequential flow from one to another. Various shapes represent different processes. For example, the diamond shape represents decision points, whilst the sphere represents start or stop on a series of activities. The squares are used to show activities and the arrow for depicting the flow of control.

Below are flowchart representations of the proposed system for all three roles identified.

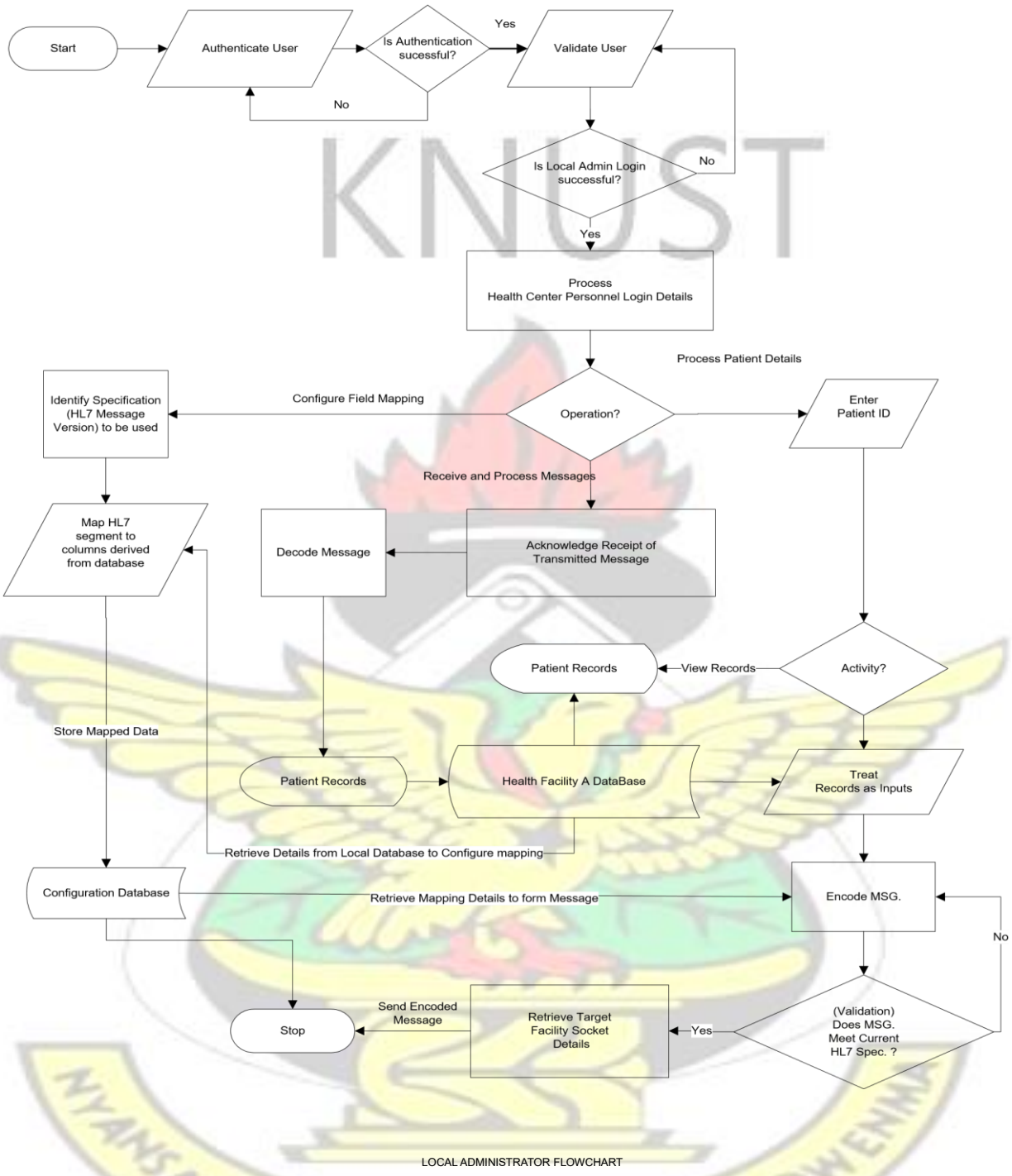


Figure 4-1: Flowchart of Local Administrator

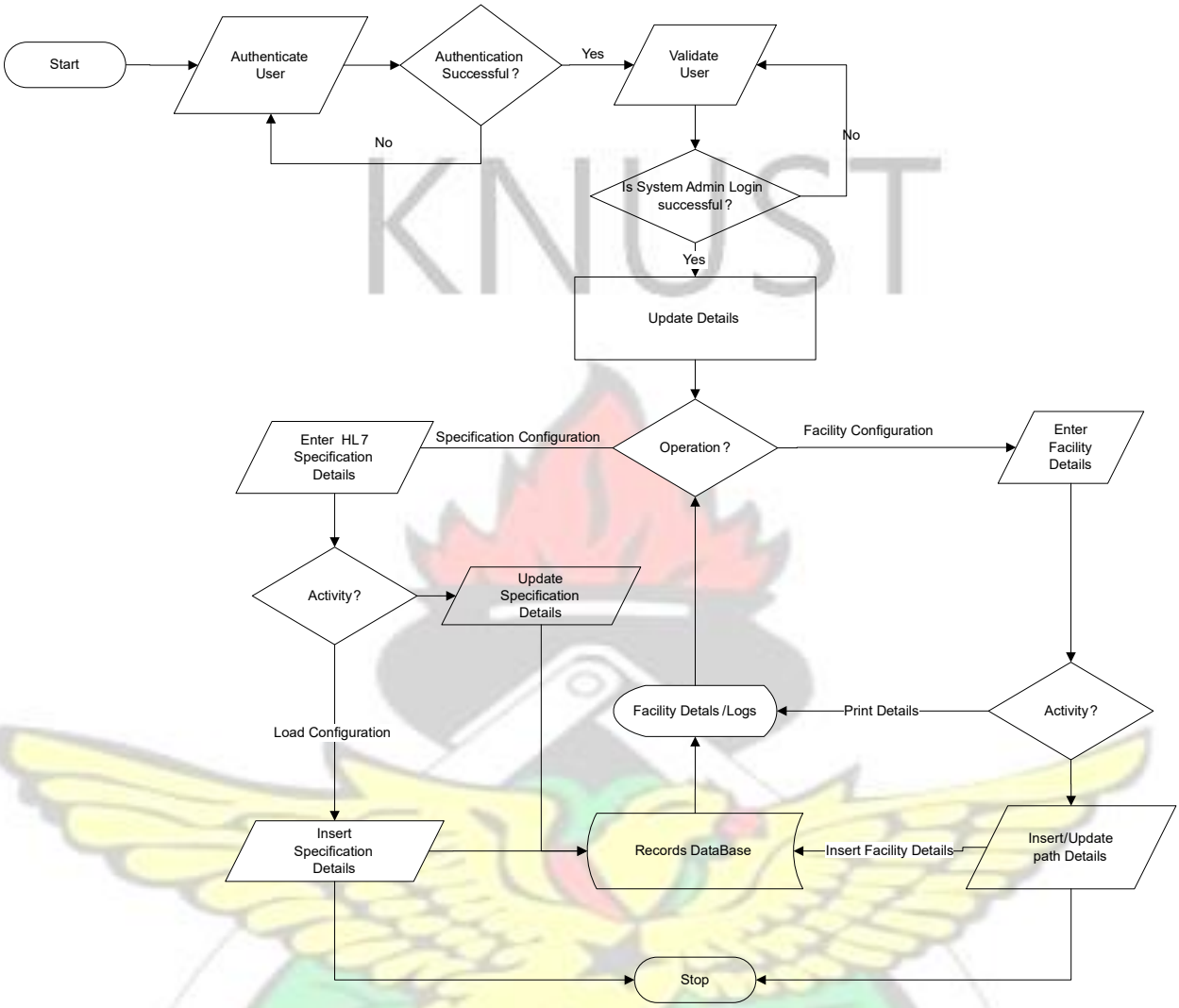


Figure 4-2: Flowchart of System Administrator

4.3 ENCRYPTION ALGORITHM

Step 1: Start

Step2: Set Private Key=XXXXXXXXXXXX

Set Hashing = True

Step 3: Get Plain Text

Sep4: Convert Plain Text to Bytes
Step5: If Hashing=True

Convert Private Key to Bytes

Hash Private Key with MD5CryptoServiceProvider

Else

Convert Private Key to Bytes

Step6: Set Triple Data Encryption Algorithm (TDES) Key= Hashed Private Key

Set TDES Mode to ECB

Set TDES Padding to PKCS7

Step7: TDES.Encrypt(Plain text using Hashed Private Key)

Step8: Release resources used by TDES

Step9: Convert Encrypted Text to Base64

Step 10: Stop

The process begun by setting a private key to a secret key known to the sender and receiver only. According to Rouse (2007), a secret or private key in cryptography is only known to the parties involved in the exchange of secret messages. Patient data can only be encrypted or decrypted using this private key. The private key was hashed with MD5CryptoServiceProvider. A hash function is employed to index the original key or value and used later when data associated with the key or value has to be retrieved. The hashing is a one-way operation and cannot be reverse engineered (Rouse, 2005).

The hashed private key was used with Triple Data Encryption Standard (TDES). TDES is computerized cryptography in which algorithms of block cipher are applied three times to each

block of data. There is an additional security through the increase in key size of TDES (Techopedia, 2012). The Patient data was encrypted with the hashed and encrypted private key.

The encrypted data was converted to base 64 to increase its complexity.

4.4 ENCRYPTION FLOWCHART

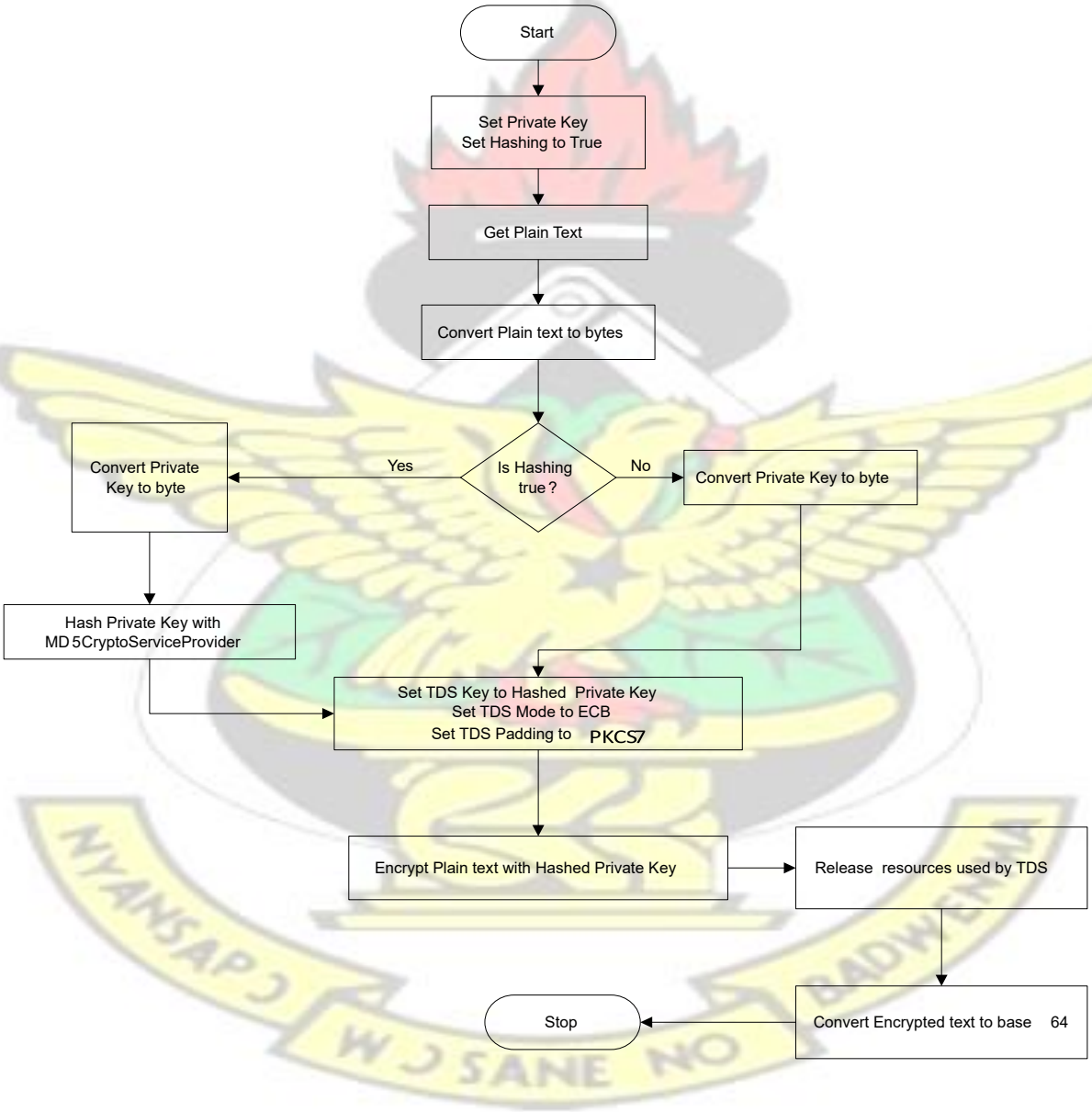


Figure 4-3:Flowchart of the encryption process

4.5 DECRYPTION ALGORITHM

Step 1: Start

Step2: Set Private Key=XXXXXXXXXXXX

Set Hashing = True

Step 3: Get Cipher Text

Sep4: Convert Cipher Text from Base64

Step5: If Hashing=True

Convert Private Key to Bytes

Hash Private Key with MD5CryptoServiceProvider

Else

Convert Private Key to Bytes

Step6: Set TDES Mode to ECB

Set TDES Padding to PKCS7

Step7: TDES.Decrypt(Cipher text using Hashed Private Key)

Step8: Release resources used by TDES

Step9: Get Plain Text

Step 10: Stop

The decryption process is similar to the encryption process. The private key that was used during the encryption process was required during the decryption process. The cipher data (patient data) was converted from base 64 to its encrypted form, and again converted the private key to bytes, and then hashed it with MD5CryptoServiceProvider. The hashed private key was encrypted with TDES. The Patient's data was subsequently decrypted with the hashed private key. The decrypted patient's data now appeared in the HL7 encoded format and is used by the requesting hospital. This

Algorithm ensures that when patient's data is intercepted by an unauthorised user, it is extremely difficult to decrypt it.

