**Implementing Cloud Securities on Mobile Blood Bank**

**For Kenya National Blood Transfusion Service**

**By**

**Kenneth Kodo**

**SCT221-6813/2015**

**A project proposal submitted to the department of Information Technology, in the School of Computing and Information Technology in partial fulfillment of the requirements for the Award of Degree in Information Technology**

**Jomo Kenyatta University of Agriculture and Technology**

**January, 2019**

# DECLARATION

Declaration by student

I hereby declare that this research proposal is my original work and has not been presented in any other university or institution for consideration of any certification

Sign…………………………………………. date ………………………………

Kenneth Kodo

Declaration by supervisor

This project has been submitted for examination with my approval as university supervisor

Sign……………………………… Date…………………………………

Mrs. Nancy Macharia

# Acknowledgement

Success and good outcome of this project requires a lot of guidance and assistance from many people and I have been highly privileged to have got all this with me. Furthermore, all that I’ve been able to put together is only due to wonderful supervision and assistance and I would not at any time forget to thank them.

Firstly, I would like to thank almighty father for his grace, favor and guidance for having me come this far. Am also grateful to the entire JKUAT and IT department for having natured me from an IT novice to now an IT professional

I respect and thank my parents and for believing in me and giving me all the support I needed to spearhead my project and for giving me mental, spiritual and financial support as walked through my career path, I surely can’t thank you enough. I owe my deep gratitude to my friends for being there always and having each other’s back all through this entire journey of degree.

# Abstract

This projects main goal is to help save life and link blood donors to blood procurers online. Furthermore, this project is also designed to handle blood transactions of the blood bank. It also helps to register the details of the donors, and store them in a centralized database to ease the process of blood searching in case of emergency.

This software application is well designed in a manner that it can suit all the blood store requirements, registered users are able to update their details such as name, personal information medical information along with their blood groups. New users can also register and view donors and search for donors using donor number, name, location and blood groups respectively. However new users can also register as potential donors provided they fill all the required details

This proposed project is the perfect solution the problems such as time, manual process of blood searching, mobilizing donors and details of blood donors. In case of an emergency, it is sometimes very difficult to get the exact match of blood group thus this may lead to delay of blood transaction. This application is well structured in a manner that a user can search donors using their blood groups to ease blood matching.

Table of Contents

[DECLARATION 2](#_Toc13828150)

[Acknowledgement 3](#_Toc13828151)

[Abstract 4](#_Toc13828152)

[**Abbreviations and acronyms** 7](#_Toc13828153)

[**Chapter 1** 8](#_Toc13828154)

[**1.0 Introduction** 8](#_Toc13828155)

[**1.1 Problem statement** 9](#_Toc13828156)

[**1.2 Proposed solution** 10](#_Toc13828157)

[**1.3 Objectives** 10](#_Toc13828158)

[**1.4 Research questions** 11](#_Toc13828159)

[**1.5 Justification** 11](#_Toc13828160)

[**1.6 Scope** 12](#_Toc13828161)

[**1.7 Methodology** 12](#_Toc13828162)

[**1.7.1 The unified process** 12](#_Toc13828163)

[**1.7.1.1 Key features** 12](#_Toc13828164)

[**1.7.2 Phases of Design Cycles** 13](#_Toc13828165)

[**1.7.2.1 Inception** 13](#_Toc13828166)

[**1.7.2.2 Elaboration** 13](#_Toc13828167)

[**1.7.2.3 Construction** 13](#_Toc13828168)

[**1.7.2.4 Transition** 13](#_Toc13828169)

[**1.8 RESOURCES** 13](#_Toc13828170)

[**1.8.1 Hardware Requirements** 13](#_Toc13828171)

[1.8.2 Software Requirements 13](#_Toc13828172)

[**1.9 BUDGET** 14](#_Toc13828173)

[**1.9.1 BUDGET** 14](#_Toc13828174)