4.6 DECRYPTION FLOWCHART

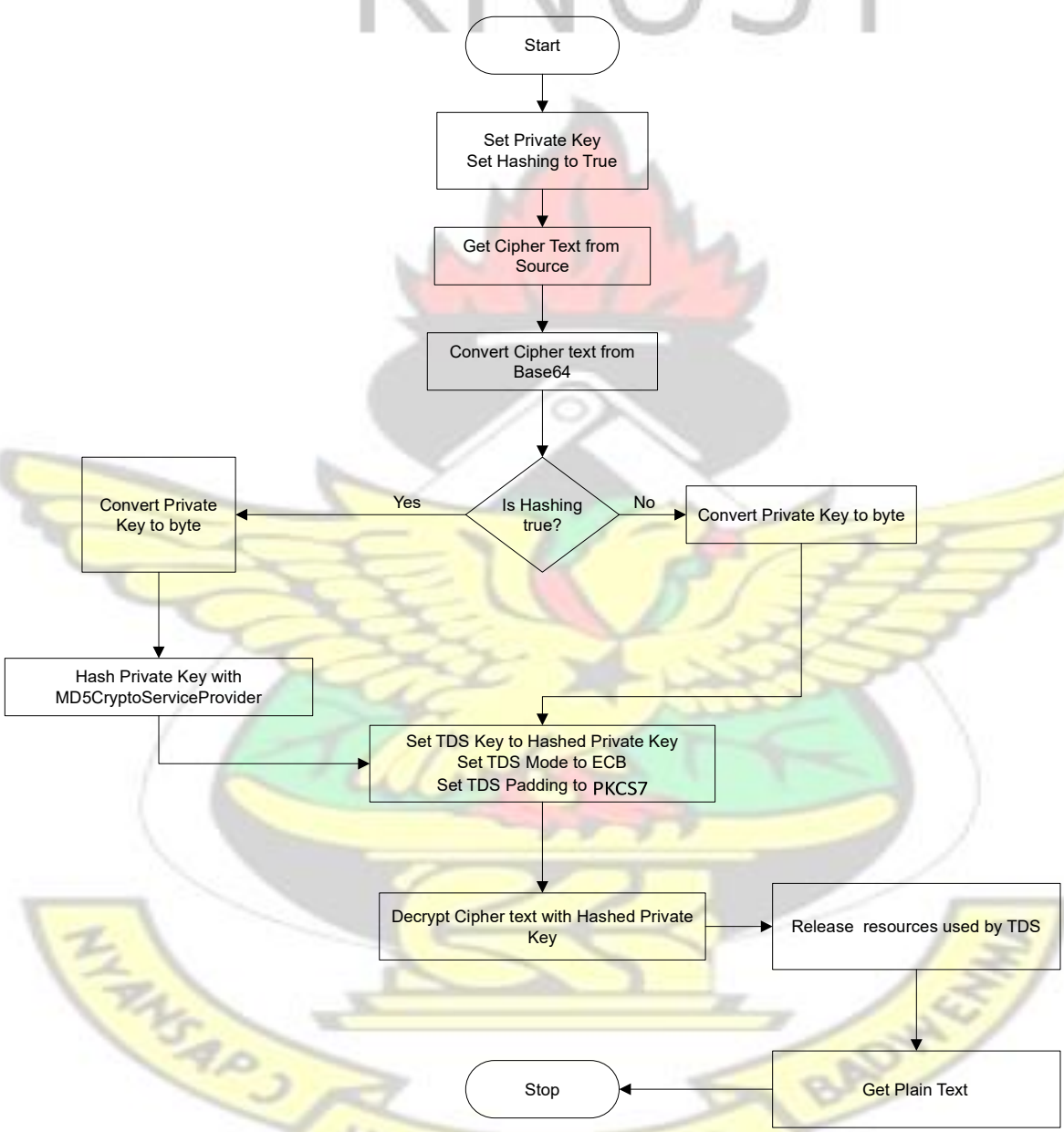


Figure 4-4: Flowchart of the decryption process

The patient's data encryption design indicates that, before a patient's data is transferred, it has to be first encoded using HL7 standard; the data is subsequently encrypted using the hashed private key of the encryption algorithm. It is then sent to the destination. Upon arrival, the encrypted data is decrypted using the private key of the encryption algorithm; after the decryption, the encoded (HL7 format) data is decoded to make meaning to the medical staff who needs the data.

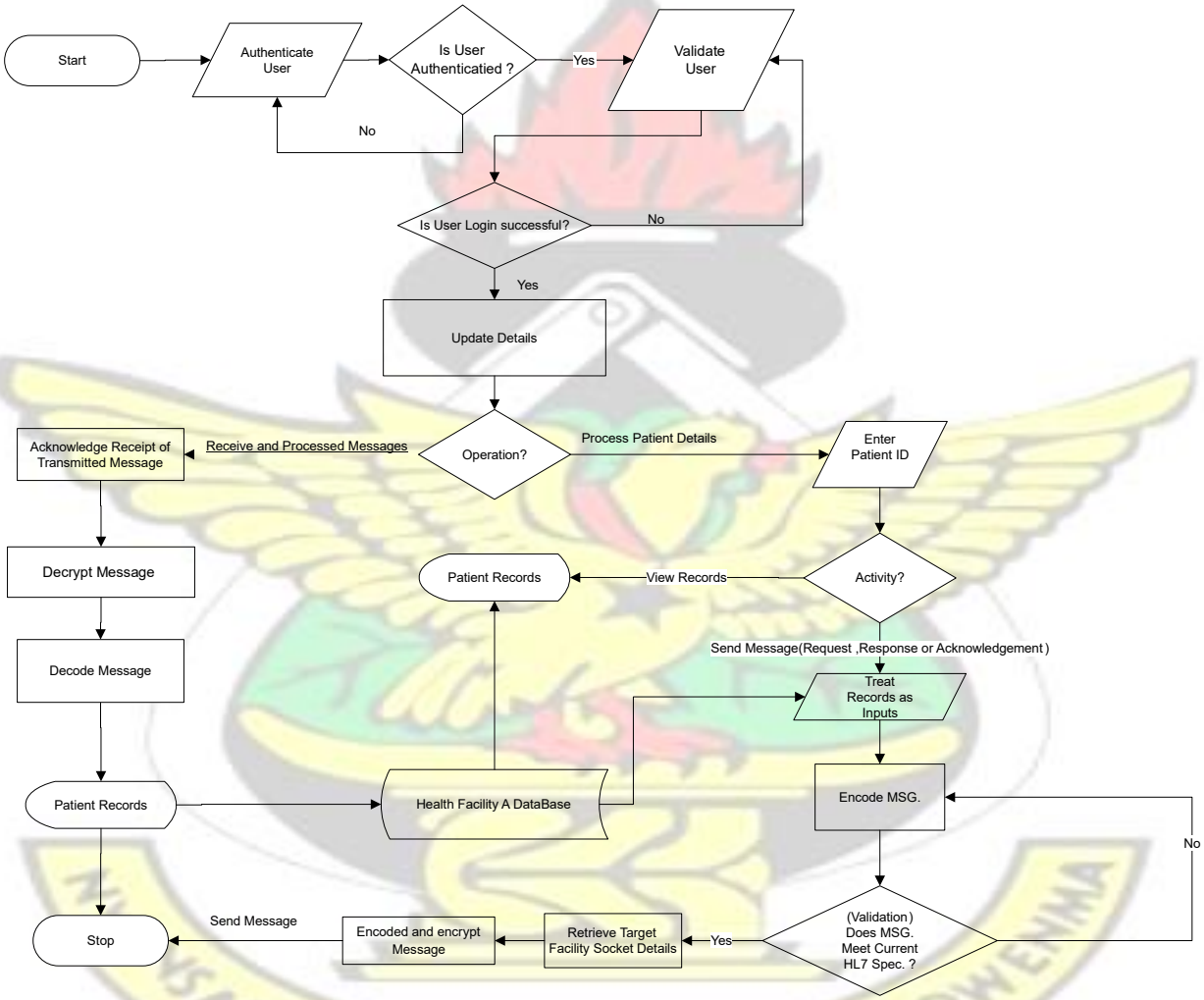


Figure 4-5: Flowchart of Physician

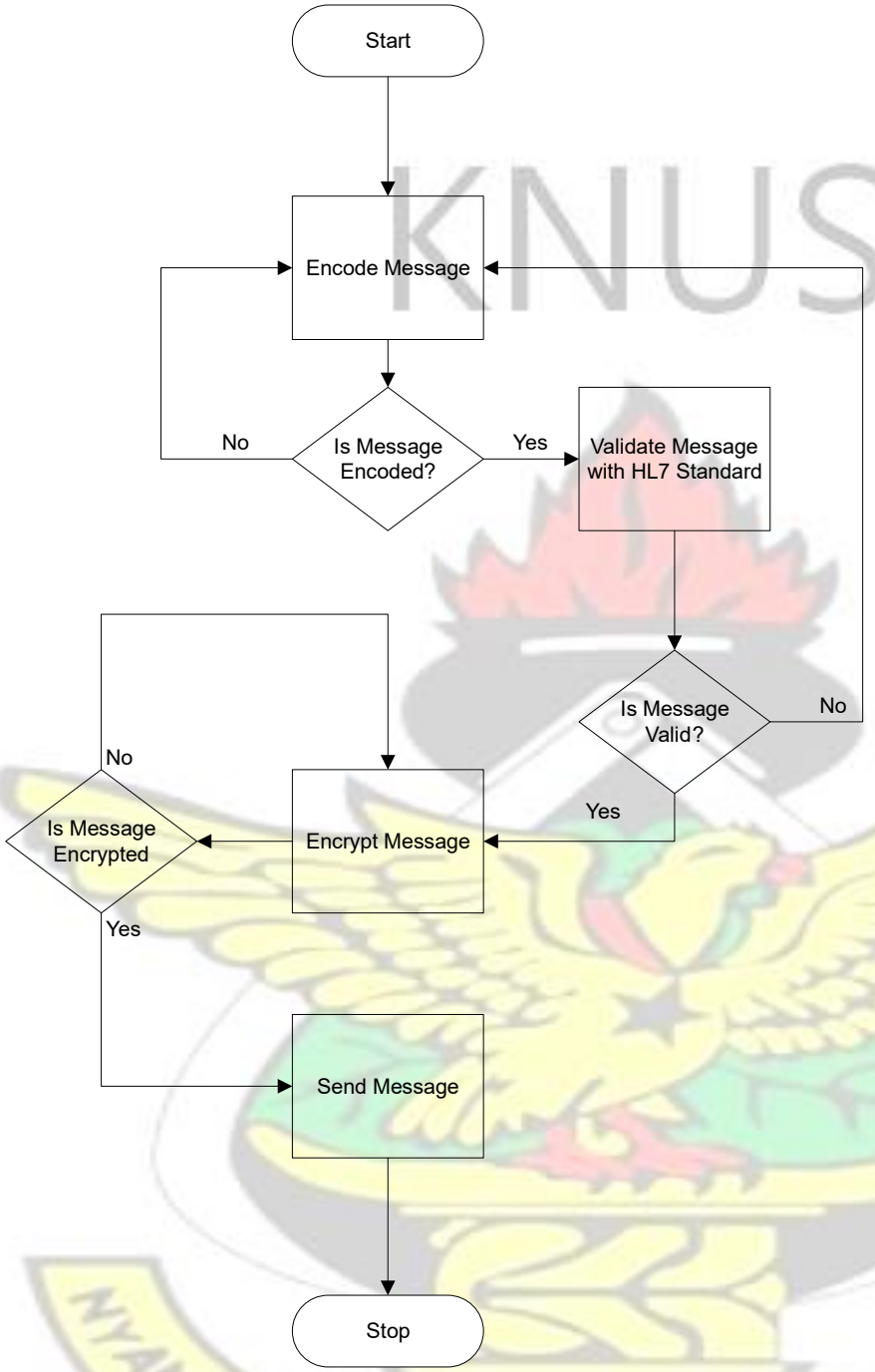


Figure 4-6: Flowchart of message sending process

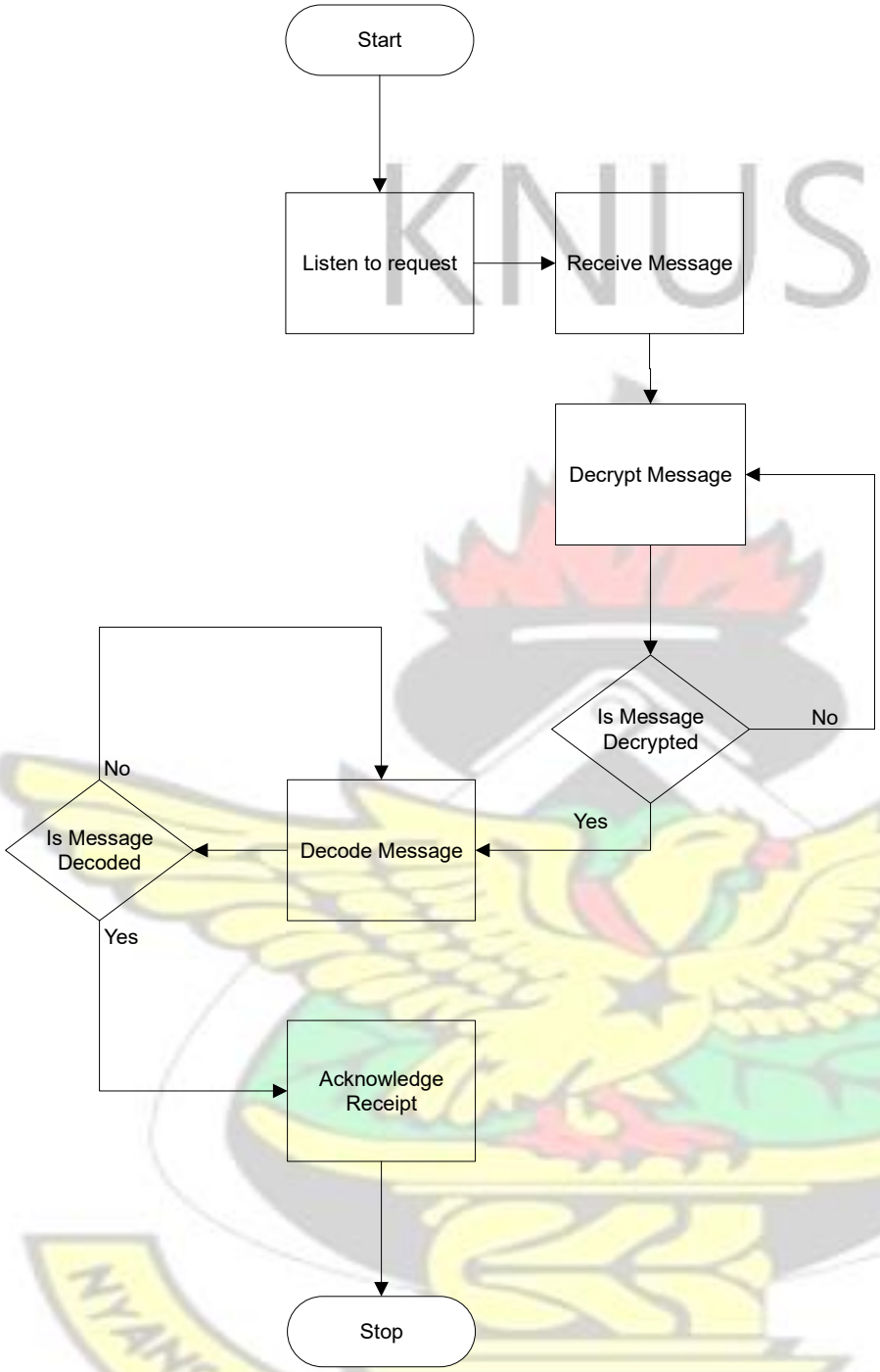


Figure 4-7: Flowchart of message receiving process

4.7 CONTEXT LEVEL DIAGRAM

A context level diagram shows the relationship that exists between the system and the external entities that interact directly with the system. It always has the system in the middle with the entities surrounding it (Wiegers, 2014).

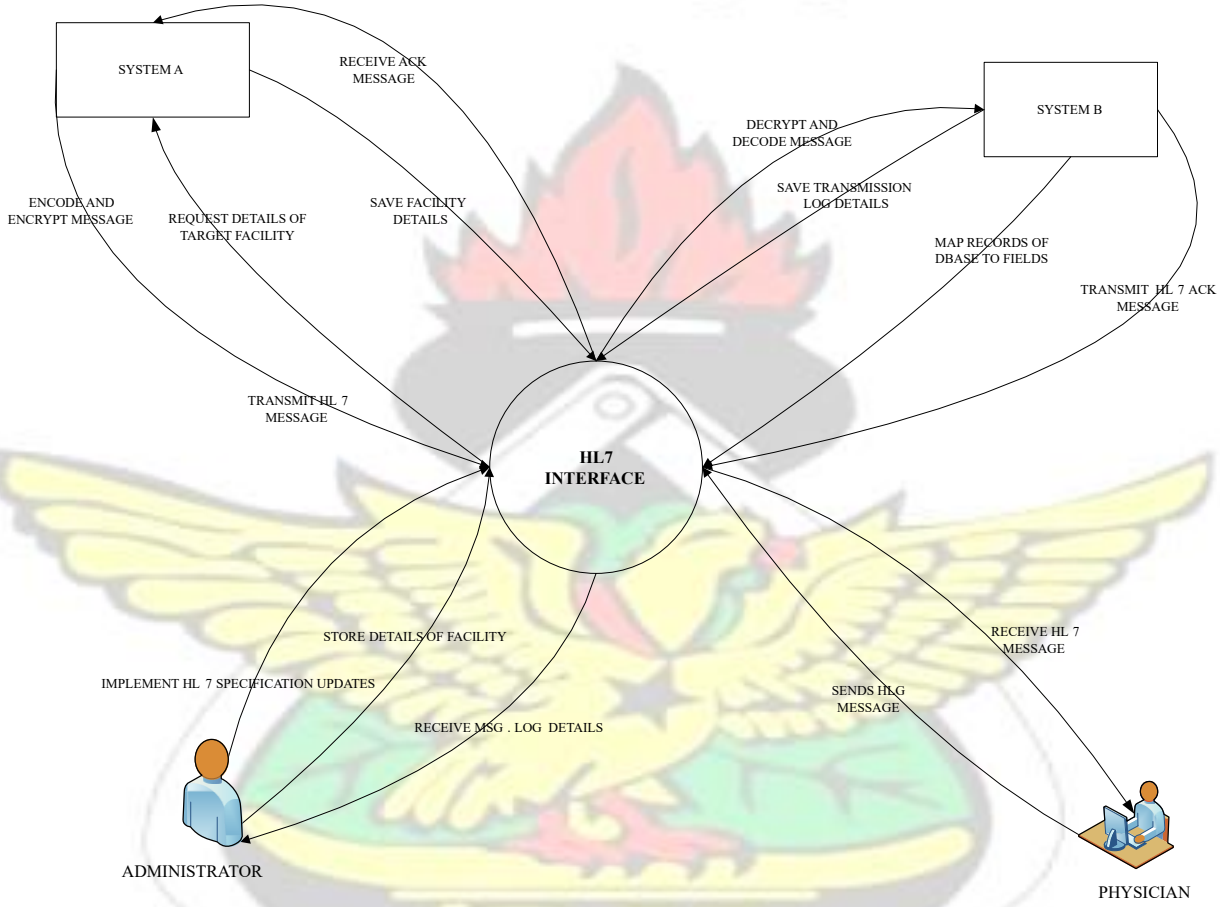


Figure 4-8: Context Level Diagram

4.8. THE DATA FLOW DIAGRAM (DFD)

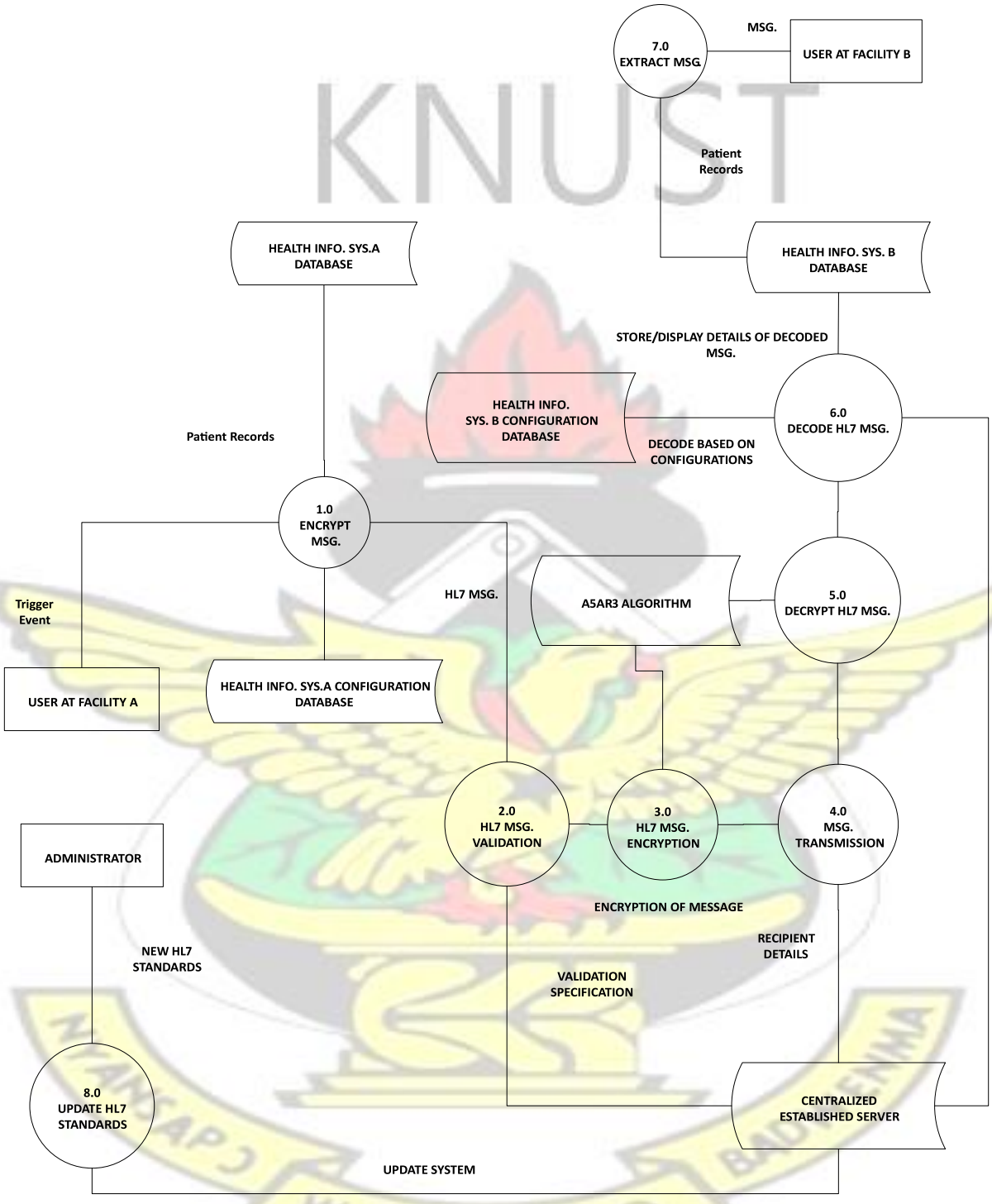


Fig 4-9: data flow diagram of the proposed system

4.4.1 Decomposition of the Sub Processes

The diagrams below shows the various decomposition levels of the processes in the data flow diagram of the proposed health level seven system.

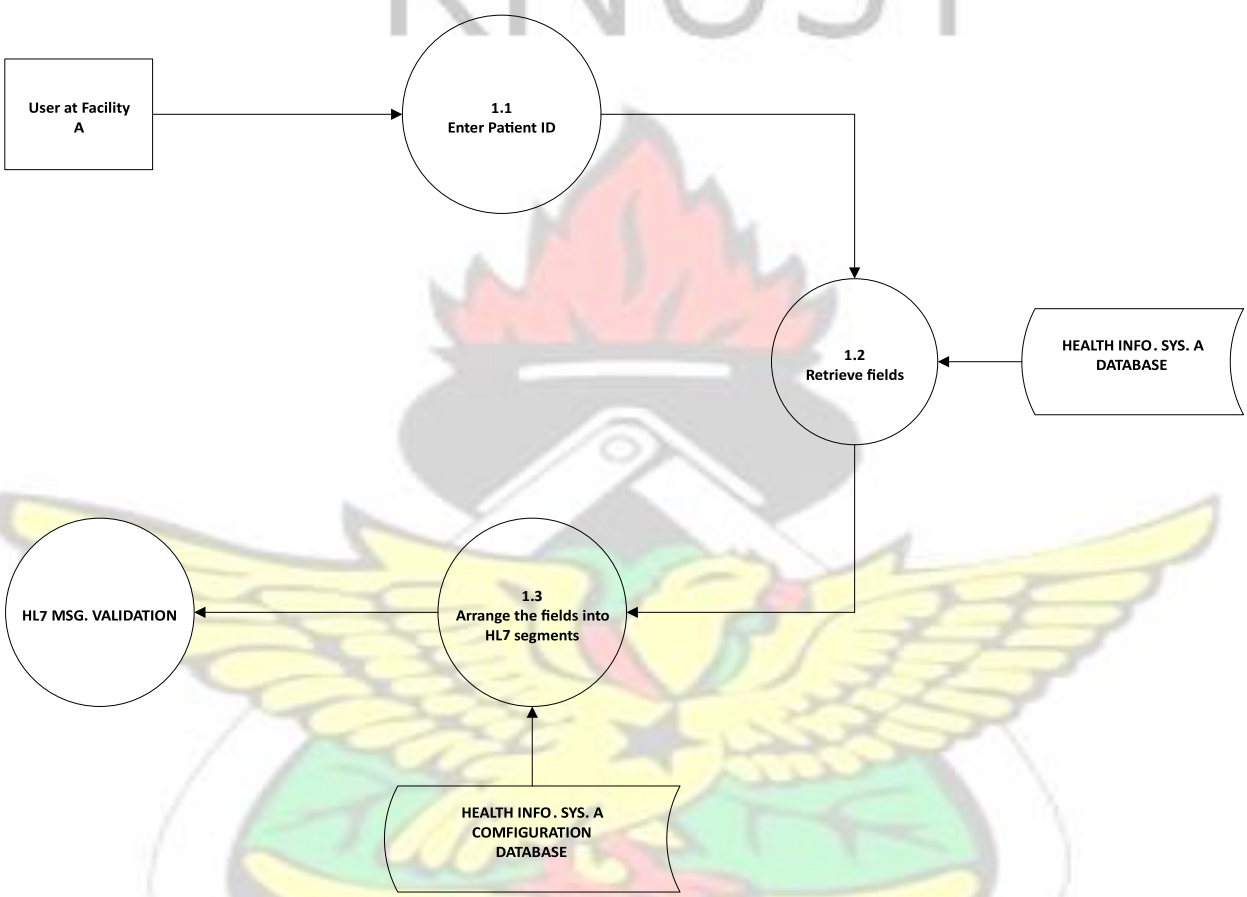


Fig 4-10: Decomposition of Process 1(Encode HL7 Message)

From figure 4-10 above, the user at facility A, queries the local database at *1.1* to retrieve the required data related to a patient at *1.2* and then formats the message at *1.3* based on the mapping configuration saved for the facility between the HL7 specification format and local database. The result is an encoded message which is then validated in the next main process.

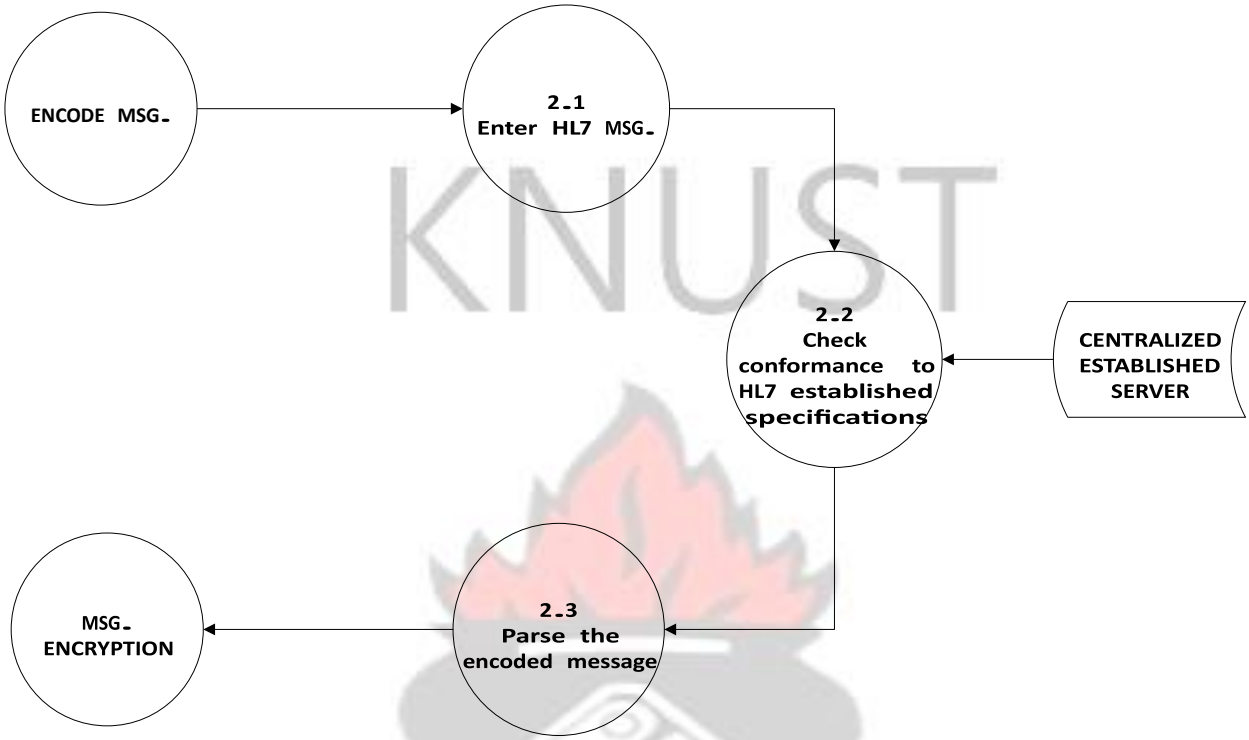


Fig 4-11: Decomposition of Process 2(HL7 Message Validation)

From figure 4.11 above, the received encoded message from process 1 is received at 2.1 and then checked for conformance at 2.2 based on the available version of the standard. From 2.2, the message is then parsed to ensure accuracy of syntax and semantics before it is sent to the next main process for encryption.