[**1.10 PROJECT SCHEDULE** 15](#_Toc13828175)

[**1.10.1**  **Time Plan** 15](#_Toc13828176)

[**1.11 Gantt Chart** 15](#_Toc13828177)

[**Chapter 2** 17](#_Toc13828178)

[**2.0 LITERATURE REVIEW** 17](#_Toc13828179)

[**Introduction** 17](#_Toc13828180)

[**2.1 Cloud Security** 17](#_Toc13828181)

[**2.2.1 Techniques of cloud security implementation** 17](#_Toc13828182)

[**Encrypted file systems** 17](#_Toc13828183)

[**Trusted Platform Module** 18](#_Toc13828184)

[**Data security using Kerberos operation** 18](#_Toc13828185)

[**System Overview of Cloud Proof** 19](#_Toc13828186)

[**2.2.2 Methods of testing cloud securities** 19](#_Toc13828187)

[Code reviews 19](#_Toc13828188)

[Source code fault injection 19](#_Toc13828189)

[Fuzzy testing 19](#_Toc13828190)

[Vulnerability scanning testing 20](#_Toc13828191)

[Risk based testing 20](#_Toc13828192)

[CONCLUSION 20](#_Toc13828193)

[Chapter 3 21](#_Toc13828194)

[3.0 SYSTEM ANALYSIS AND DESIGN 21](#_Toc13828195)

[3.1Introduction 21](#_Toc13828196)

[3.2 Feasibility Study 21](#_Toc13828197)

[3.2.1 Legal feasibility 21](#_Toc13828198)

[3.2.2 Operational feasibility 21](#_Toc13828199)

[**3.2.2.1 Operational feasibility report** 21](#_Toc13828200)

[**3.2.3Economic feasibility** 22](#_Toc13828201)

[**3.2.3.1 Economic feasibility report** 22](#_Toc13828202)

[**3.2.4 Schedule feasibility** 22](#_Toc13828203)

[**3.2.5 Behavioral feasibility** 22](#_Toc13828204)

[**3.3 Requirement Elicitation** 22](#_Toc13828205)

[**3.3.1 Stratified Sampling** 22](#_Toc13828206)

[**3.3.2 Questionnaires** 23](#_Toc13828207)

[**3.3.2.1 Questionnaire report** 24](#_Toc13828208)

[**3.3.2.2Report from blood donors** 25](#_Toc13828209)

[**3.3.3 Interviews** 27](#_Toc13828210)

[3.3.3.1 Interview report 28](#_Toc13828211)

[**3.3.4 Observation** 29](#_Toc13828212)

[**3.4 Functional Requirements** 30](#_Toc13828213)

[3.5 Non-functional requirements 30](#_Toc13828214)

[3.6 System design 31](#_Toc13828215)

[**3.6.1 Logical Design** 31](#_Toc13828216)

[**3.6.1.1 Flow chart diagrams** 31](#_Toc13828217)

[3.7Database Design 36](#_Toc13828218)

[**3.7.1 Normalization** 36](#_Toc13828219)

[Un-normalized Tables of Data 36](#_Toc13828220)

[3.7.2 ERD- DIGRAM 39](#_Toc13828221)

[*3.7.3Phi*sical design 40](#_Toc13828222)

[3.8 References 42](#_Toc13828223)

# **Abbreviations and acronyms**

**IT:** Information Technology

**KBTS:** Kenya National Blood Transfusion Service

**RBTCs:** Regional Blood Transfusion Centers

**RUP:** Rational unified process

**PCS:** Paper Card System

**BDs:** Blood Donors

**RAM:** Random Access Memory

# **Chapter 1**

# **1.0 Introduction**

The Kenya National Blood Transfusion service was established in the year 2000 under the ministry of health. KNBTS mandate was collecting, testing, processing and distributing of blood and blood products to all transfusing hospitals this is according to (Wikipedia, 2016). Moreover, KNBTS has six Regional Blood Transfusion Centers along with fourteen satellite centers all over the country. (Wikipedia, 2016)

KNBTS depends on the satellite centers and RBTCs and institutions ie.institutions of learning and companies to conduct blood drive. Mostly the KNBTS partner with Kenya Red Cross and other organizations to help in mobilizing and advertisement of blood drives during emergencies (Osaro, 2011). Kenya needs about 400,000 units of blood annually while KNBTS manages to collect 140,000 units annually compared to an estimated population of 42 million people. This is according to (Oduor, 2011).