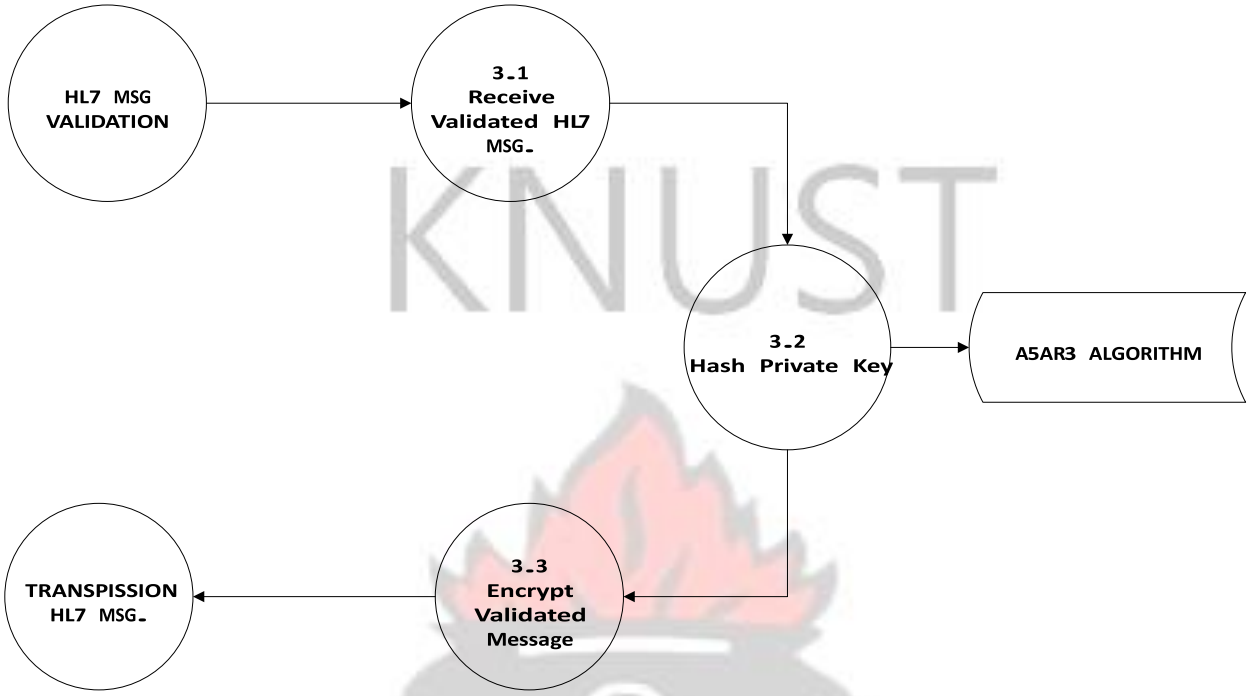


Fig 4-12: Decomposition of Process 2(HL7 Message Encryption)

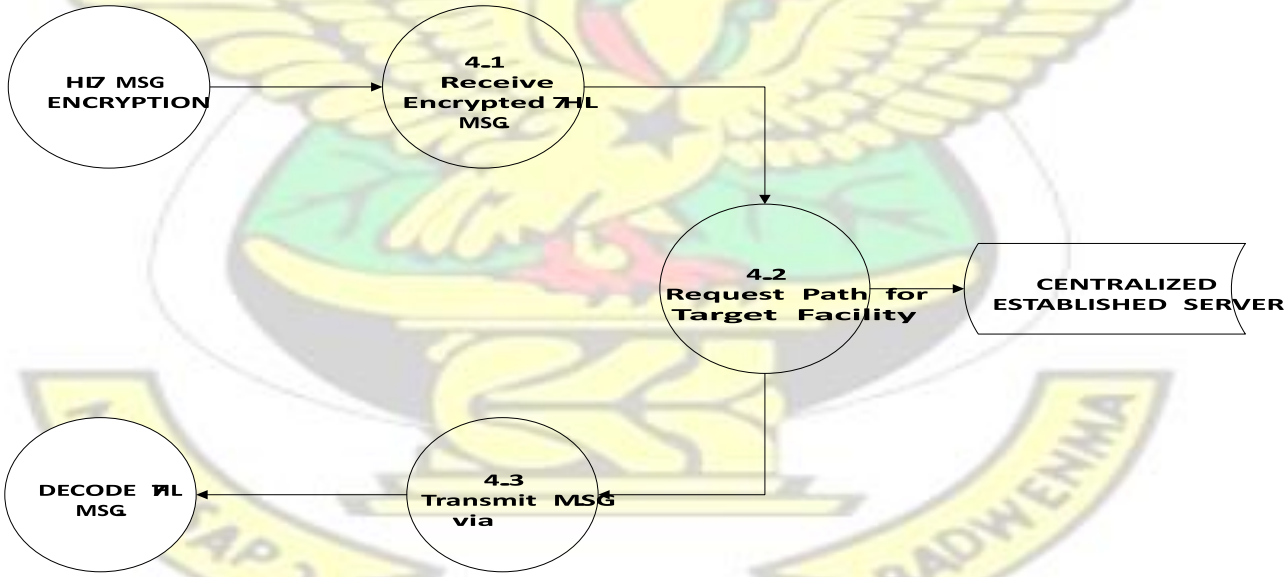


Fig 4-13: Decomposition of Process 2(HL7 Message transmission)

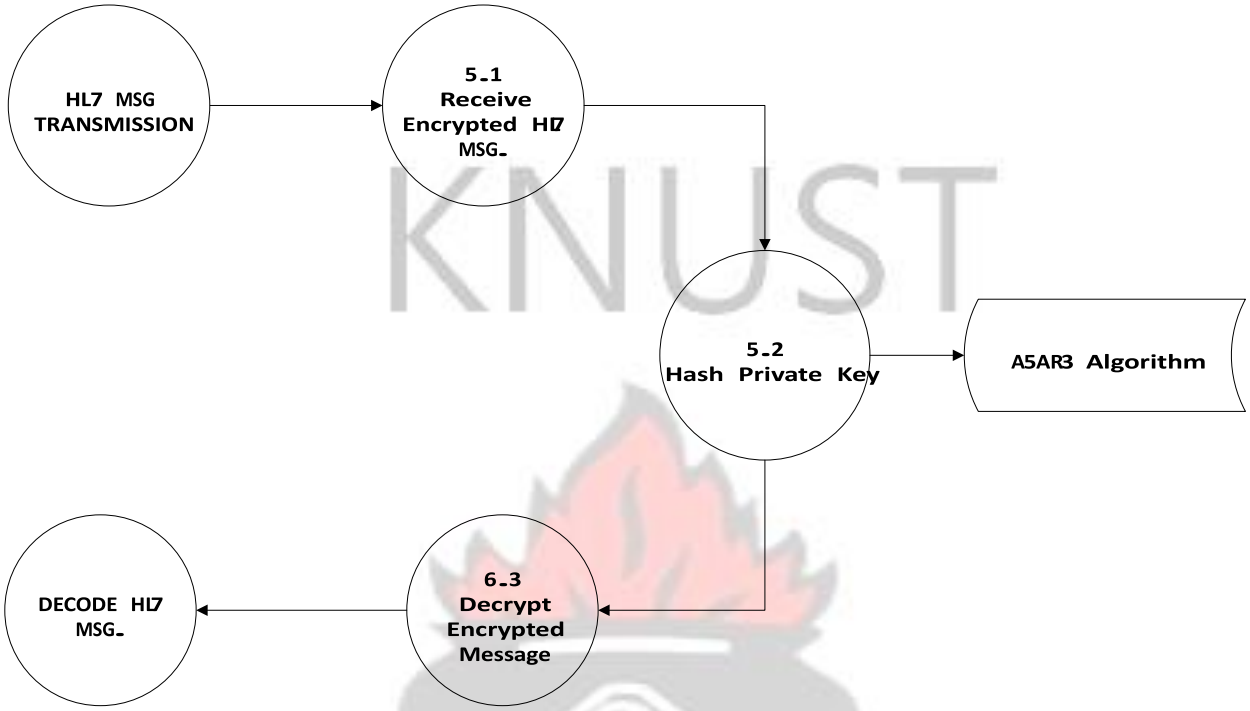


Fig 4-14: Decomposition of Process 2(HL7 Message Decryption)

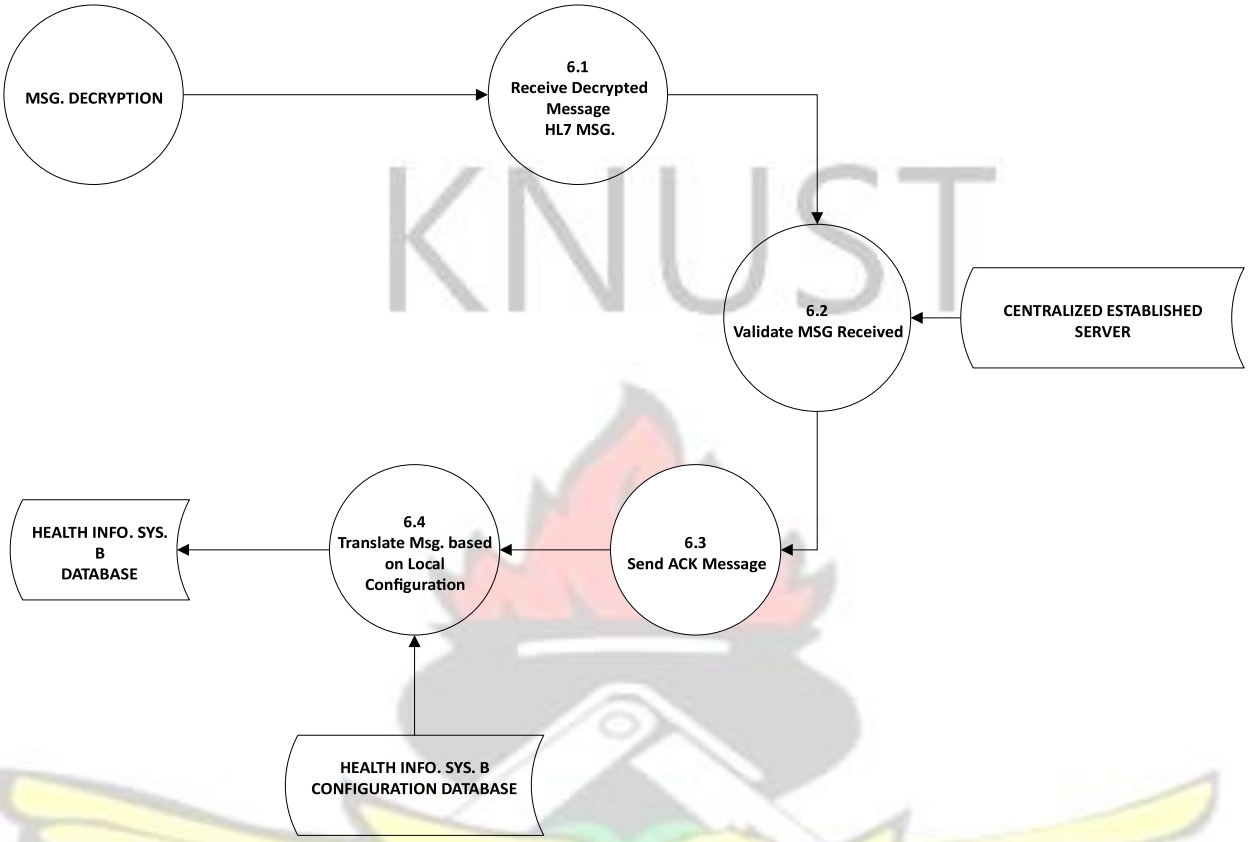


Fig 4-15: Decomposition of Process 2(HL7 Message Decoding)

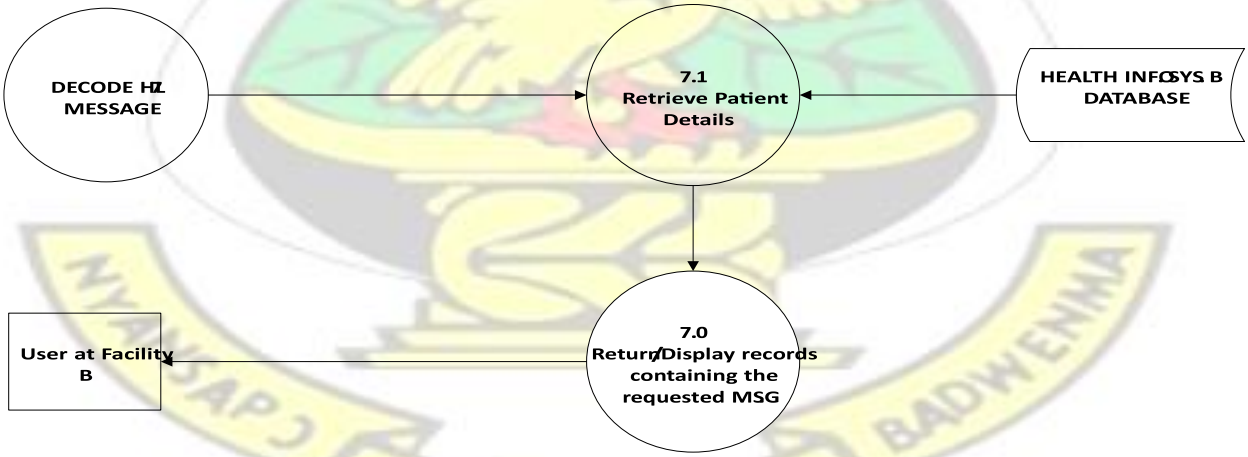


Fig 4-16: Decomposition of Process 2(HL7 Message Extraction) After the message has been decoded in process 6, user at facility B is then able to view or display the records by passing the necessary parameter at 7.0. At 7.1, the details are retrieved and displayed accordingly.