KNBTS uses paper cards system (PCS) to recruit blood donors (BDS) then later keep the donor records in a local database per station or per region and disseminate results to BDS who are scattered all over the country, the PCS are used to specifically to capture personal data and medical history of the BDs (kimani ,2017). Therefore with this information there is need to automate the process by maintaining all the information pertaining to blood donors, different blood groups available in the store and help them manage in a better way. Furthermore, this will provide transparency in this sector and it will make the process of obtaining blood bank fast, hustle free and corruption free hence the system of blood store management will be more flexible, effective and more reliable.

The proposed project initiates a plan of using cloud computing services and specifically infrastructure as a service. This will enhance easy and fast access of information by the users from anywhere, it will be reliable as one can retrieve data at any given time. This projects’ main concern is on security of data in the cloud. The project initiates plans to secure the donors data and the entire sytems with multiple cloud security solutions while on cloud.

## **1.1 Problem statement**

(KNBTS), each year 400,000 units of blood supply is needed. However, this demand has not been met ever since. Currently the public can only know about blood drives through advertisements, social media, and media stations and through their unpopular site. (Oduor, 2011) With this proposed system, it will be easy monitor, manage and alert blood donors about upcoming blood drives through the mobile application.

The current system requires a potential donor to go through fresh capture of personal and medical record. This is done regardless of whether one has ever donated before. Moreover, the process of recording donor details in every session of blood donation as this is time consuming and tedious the officers in charge of the process can make some errors thus some information may be lost. However with this proposed system the cloud is always available, and contains updated data above all users are assured of data security.

The current information system in use is not operational efficient and flexible hence this makes the process filled with a number of limitations. Firstly, there is no effective centralized database of blood donors with their details. Cloud computing on the other hand allows users to be very flexible in the sense that they can access the application from anywhere and it is always available.

According to (Grobauer, 2011) cloud computing also faces a number of threats that thwarts its services. Firstly, account/service hijacking; it’s often the case that only passwords are required to access account and manipulate data. Therefore the usage of two-factor authentication is mostly preferred to limit hijackers from access. Secondly, data loss; the data stored could be lost due to the hard drive failure. A CSP could accidentally delete the data, an attacker could also modify the data. Therefore this project intends to use the best way to prevent data loss by putting in place proper data backup solutions, which solves the data loss problems. Finally, Secure Data Transmission; when transferring the data from clients to the clients to the cloud, the data needs to be transferred by using an encrypted secure communication channel like SSL/TLS. Hence, this prevents different attacks where data could be stolen by an attacker intercepting communication. (Walloschek, 2011).

## **1.2 Proposed solution**

According to the statement of problem above it is now evident that the existing system has many limitations. Furthermore this field needs error free and fast system since the blood are mostly needed in emergency situation to save life. Therefore, this research intends to implement an online cloud based blood store and mobile application that will automate the process of mobilizing, donor education, recruiting and searching of blood donors and supply of blood-to-blood procurers.

The cloud based online blood store management information system is intended to automate and ease the process of searching for blood in case of emergency and maintain records of blood donors, blood donation programs and bloodstocks. Furthermore, this application will also assist in connecting blood donors to blood procurers online; users will be able to view information about the registered donors such as name, location, personal information along with medical information and their details of blood group.

This project intends to use a database management system; database is collection of related data stored in a disk and accessible possibly by many concurrent users. Therefore, this project has been planned to be having the view of distributed architecture, with centralized storage of the database along with the constructs of MS-SQL server while all user interfaces designed using android technologies.

This application initiates a plan to register blood donors as per their location thus this will ease emergency situations and in case there is need of blood drive the registered donors will be easily contacted. This system is well structured to have all volunteer donors and their records in a centralized database to ease the process of blood searching in case of an emergency. Moreover, it will be easy to help choose the donor with right medical details and right blood group.

Automated system will able to keep track of each blood type available in the store.

## **1.3 Objectives**

Objective; specific result that a person or a system aims to achieve within a period and with available resources.

To investigate cloud securities on mobile applications.

To examine techniques of implementing cloud securities

To establish methods of testing cloud securities.

## **1.4 Research questions**

What is the role cloud securities on mobile applications?

What are the techniques of implementing cloud securities?

What are the methods of testing cloud securities?

## **1.5 Justification**

This project is important because it intends to implement a cloud-based mobile application platform that that will enable people to contribute towards saving lives of people who need blood. Therefore, this system will connect blood donors to blood procurers easily. Moreover, with this system, it will be easier and faster to search for matching blood; this will be done by simply searching for a donor using the blood type and blood specification needed. Furthermore, it will also be easier to search for donor using location as well as name.

This system will save reduce death rates in that the system also contains donor’s details and contact information so that those in need of blood don’t take much time in searching for blood donors whom they have no information about them and their whereabouts. Finally this system will be flexible and effective in emergencies as it will save time and hustle of searching for blood donors. Using this platform will be of great benefit to users some of the benefits this platform will earn the users include.

**Being up to date**, this proposed system will have the most recent data considering that considering that there will be continuous update of the database.

**Improved mobility;** Users will be sure of data availability to them no matter where they are in the country. Moreover, users can access the platform from anywhere via smart phones and tablets, laptops provided there is internet access.

**Availability;** access to the platform will be available at any time, provided the user is connected to the internet

**Flexibility;** the cloud platform is very flexible as users are able to access the platform from any location without any limitation

**Cost;** using the cloud services is more cheaply compared to hiring physical servers.

## **1.6 Scope**

This project initiates an execution plan that will be done in regional blood transfusion centers, satellite centers, hospitals and organization that will organize for blood drives. Furthermore, this project aims at implementing a well-structured and effective cloud based web application that will enhance donor mobilization, fast blood donation, blood searching, donor education and successful blood drives hence this will help save life.

# **1.7 Methodology**

## **1.7.1 The unified process**

The unified process is a traditional cathedral style of incremental design driven by constructing views of system architecture.

### **1.7.1.1 Key features**

1. it is component based commonly used to coordinate object oriented programing projects
2. it uses UML a diagrammatic notation for object oriented design
3. The design process is anchored, and driven by use cases, which help keep sight of the anticipated behaviors of the system.
4. It is architecture centric and its design is iterative via a prescribed sequence of design phases within a cyclic process.

## **1.7.2 Phases of Design Cycles**

Design in the unified process proceeds through a series of cycles, each of which has the following phases.

### **1.7.2.1 Inception**

Produces a commitment to go ahead and by the end of this phase a business case should have been made, feasibility of the project assessed and the scope of the design should be known.

### **1.7.2.2 Elaboration**

Leads to a working specification of the system and at the end of this phase a basic architecture should have been produced a plan of construction agreed, all significant risks identified, and those risks identified, and those risks considered to be major should have been addressed.

### **1.7.2.3 Construction**

Produces beta-release system and the end of this phase a working system should be available, sufficient for preliminary testing under realistic conditions.