4.8 CHARTS

4.4.2 Input-Process-Output (IPO) Charts

IPO chart refers to a diagram that lists all related inputs, processing steps and desired outputs (Radatz, Geraci, Katki, & Lane, 1990). For the purpose of this study, the focus will be on developing IPO charts for seven main modules. These include:

- HL7 Mapping Configuration
- HL7 Message Encoding
- HL7 Message Validation
- HL7 Message Encryption
- HL7 Message Decryption
- HL7 Message Decoding
- User Management

IPO CHART

SYSTEM: HL7 System

PREPARED BY: Asare Michael Tetteh

MODULE: HL7 Mapping Configuration **DATE:**10/04/2016

CALLED OR INVOKED BY:	**CALLS OR INVOKES:** HL7 System Mapping Module
INPUTS: Data from Native Database Tables Data from HL7 Segments (HL7 Fields)	**OUTPUTS:** Mapped Configuration Database
PROCESS: Store data related to mapped data Update data related mapped data	
LOCAL DATA ELEMENTS	

Figure 4-17 IPO Chart for the HL7 Mapping Configuration module

IPO CHART

SYSTEM: HL7 System

PREPARED BY: Asare Michael Tetteh

MODULE: HL7 Message Encoding **DATE:10**/04/2016

CALLED OR INVOKED BY:	**CALLS OR INVOKES:** HL7 MAPPER Encoding Module
INPUTS: Data from Native Database Tables Data from Mapping Configuration Table	**OUTPUTS:** Updated target database
PROCESS: Format records from native database based on configuration details	
LOCAL DATA ELEMENTS	

Figure 4-18: IPO Chart for the HL7 message Encoding module

IPO CHART

SYSTEM: HL7 System

PREPARED BY: Asare Michael Tetteh

MODULE: HL7 Message Validation DATE:10/04/2016

CALLED OR INVOKED BY:	**CALLS OR INVOKES:** HL7 MAPPER Validation Module
INPUTS: HL7 Message	**OUTPUTS:** Validated HL7 Message

PROCESS:
Get message type
Compare message structure to in-built HL7 specifications Parse message to HL7 standard

LOCAL DATA ELEMENTS

Figure 4-19: IPO Chart for the HL7 message Validation module

IPO CHART

SYSTEM: HL7 System

PREPARED BY: Asare Michael Tetteh

MODULE: HL7 Message Encryption DATE:10/04/2016

CALLED OR INVOKED BY:	**CALLS OR INVOKES:** A5AR3 Encryption Algorithm Module
INPUTS: Hashed Private Key	**OUTPUTS:** Encrypted HL7 Message
PROCESS: Get Private Key Hashes Private Key Encrypt HL7 Message	
LOCAL DATA ELEMENTS	

Figure 4-20: IPO Chart for the HL7 Message Encryption Module

IPO CHART

SYSTEM: HL7 System

PREPARED BY: Asare Michael Tetteh

MODULE: HL7 Message Decryption DATE:10/04/2016

CALLED OR INVOKED BY:	**CALLS OR INVOKES:** A5AR3 Decryption Algorithm Module
INPUTS: Hashed Private Key	**OUTPUTS:** Decrypted HL7 Message
PROCESS: Get Private Key Hashes Private Key Decrypt HL7 Message	
LOCAL DATA ELEMENTS	

Figure 4-21: IPO Chart for the HL7 Message Decryption Module

IPO CHART

SYSTEM: HL7 System

PREPARED BY: Asare Michael Tetteh

MODULE: HL7 Message Decoding **DATE:10**/04/2016

CALLED OR INVOKED BY:	**CALLS OR INVOKES:** HL7 System Decoding Module
INPUTS: Data from Native Database Tables Data from Mapping Configuration Table	**OUTPUTS:** Updated target database
PROCESS: Format records from native database based on configuration details	
LOCAL DATA ELEMENTS	

Figure 4-22: IPO Chart for the HL7 Message Decoding Module

IPO CHART

SYSTEM: HL7 System

PREPARED BY: Asare Michael Tetteh

MODULE: User Management **DATE:**10/04/2016

CALLED OR INVOKED BY: User Management	**CALLS OR INVOKES:** Create User Modify User Delete User Create Profile Edit Profile Activate/Deactivate Users Lock/Unlock Users
INPUTS: User Information	**OUTPUTS:** Create User Account
PROCESS: The various user management actions are performed	
LOCAL DATA ELEMENTS	

Figure 4-23: IPO Chart for the HL7 Message User Management Module

4.9 Data Dictionary

4.4.3 Entity Relationship Modelling

Below is a list of database tables required to support the processes of the proposed system. For each table, a description is provided to aid in understanding the role each of them play.

ENTITY NAME	DESCRIPTION
Database Type	This table contains information about the various types of databases.
Database Details	This table saves information about the details of the databases used by the native information system.
Facility Profile	This table contains information about the facility.
Column Field Map	This table stores information about the various mapping configuration.
User Profile	This table saves information about the various user roles/profile.
Users	This table stores details of the users and their login details.

Table 4-1: List of database

4.4.4 Database Tables

In this section, for each of the tables enlisted above, the study expatiates to provide details of the various attributes of all fields.

Physical Name	Data Type	Req'd	PK	Notes
PKID	GUID	☑	☐	This is a unique field that identifies a user
UserID	CHAR(50)	☑	☑	This field stores the login name of a user
UserName	CHAR(120)	☑	☐	This field stores the full name of a user
ProfileID	CHAR(100)	☑	☐	This field determines the privileges of a user
Password	CHAR(128)	☐	☐	This field stores the stores the pasword of a user
Email	CHAR(50)	☐	☐	This field stores the email of a user
PasswordQuestion	CHAR(255)	☐	☐	This field stores the security quetion of a user
PasswordAnswer	CHAR(255)	☐	☐	This field stores the answer to the security quetion of a user
IsApproved	BOOL	☐	☐	This field stores the status of a user
Comment	CHAR(255)	☐	☐	This field stores the comments about a user
CreationDate	TIMESTAMP	☐	☐	This field stores the date a user was created
LastLoginDate	TIMESTAMP	☐	☐	This field stores the date of a user's last login
LastPasswordChangedDate	TIMESTAMP	☐	☐	This field stores date of the last time password was changed of a user
LastActivityDate	TIMESTAMP	☐	☐	This field stores the last activity date of a user
IsLockedOut	BOOL	☐	☐	This field determines whether a user is locked out of the system
LastLockedOutDate	TIMESTAMP	☐	☐	This field stores the last locked out date of a user
FailedPasswordAttemptCount	INTEGER	☐	☐	This field counts failed login attempts of a user
FailedPasswordAttemptWindowStart	TIMESTAMP	☐	☐	This field stores the date when failed attempt started of a user
FailedPasswordAnswerAttemptCount	INTEGER	☐	☐	This field counts failed attemptsl of a user
FailedPasswordAnswerAttemptWindowStart	TIMESTAMP	☐	☐	This field stores when a failed security answer was first provided
FaciilityID	CHAR(50)	☐	☐	This field stores user reference to a facility
		☐	☐	

Figure 4-24 Users table

	Physical Name	Data Type	Req'd	PK	Notes
▶	Profile	VARCHAR(100)	☑	☑	This field uniquely identifies a user profile
	Description	VARCHAR(150)	☐	☐	This field stores the name of the profile or role
			☐	☐	

Figure 4-25 User Profile Table

	Physical Name	Data Type	Req'd	PK	Notes
▶	FacilityID	VARCHAR(50)	☑	☑	This field stores data that uniquely identifies a Facility
	FacilityName	VARCHAR(50)	☑	☐	This field stores the name of the facility
	Logo	LONGVARBINARY	☑	☐	This field stores the logo of the facility
	Address	VARCHAR(50)	☑	☐	This field stores the address of the facility
	Email	VARCHAR(50)	☑	☐	This field stores the official email address of the facility
	Telephone	VARCHAR(50)	☐	☐	This field stores the official telephone number of the facility
	Location	VARCHAR(50)	☑	☐	This field stores the location of the facility
	ReceivingURL	VARCHAR(150)	☑	☐	This field stores the URL that serves as the receiving point of messages of the facility
	InformationSystem	VARCHAR(150)	☑	☐	This field stores the name of the Infomration System implemented by the facility
	DataSource	VARCHAR(150)	☑	☐	This field stores the connection string of the facility
			☐	☐	

Figure 4-26 Facility Profile Table

	Physical Name	Data Type	Req'd	PK	Notes
▶	DBID	VARCHAR(50)	☑	☑	This field uniquely identifies the details or attributes of the databse
	FacilityID	VARCHAR(50)	☑	☐	This field acts as a reference to the details sored for the facility (FK2)
	TypeID	VARCHAR(50)	☑	☐	This field acts as a reference to the details sored for the database type (FK1)
	Name	VARCHAR(50)	☑	☐	This field stores the name of the database
	Connstr	VARCHAR(250)	☑	☐	This fieldstores the connection string of the database
			☐	☐	

Figure 4-27 Database Details Table

	Physical Name	Data Type	Req'd	PK	Notes
▶	DBTypeID	VARCHAR(50)	☑	☑	This field stores data that uniquely identifies the databse type
	Type	VARCHAR(50)	☑	☐	This field stores the name or category of the database
			☐	☐	

Figure 4-28 Database Type Table

	Physical Name	Data Type	Req'd	PK	Notes
▶	MapID	VARCHAR(50)	☑	☑	This field uniquely identifies a Mapping Configuration
	FacilityID	VARCHAR(50)	☑	☐	This field acts as reference to the Facility Details(FK)
	DB_Name	VARCHAR(50)	☑	☐	This field stores the database name which contains the table and column to Map to
	DB_Column	VARCHAR(50)	☑	☐	This field stores the name of the column within the database table
	msg_Segment	VARCHAR(50)	☑	☐	This field stores the name of the HL7 Segment that contains the field to be mapped
	msg_Fields	VARCHAR(50)	☑	☐	This field stores the name of the HL7 field that is to be mapped
	DB_Table	VARCHAR(50)	☑	☐	This field stores the table name which contains the column to be Mapped to
	Repeats	BIT	☐	☐	This field stores the details that indicate whether the HL7 field repeats
	Mandatory	BIT	☐	☐	This field stores the details that indicate whether the HL7 field is mandatory
	SegmentIndex	INTEGER	☐	☐	This field stores the details that indicate the index of the HL7 field within the Segment
			☐	☐	

Figure 4-29 ColumnFieldMap Table

4.4.5 Database Schema

The proposed system is to be implemented on a relational database. The database schema below shows the various tables with their associated fields and data types, as well as the relationships between the tables enlisted in the previous sections.

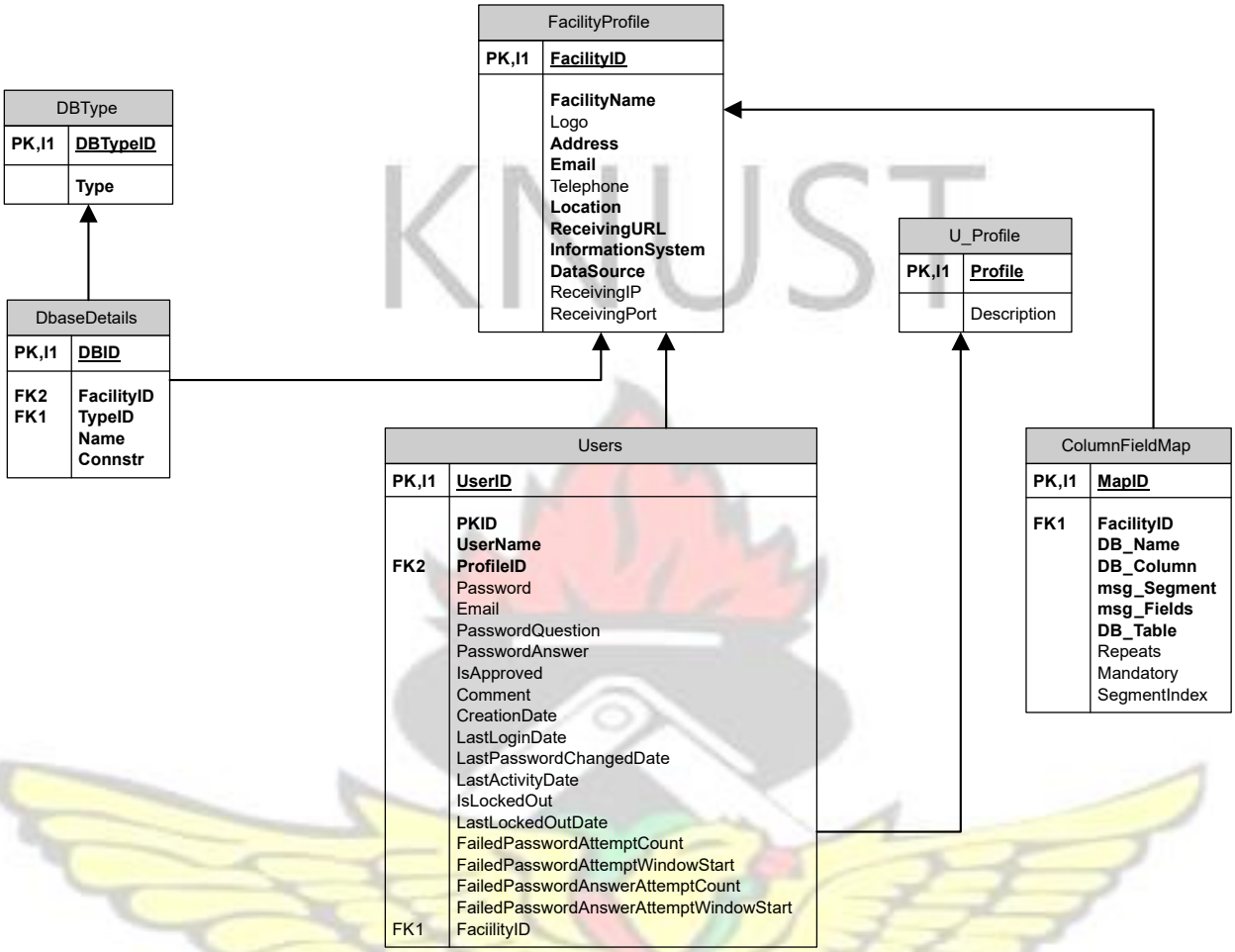


Figure 4-30 Database Schema

OBJECT MODELLING OF THE PROPOSED SYSTEM

Object modelling is a technique used for identifying objects within the systems environment and relationships between these objects. An object is something or is capable of being seen, or otherwise sensed and about which users store data and associate behaviours.

4.4.6 Sequence Diagram

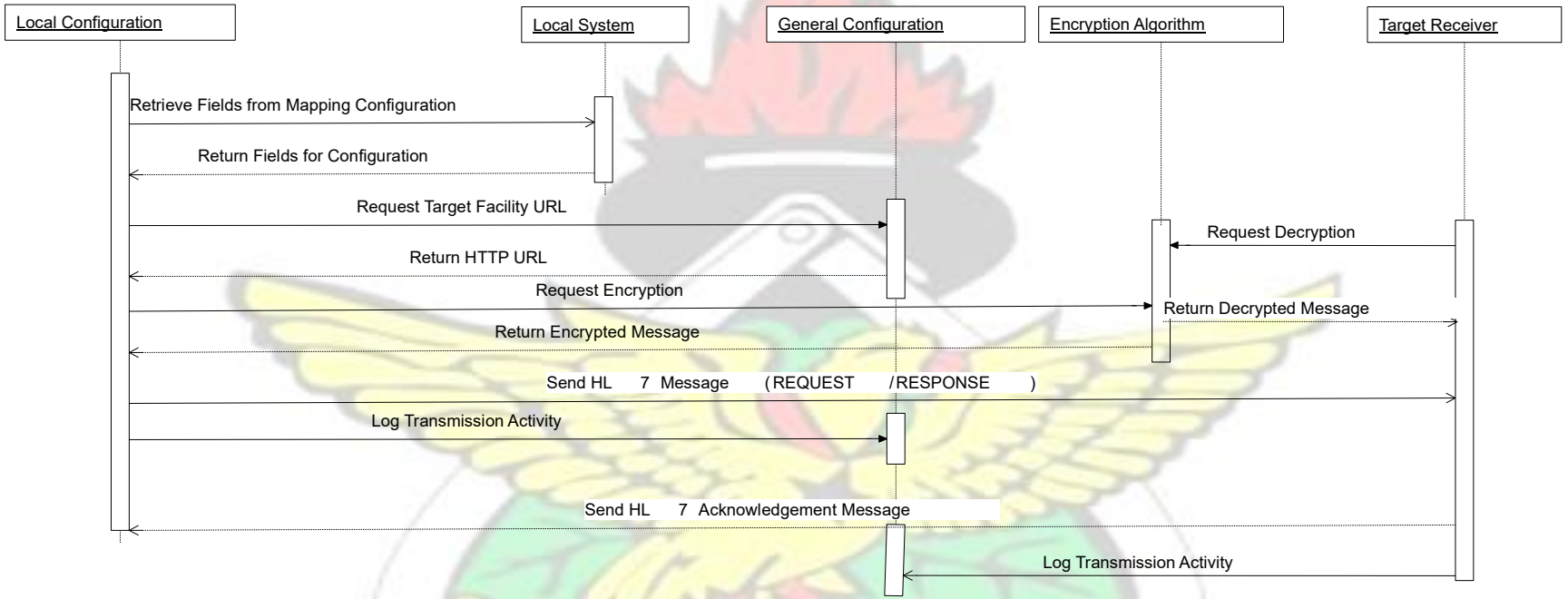


Figure 4-31 UML Sequence Diagram

4.4.7 Use Case Modelling

A Use Case represents a discrete unit of interaction between a user (human or machine) and the system. This interaction is a single unit of meaningful work, such as Create Account or View Account Details (Sparx, 2004).

Actors are human or machine entities that use or interact with the system to perform a piece of meaningful work that helps them to achieve a goal. The set of Use Cases an actor has access to define their overall role in the system and the scope of their action. (Sparx, 2004)

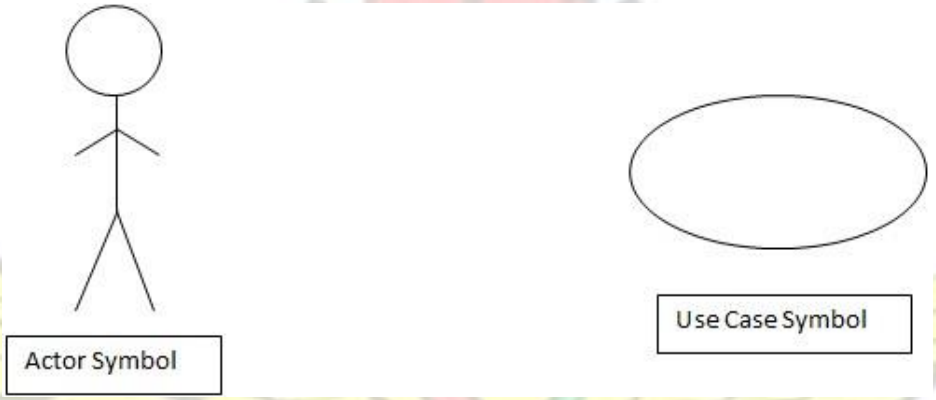


Figure 4-32 Use Case Diagram Symbols

4.4.8 Use Case Modelling of the Proposed System

System Users

- System Administrator

✓ Manages Facilities (creates new facility details, updates facilities)

✓ Maintains the system

✓ Configures the system for use

✓ Update HL7 specifications

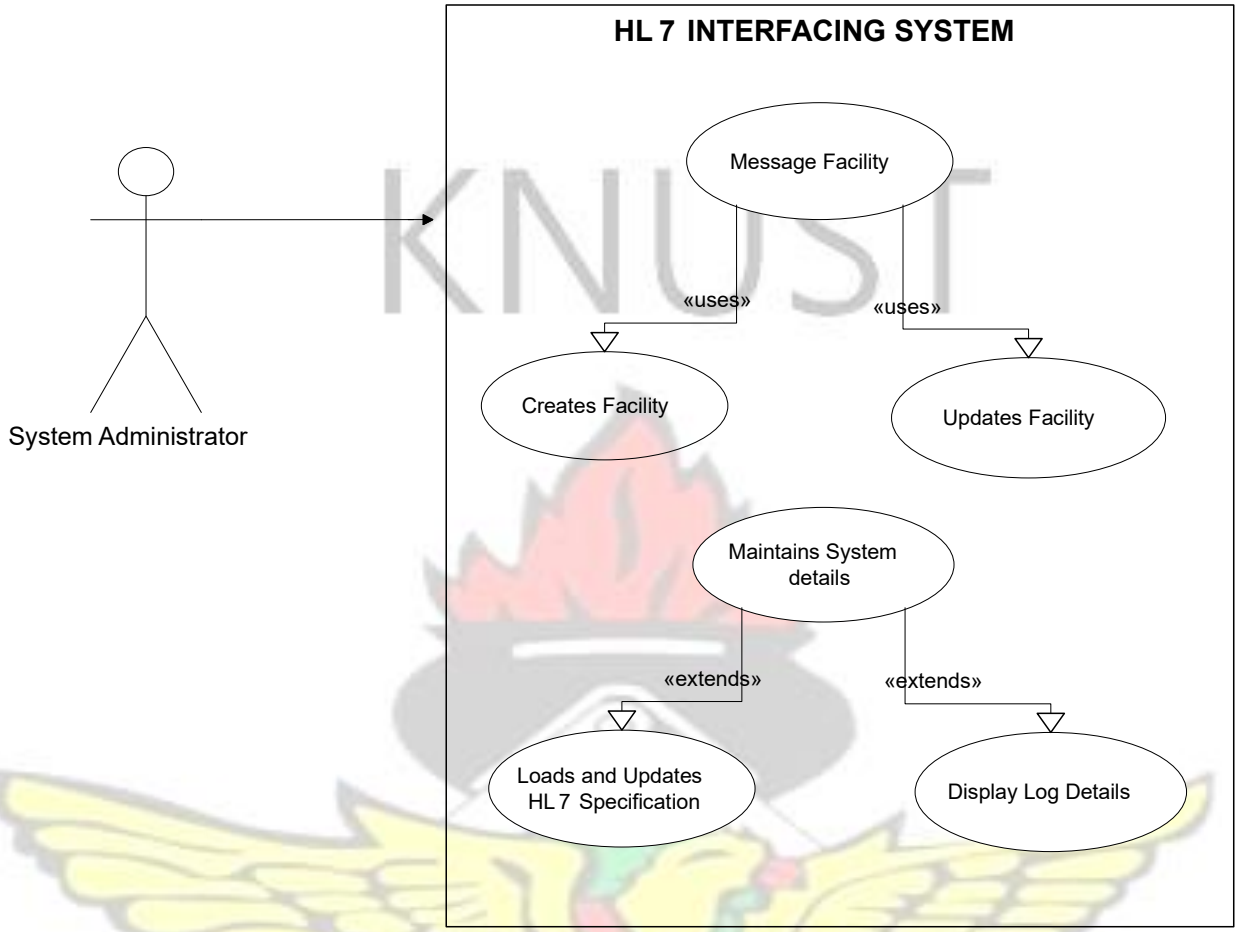


Figure 4-33 Use Case Diagram showing the system administrator and his functions

- Local Administrator

✓ Maps HL7 segment fields to local database columns/fields.

✓ Manages Users (creates new user account, updates user details)

✓ Forms the HL7 message by retrieving required fields from the local database.

✓ Sends the formed HL7 message.

✓ Receives HL7 message.

✓ Receives and Sends HL7 ACK message.

✓ Update records in the local database.

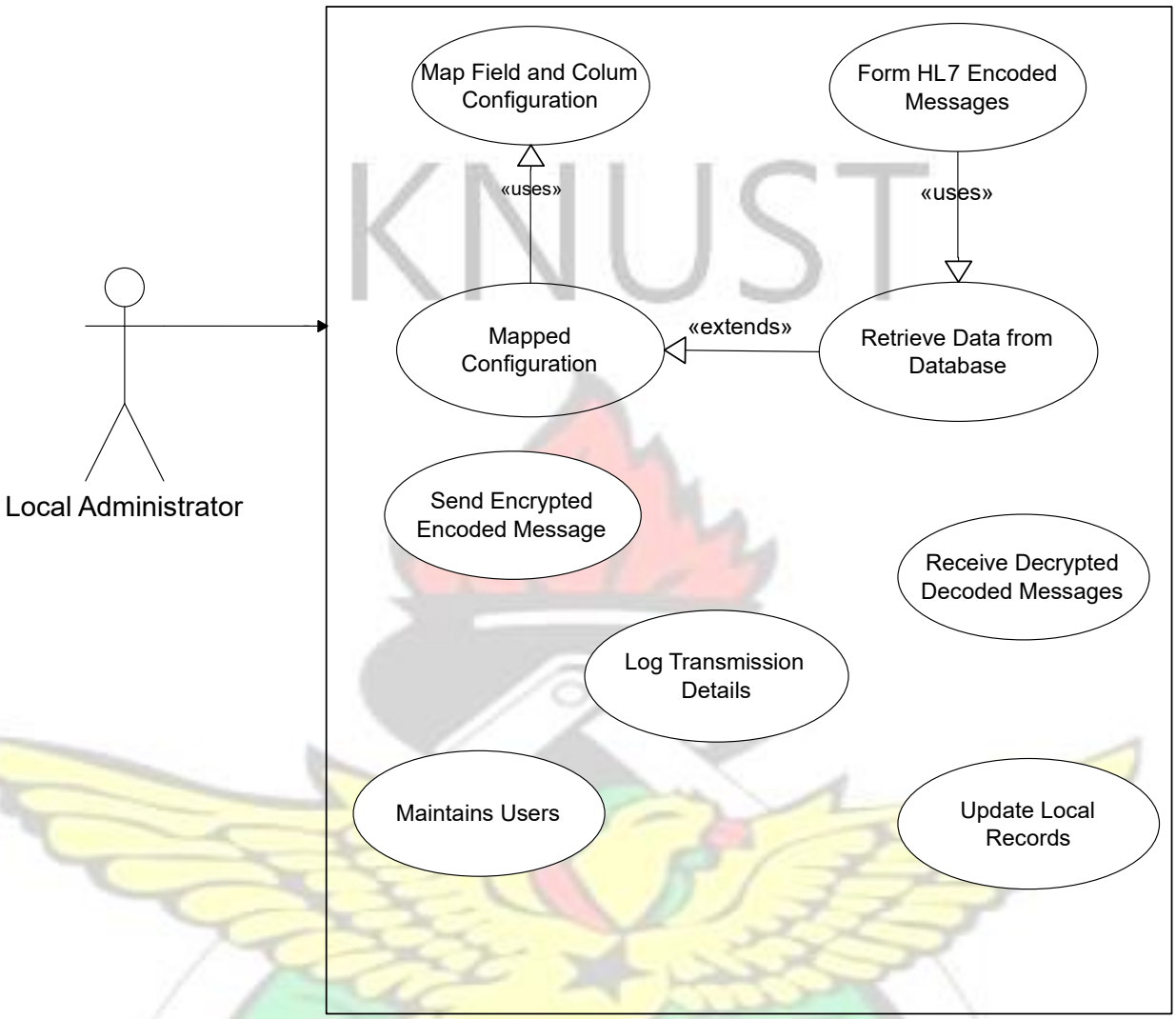


Figure 4-34 Use Case Diagram showing the user and his functions

- Physician

✓ Forms the HL7 message by retrieving required fields from the local database.

✓ Sends the formed HL7 message.

✓ Receives HL7 message.

✓ Receives and Sends HL7 ACK message.

- ✓ Update records in the local database.

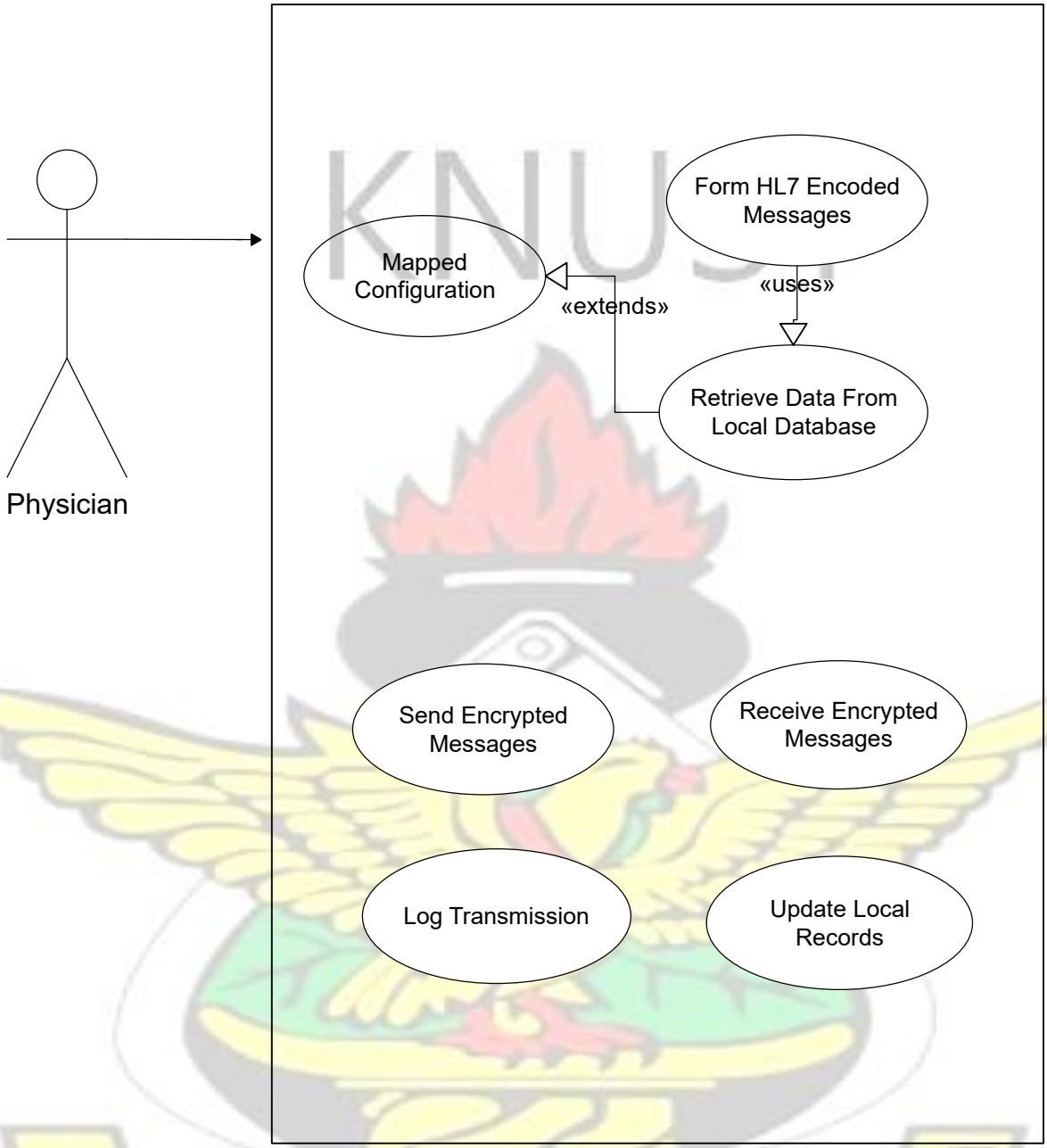


Figure 4-35 Use Case Diagram showing the Physician and his functions

4.10 SUMMARY

This chapter has looked at the outline of the system as well as the analysis of the system. This included the use of flow charts, data flow diagrams, context level diagrams and the decomposition of various processes.

The study evaluated the activities and identified desired objectives, and determined procedures for effectively attaining the objectives.

With the help of the context diagrams, the chapter defined boundaries between parts of the system and its environment and showed entities that interact with them.

The chapter basically broke down the system into various simpler parts for easy comprehension.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 DISCUSSION

The purpose of this study was to secure HL7 data transfer with an enhanced TDES encryption algorithm. It was evident there is an evolution of moving from pen and paper to Hospital Information Systems by Medical institutions. The need to secure medical data both on transit and at rest is paramount. The concentration had always been on securing data at rest; securing data on transit was an option, where organization opted for SSL/TLS to secure the channel of transmission. The study sought to make secure data on transit a permanent feature of the HL7 Standard.

5.1.1 Results

A typical HL7 encoded message is made up of the following : | used as field separator, ^ used as component separator, & used as subcomponent separator, ~ used as field repeat separator, and \ used as escape character.

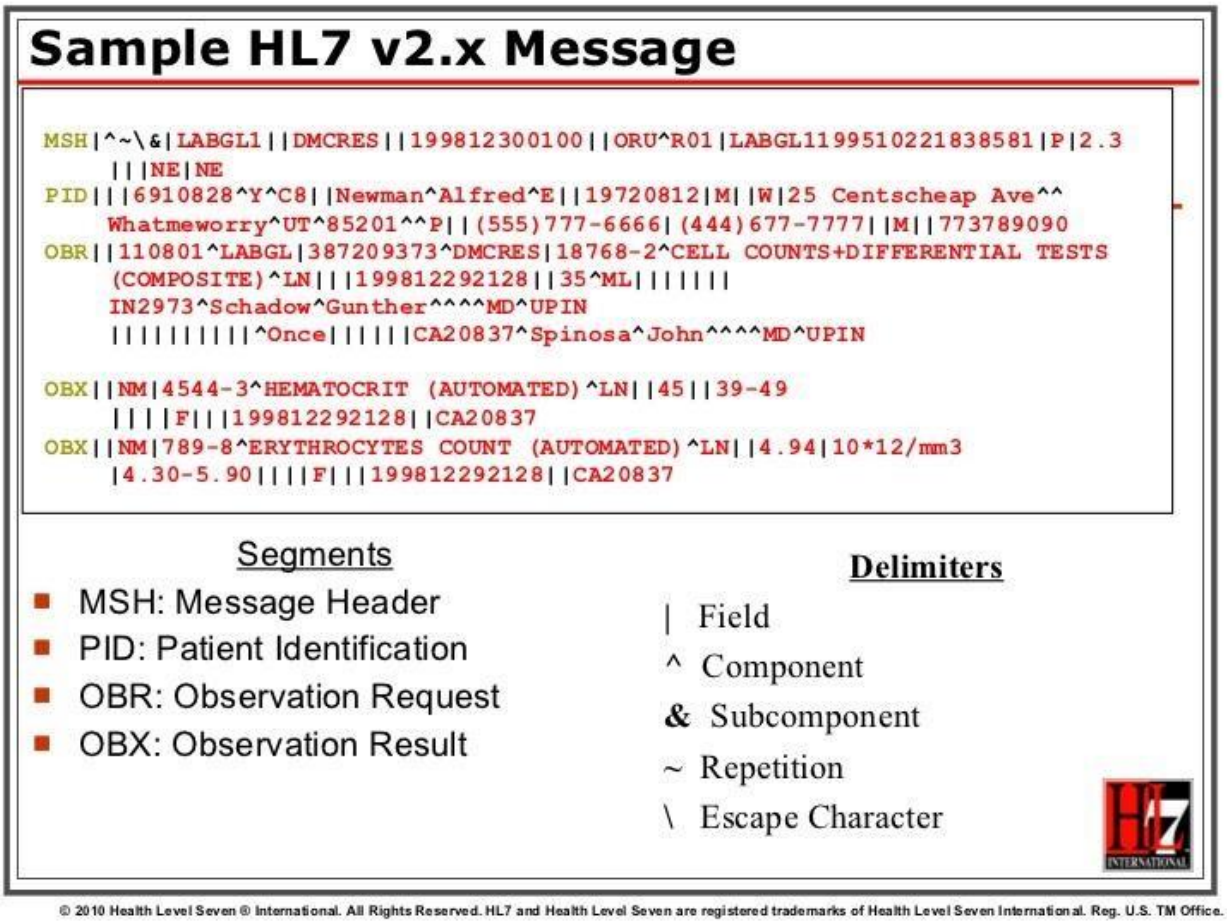


Figure 5-1 Sample HL7 Message, source: (Abdul-Malik, 2011)

```
MSH|^~\&|its|Sample Facility|RHMS|Ridge Hospital|20160427130543||ADT^A01|MSG0001|P|2.5|123
PID||PT/2014/0000001|PT/2014/0000001||Gyamfi^Owusu Ansah||19901111000|Male|||^^Airport
West||0243334456|||^Single|^Jewish
PV1||||||||||||||||||||||||||||||||||||||||||||||||201508170000
```

Figure 5-2: Patient's data encoded with HL7 messaging standard

The Figure 5-2 shows patient's data encoded with HL7 messaging standard. It is easy to make meaning out of the encoded message. When this kind of message is transmitted over a network, it can easily be intercepted and interpreted.

Figure 5-3: Encrypted Patient's data

Figure 5-3 shows the results of the encrypted patient's data. It is not possible to make meaning out of this cipher text. This will make the patient data secured whilst on transit. A facility can decide to use or not to use SSL/TLS since the data is already encrypted.

The solution proposed by this study makes security a default feature of the HL7 messaging standard.

5.2 CONCLUSION

The study employed the use of TDES Algorithm. The private key of TDES Algorithm is crucial for encrypting or decrypting a message, hence the need to protect the key.

The Algorithm was enhanced by first hashing the private key with MD5CryptoServiceProvider

(Hence A5AR3MY). The hashed private key cannot be reverse engineered thereby protecting the private key. It is after the hashing of the private key, that it will be used to encrypt the HL7 message.

The decryption process is similar to the encryption process. During the decryption, the private key will have to be hashed before it can be used to decrypted the encrypted HL7 message.

5.3 RECOMMENDATION

HL7 is gradually gaining grounds in medical institutions. The focus is always on data at rest; medical facilities concentrate on securing data at rest, whilst securing data on transit is an option. Securing data on transit should be a default feature of the HL7.

The study recommends the implementation of A5AR3MY Algorithm with the HL7, which will encrypt the encoded HL7 message before transmission, then decrypt the encrypted HL7 message when it gets to its destination. This will ensure security of data on transit. Medical facilities will not have to worry about employing SSL/TLS. This is because intercepted message will not make meaning to an attacker, thereby protecting patient confidentiality.

REFERENCES

[1] Abdul-Malik, S. (2011, January). *HL7*. Retrieved May 5, 2016, from Slideshare: http://www.slideshare.net/AShakir/hl7-v2-messaging-conformance-jan-2011

[2] Anderson, R. (2006). Under threat: patient confidentiality and NHS computing . *6* (4).

[3] Author, G. (2011, November 2). *5 Consequences of an Information Security Breach*. Retrieved March 20, 2016, from BestTechie: https://www.besttechie.com/5-consequences-informationsecurity-breach/

[4] Beal, V. (2001, April 5). *encryption*. Retrieved March 20, 2016, from Webopedia: http://www.webopedia.com/TERM/E/encryption.html

[5] Behrens, M. (2014, November 20). *Understanding the 3 Main Types of Encryption*. Retrieved March 20, 2016, from Atomic Object: https://spin.atomicobject.com/2014/11/20/encryptionsymmetric-asymmetric-hashing/

[6] Blog, T. (2015, July). *The Pros and Cons of Using a Virtual Private Network*. Retrieved March 23, 2016, from Thrivenetworks: http://www.thrivenetworks.com/blog/2011/07/28/the-pros-andcons-of-using-a-virtual-private-network/

[7] Bord, J. D. (2013). *Confidentiality.* Retrieved April 11, 2016, from washington.edu: https://depts.washington.edu/bioethx/topics/confiden.html

[8] Bray, T. J. (2011, January 7). *Encyclopedia of Information Assurance.* Retrieved March 20, 2016,

from tandfonline: http://www.tandfonline.com/doi/abs/10.1081/E-EIA-120046566#.Vu683uKLTbg

[9] Burkett, J. S. (2012). Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA. *21* (1).

[10]Care, S. B. (2013, July). *Overview of Healthcare Interoperability Standards.* Retrieved March 21, 2016, from https://www.hiqa.ie/system/files/Healthcare-Interoperability-Standards.pdf

[11]Chao, H., Twu, S., & Hsu, C. (2005). A patient-identity security mechanism for electronic medical records during transit and at rest. *PubMed* , 1-4,13.

[12]Chapple, M. (2010, April). *Data encryption methods: Securing emerging endpoints.* Retrieved March 21, 2016, from Techtarget: http://searchsecurity.techtarget.com/tip/Data-encryptionmethods-Securing-emerging-endpoints

[13]Cod, C. (2013). *Confidentiality, Patient/Physician.* Retrieved April 11, 2016, from Aafp: http://www.aafp.org/about/policies/all/patient-confidentiality.html

[14]Com, S. (2015, October 26). *What is SSL*. Retrieved March 23, 2016, from SSL: http://info.ssl.com/article.aspx?id=10241

[15]Conn, J. (2015, August 26). *Healthcare Information Technology.* Retrieved August 27, 2015, from Modern Healthcare: http://www.modernhealthcare.com/article/20150826/NEWS/150829921/80-of-health-itleaders-say-their-systems-have-been-compromised

[16]Damoah, D., Debrah, K., Nelson, M., Takyi, A., Ansong, E., Goga, et al. (2014). A framework for adapting health-level7 techniques in Ghanaian institutions.

[17]Dömstedt, B., & Jansson, J. (2001). *The Theory of Dynamic Encryption,a New Approach to Cryptography.* Retrieved March 21, 2016, from Protego: http://www.protego.se/pdf/dyn_enc1.pdf

[18]Gilbert, B. (2015). *What Is A VPN*. Retrieved March 23, 2016, from What is my IP: https://www.whatismyip.com/what-is-a-vpn/

[19]Grabbe, O. (2011). The DES Algorithm Illustrated. *Laissez Faire City Times* , 3-5.

[20]Hamdan, O., Alanazi, B., B, Z., A, Z. A., Hamid, A., Hamid, A., et al. (2010). New Comparative Study Between DES, 3DES and AES. *JOURNAL OF COMPUTING* .

[21]Hayaati, N., & Mohd, A. (2012). *E-LEARNING STAKEHOLDERS INFORMATION SECURITY VULNERABILTY MODEL.* Retrieved March 20, 2016, from cranfield: https://dspace.lib.cranfield.ac.uk/bitstream/1826/7387/1/Najwa_Hayaati_Mohd_Alwi_Thesis_2012.pdf

[22]HL7. (2007, August). *Encryption*. Retrieved March 23, 2016, from HL7: http://wiki.hl7.org/index.php?title=Implementation_FAQ:Encryption_and_Security

[23]HL7. (2011, February). *HL7 International*. Retrieved March 15, 2016, from HL7: https://www.hl7.org/documentcenter/public_temp_026EC67C-1C23-BA17-0C29030975C47A9B/calendarofevents/himss/2011/HL7%20Organizational%20Backgrounder%20and%20Standards%20Descriptions.pdf

[24]HL7, A. (2010, June 17). *About HL7.* Retrieved March 21, 2016, from HL7: http://www.hl7.org/about/index.cfm?ref=common

[25]Hong, K.-S. (2003). An integrated system theory of information security management. *7* (1).

[26]Howe, J. (2011, Arpril 14). *Resources*. Retrieved August 27, 2015, from Private Wifi: http://blog.privatewifi.com/a-hacker%E2%80%99s-toolkit/

[27]Jung, B., Han, I., & Lee, S. (2001). Security Threats to Internet: A Korean. *38*.

[28]Kim, E. B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. *22* (4).

[29]Kioskea. (2014, June). *Data Transmission.* Retrieved March 18, 2016, from CCM: http://ccm.net/contents/701-data-transmission-transmission-modes

[30]Konstantinos Koumaditis, M. T. (2013). SOA implementation critical success factors in healthcare. *Emerald Insight , 26* (4), 343-349.

[31]Konstantinos, K., Marinos, T., Paulo, R., & Da, C. (2013). SOA implementation critical success factors in healthcare. *Emerald Insight , 26* (4), 343-349.

[32]Li, D. C. (2015). Online Security Performances and InformationSecurity Disclosures. *55* (2).

[33]Magaqa, V. L. (2012, October 3). *researchspace*. Retrieved March 15, 2016, from researchspace: http://researchspace.ukzn.ac.za/xmlui/bitstream/handle/10413/10383/Magaqa_Vuminkosi_Lionel_Longsdale_2010.pdf?sequence=1

[34]Mahan, R., Burnette, J., Fluckiger, J., Goranson, C., Clements, S., Kirkham, H., et al. (2011, September). *Secure Data Transfer Guidance forIndustrial Control and SCADA Systems.* Retrieved Marh 18, 2016, from PNNL: http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

[35]Manes, C. (2014, December 19). *Security 101: at rest or in transit – protecting data with encryption.* Retrieved April 11, 2016, from gfi.com: http://www.gfi.com/blog/protecting-datawith-encryption/

[36]Marinič, M. (2015, May 20). The Importance of Health Records. *Scientific Research Publishing* , p. 617.

[37]Microsoft. (2015). *HL7 Message Structure*. Retrieved August 28, 2015, from Microsoft: https://msdn.microsoft.com/en-us/library/ee409289.aspx

[38]Morad, B., Craig, K., Amir, A. R., & Ali, E. (2011). Modeling healthcare processes as service orchestrations and choreographies. *Emerald Insight , 17* (4), 568-593.

[39]Mweebo, K. (2014). Security of electronic health records in a resource limited setting: The case of smart-care electronic health record in Zambia. *AUSTRALIAN EHEALTH INFORMATICS AND SECURITY CONFERENCE* (pp. 35-38). Joondalup: Australian eHealth Informatics and Security Conference.

[40]Mweebo, K. (2014). Security of electronic health records in a resource limited setting: The case of smart-care electronic health record in Zambia. *AUSTRALIAN EHEALTH INFORMATICS AND SECURITY CONFERENCE* (pp. 35-38). Joondalup: Australian eHealth Informatics and Security Conference.

[41]Mweebo, Keith. (2014). Security of electronic health records in a resource limited setting: The case of smart-care electronic health record in Zambi. Australian eHealth Informatics and Security.

[42]Orion, H. (2013, March 24). *HL7 Interface Engine*. Retrieved March 15, 2016, from HL7.com: http://www.hl7.com/interface-engine.html

[43]Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A design Science Research

Methodology for Information Systems Research. *Management Information Systems , 24*, 45-78.

[44]Peterson, A. (2015, March 20). *The Switch*. Retrieved August 27, 2015, from The Washintion Post: https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-theyear-of-the-health-care-hack-and-its-only-going-to-get-worse/

[45]Petri, P. (2006). A DESIGN THEORY FOR INFORMATION SECURITY AWARENESS.

[46]Press, A. (2015, August 3). *Healthcare Information Technology* . Retrieved August 27, 2015, from Modern Healthcare: http://www.modernhealthcare.com/article/20150803/NEWS/308029998/indiana-medicalsoftware-company-hack-affected-3-9m-people

[47]Radatz, J., Geraci, A., Katki, F., & Lane, J. (1990). *IEEE Standard Glossary of Software Engineering.* New York: The Institute of Electrical and Electronics Enginnering.

[48]Reina, V. (2014, March 25). *THE IMPORTANCE OF MEDICAL RECORDS: A CRITICAL PROFESSIONAL RESPONSIBILITY.* Retrieved March 21, 2016, from Gapmedics: http://www.gapmedics.com/blog/2014/03/25/the-importance-of-medical-records-a-criticalprofessional-responsibility/

[49]Ronan, F., James, C., & Manfred, H. (2011). Collaborative development of trusted mashups. *Emirald Insights , 7* (3), 264-284.

[50]Rouse, M. (2014, November). *Encryption.* Retrieved March 21, 2016, from Techtarget: http://searchsecurity.techtarget.com/definition/encryption

[51]Rouse, M. (2005, September). *Hashing*. Retrieved April 09, 2016, from Techtarget: http://searchsqlserver.techtarget.com/definition/hashing

[52]Rouse, M. (2007). *Pivate Key*. Retrieved April 09, 2016, from Techtarget.com: http://searchsecurity.techtarget.com/definition/private-key

[53]Shackleford, D. (2014, May). *Regulations and Standards:Where Encryption Applies.* Retrieved April 11, 2016, from sophos: https://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/PublicSectorBenelux/sophos-encryptionregulations-standards-wpna.pdf?la=en

[54]Shephard, D. (2015, March 16). *84 Fascinating & Scary IT Security Statistics*. Retrieved April 21, 2016, from NetIQ Communities: https://www.netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/

[55]Sookasa, R. (2015, April 11). *Resources*. Retrieved March 23, 2016, from Sookasa: https://www.sookasa.com/resources/HIPAA-encryption/

[56]Sparx, S. (2004). *The Use Case Model.* Retrieved 04 28, 2011, from Sparx Systems: http://www.sparxsystems.com.au/resources/tutorial/use_case_model.html

[57]Staggers, N., Weir, C., & Phansalkar, S. (2008). *NCBI*. Retrieved March 15, 2016, from NCBI: http://www.ncbi.nlm.nih.gov/books/NBK2644/#_ch47_rl1_

[58]Stallings, W. (2011). *NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS FOURTH EDITION.* Retrieved April 11, 2016, from Prentice Hall: http://sbmu.ac.ir/uploads/3._Networksecurity-essentials-4th-edition-william-stallings.pdf

[59]techopedia. (2013, April 2). *Data Transfer*. Retrieved March 16, 2016, from techopedia: https://www.techopedia.com/definition/18715/data-transfer

[60]Techopedia, T. (2012, Januar 13). *Triple DES*. Retrieved April 09, 2016, from techopedia: https://www.techopedia.com/definition/4144/triple-des

[61]Thakur, D. (2013, June 22). *Data Transmission*. Retrieved March 18, 2016, from Computer Notes: http://ecomputernotes.com/computernetworkingnotes/communication-networks/datatransmission

[62]Themistocleous, K. K. (2015). Organizational structures during SOA implementation: the case of a Greek healthcare organization. *Emerald Insight , 9* (3), 263-285.

[63]Townsend, P. (2013, April 2). *townsend security*. Retrieved March 20, 2016, from townsend security: http://info.townsendsecurity.com/why-unprotected-data-business-problem-video

[64]Tutorialspoint. (2015, July 28). *Triple DES*. Retrieved April 17, 2016, from tutorialspoint: http://www.tutorialspoint.com/cryptography/triple_des.htm

[65]Vithiatharan, R. N. (2014). The potentials and challenges of big data in public health. Australian eHealth Informatics and Security.

[66]Weerasinghe, D., Rajarajan, M., Elmufti, K., & Rakocevic, V. (2008). Patient privacy protection using anonymous access control techniques. *PubMed* , 235-240.

[67]Weiss, K. P. (1993). Data Integrity and Security: Who's in Charge Here Anyway? *1* (4).

[68]Wiegers, K. (2014, February 26). *Requirements Best Practices*. Retrieved April 11, 2016, from Jamasoftware: http://www.jamasoftware.com/blog/defining-project-scope-context-use-casediagrams/

[69]Wieringa, R. (2013, August 4). *ntroduction to design science*. Retrieved April 11, 2016, from refsq.org: https://refsq.org/wp-content/uploads/2013/05/Wieringa-2013-REFSQ-DS-Introduction-to-design-science-methodology-slides.pdf

[70] Zero, D. B. (2011, January 18). *HL7 and security*. Retrieved March 16, 2016, from dib0: http://www.dib0.nl/code/256-hl7-and-security

APPENDICES

Appendix I

HL7 Message Structure

Trigger event	Abstract message
ADT^A04^ADT_A01	Admissions, Discharge, and Transfer
MSH	Message Header
EVN	Event Type
PID	Patient Identification
[PD1]	Additional Demographics
[{ ROL }]	Role
[{ NK1 }]	Next of Kin / Associated Parties
PV1	Patient Visit
[PV2]	Patient Visit - Additional Information
[{ ROL }]	Role
[{ DB1 }]	Disability Information
[{ OBX }]	Observation/Result
[{ AL1 }]	Allergy Information
[{ DG1 }]	Diagnosis Information
[DRG]	Diagnosis Related Group
[{	
PR1	Procedures

[{ ROL }]	Role
}]	
[{ GT1 }]	Guarantor
[{	
IN1	Insurance
[IN2]	Insurance Additional Information
[{ IN3 }]	Insurance Additional Information - Cert.
[{ ROL }]	Role
}]	
[ACC]	Accident Information
[UB1]	Universal Bill Information
[UB2]	Universal Bill 92 Information
[PDA]	Patient Death and Autopsy

Appendix II

Code for User Authentication

```
protected void btnAuth_Click(object sender, EventArgs e)
{
    string userid = txtuser.Text;

    if (userid == "")
        userid = "";
    else
        Session["username"] = userid;

    iSchoolUsers ob = new iSchoolUsers();

    string profile = "";
    if (userid == "Dangbanduri")
    {
        profile = "Administrator";
    }
    else { profile = ob.GetProfile(userid); }

    if (profile == "None")
    {
        lblMess.Visible = true;
        lblMess.Text = "User ID Does Not Exist";
    }
    else
    {
        Response.Redirect("~/UserLog/UserLogin.aspx");
    }
}
```

Appendix III

User Validation

```
protected void Page_Load(object sender, EventArgs e)
{
    if (!this.Page.IsPostBack)
    {
        string str2;
        string str = "";
        str = (string)this.Session["username"];
        if (((str2 = str) == null) || (str2 == ""))
        {
            base.Response.Redirect("~/Default.aspx");
        }
        else
        {
            TextBox box = (TextBox)this.iSchoolLogin.FindControl("UserName");
            TextBox box2 = (TextBox)this.iSchoolLogin.FindControl("Password");
            box.Text = str;
            box.Enabled = false;
            box2.Focus();
        }
    }
}

protected void LoginButton_Click(object sender, EventArgs e)
{
    string user = iSchoolLogin.UserName;
    string pass = iSchoolLogin.Password;
    TextBox txtUser = (TextBox)iSchoolLogin.FindControl("UserName");
    iSchoolUsers ob = new iSchoolUsers();

   if (!ob.ValidateUser(user, pass))
    {
        iSchoolLogin.FailureText = "Login Attempt not Successful, Please try again";
    }
    else
    {
       //take user to portal
    }
}
```

Appendix IV

Code to generate message

```
private void genmsg(string patientid,string visitid,string msg,string facility)
{
    try
    {
        Session["tmpfacility"] = facility;
        Session["tempgenmsg"] = obj.ADT_A01SegmentList("PatientID", patientid, visitid, facility);
        Response.Redirect("SendMsg.aspx");
    }catch(Exception)
    {
    //Dispaly Exception
    }
}
```

Appendix V

Code for Encrypting HL7 Message

```
public static string Encrypt(string toEncrypt)
{
    byte[] keyArray; //initialise array
    byte[] toEncryptArray = UTF8Encoding.UTF8.GetBytes(toEncrypt);//convert from byte


    if (_useHashing) //check fi the results has been hashed
    {
        MD5CryptoServiceProvider hashmd5 = new MD5CryptoServiceProvider();// if using hashing convert
        keyArray = hashmd5.ComputeHash(UTF8Encoding.UTF8.GetBytes(_salt));
        hashmd5.Clear();
    }
    else
    {
        keyArray = UTF8Encoding.UTF8.GetBytes(_salt);//else use byte
    }

    using (TripleDESCryptoServiceProvider tdes = new TripleDESCryptoServiceProvider())//
    {
        tdes.Key = keyArray;
        tdes.Mode = CipherMode.ECB;
        tdes.Padding = PaddingMode.PKCS7;

        ICryptoTransform cTransform = tdes.CreateEncryptor();
        byte[] resultArray = cTransform.TransformFinalBlock(toEncryptArray, 0, toEncryptArray.Length);//encryption
        tdes.Clear();

        return Convert.ToBase64String(resultArray, 0, resultArray.Length);//convert to 64bit again
    }

}
```

Appendix VI

Code for Decrypting HL7 Message

```
public static string Decrypt(string cipherString)
{
    byte[] keyArray;
    byte[] toEncryptArray = Convert.FromBase64String(cipherString);//Convert from base64


    if (_useHashing)//check wherther you hashed
    {
        MD5CryptoServiceProvider hashmd5 = new MD5CryptoServiceProvider();
        keyArray = hashmd5.ComputeHash(UTF8Encoding.UTF8.GetBytes(_salt));
        hashmd5.Clear();
    }
    else
    {
        keyArray = UTF8Encoding.UTF8.GetBytes(_salt);
    }

    using (TripleDESCryptoServiceProvider tdes = new TripleDESCryptoServiceProvider())
    {
        tdes.Key = keyArray;
        tdes.Mode = CipherMode.ECB;
        tdes.Padding = PaddingMode.PKCS7;

        ICryptoTransform cTransform = tdes.CreateDecryptor();
        byte[] resultArray = cTransform.TransformFinalBlock(toEncryptArray, 0, toEncryptArray.Length);

        tdes.Clear();
        return UTF8Encoding.UTF8.GetString(resultArray);//get plain string
    }
}
```

Appendix VII

Generated HL7 Message

Appendix

Generated Message

```
MSH|^~\&|its|Sample Facility|RHMS|Ridge Hospital|20160422114419||ADT^A01|MSG0001|P|2.5|123
PID||PT/2014/0000001|PT/2014/0000001||Gyamfi^Owusu Ansah||199011110000|Male|||^^Airport
West||0243334456|||^Single|^Jewish
PV1||||||||||||||||||||||||||||||||||||||||||||||||201508170000
```

VIII

Encrypted HL7 Message

Message Status

```
z+rO8mWp4b1SDh4JnKhTb+3FhRDtpr6/qVDdJ+bVnzYVBITY8UVW3F4Dn5RzO5xscOiU7etG4YrmQHOyNxW9y9MyA8GG4I
LXm603rE7g/LcvDQ4Bwl3bsf4sm9ITP9xjyI938c6YbKNOJTI6zBOmz8iPd/HOmGyjTiUyOswTps8vamFvOHvTzQp1sP96NbG8
bwhMBBye2p4XSci4eXpqsxIZA07hg+omxF2cUjyOv0eE+rBTB1dN5/jkUt7DSgk7IkK9x/H+zBal9HdMlc2V75O5oL/bQEsztq2Q0
xpbMH1mF7tyqPOt52YXu3Ko863nZhe7cqjzredmF7tyqPOt5+uDiv7N1hZ8m/cuO4UsRtbVMhh59NUuZ08MTW+wkEw4TUAM
TrvSTUm+opY1g7jycfznhG6VEiDI+HSrmkoMIA7h2QAp4MrQfVHXGV3J5coC6bHzy7ergHuvZgmFmKDjP5rIcJBBEmOeyCAH
dZI5UImC5ghIvdMjhX1CwAlwwWORLAuAA5zDcg9ST179bUt1CCwLgAOcw3IPeAWmPlJ0M7UyZsRAPIzZNwmIhnwPc4QrD4
yOvI8DLEtFJHqQOxRNyLYwTpqHDr4WByedTDKb2tyvmzE2BXkchfPfwvdlx9j2j9+NtYlHSFjj/Gj2i8I6mXmnP+UD0J+vZhe7cqjzr
edmF7tyqPOt52YXu3Ko863nZhe7cqjzredmF7tyqPOt53+JAfBdqyIjiPFjLn+TNP6cRBq5jPycyrf1qKmE11r+5fbti/w0YqdpRDXOz
ETy5N5beaNXdMGJcOiU7etG4YqEEXYYILwE06OJExpaMf7WyCAHdZI5UImC5ghIvdMjhQ9Dd5qlgmXp2qq7dsSii8wvfKoUDa
Ni6g==
```

Send

Appendix IX

Decrypted HL7 Message

Appendix