### **1.7.2.4 Transition**

Introduces the system to its intended users

# **1.8 RESOURCES**

## **1.8.1 Hardware Requirements**

1. Laptop with the following
2. Memory (RAM) -1GB
3. Hard Disk space -80GB
4. Processor- 1.6 GHz
5. Modem

## 1.8.2 Software Requirements

Windows 7 operating system

Microsoft SQL SERVER

Microsoft android studio 2010

Virtualization software

# **1.9 BUDGET**

## **1.9.1 BUDGET**

|  |  |  |  |
| --- | --- | --- | --- |
| **ITEM** | **PRICE PER UNIT** | **NO. OF UNITS** | **TOTAL (KSH)** |
| Laptop | 30,000 | 1 | 30000 |
| Modem | 3,000 | 2 | 3,000 |
| Antivirus software(Kaspersky) |  | 1 | 1,200 |
| Miscellaneous |  |  | 3,000 |
| Internet |  |  | 3,500 |
| Total |  |  | 40,700 |

# **1.10 PROJECT SCHEDULE**

## **1.10.1 Time Plan**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **Duration weeks** | **Proposed start date** | **Proposed finish date** | **Actual start date** | **Actual finish date** | **Deliverables** |
| **1** | Project identification | **1** | **10/01/19** | **15/01/19** | **12/01/19** | **16/01/19** | Problem statement definition |
| **2** | Draft proposal | **1** | **20/01/19** | **23/01/19** | **22/01/19** | **28/01/19** | Draft proposal |
| **3** | Final proposal | **2** | **29/01/19** | **4/02/19** | **29/02/19** | **11/02/19** | Final proposal |
| **4** | Literature review | **1** | **01/05/2019** | **7/05/2019** | **25/05/2019** | **06/06/19** | Literature review |
| **5** | Data collection and analyses | **2** | **10/05/2019** | **22/05/2019** | **14/05/2019** | **06/06/19** | Requirement specification |
| **6** | System design | **3** | **25/05/2019** | **01/06/2019** | **10/06/2019** | **06/06/19** | System design |
| **7** | System development | **4** |  |  |  |  | Working system |
| **8** | Testing | **2** |  |  |  |  | Working system |
| **9** | Project report | **1** |  |  |  |  | Project report |
|  |  |  |  |  |  |  |  |

## **1.11 Gantt Chart**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Activities** |  | **JAN** | | | | **FEB** | | | | **MARCH** | | | | **APRIL** | | | | **MAY** | | | | **JUNE** | | | | **JULY** | | | |
| **Week** | **Hrs.** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** |
| Project Identification | 3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Draft Proposal  Writing | 8 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Final Proposal | 8 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Literature Review | 8 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Data collection and analyses | 12 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| System design | 48 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| System Development | 48 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Testing and Implementation | 12 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Project Report |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Table 3: GANT CHART

KEY: Proposed time  Actual time

# **Chapter 2**

# **2.0 LITERATURE REVIEW**

## **Introduction**

This chapter discusses literature on cloud security and various frameworks and approaches to be used to develop an efficient mobile blood bank application. This chapter also initiates a plan to speak volume on how to create a top most secured cloud environment that is free from threats and intruders.

## **2.1 Cloud Security**

Cloud security consist of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems data and infrastructure.( Hashizume, 2013). Furthermore, these security measures are put in place to protect data, support regulatory compliance and protect customers’ privacy as well as setting authentication rules for individual users and devices. However, cloud security also faces challenges 1**) Data breaches** which is caused by human error, application vulnerabilities or poor security practices.2) **Access management** the cloud offers access of data from anywhere but only authorized users of the application should be allowed access. 3) **Denial of service attack** this attack has its final goal to stop the functioning of the targeted application so that no one can access it. 4) **APTs advanced persistent threats** this are parasitical form of cyber-attack that infiltrates systems to establish a foothold in the IT structure of target applications, this is according to (Avram, 2014)

## **2.2.1 Techniques of cloud security implementation**

### **Encrypted file systems**

Encryption is use of complex algorithm to hide original information with the help of encryption key. Furthermore, the data is converted onto unreadable form called cipher text and then stored into a remote server.( Priya, 2015) EFS system is a technique used to encrypt data within the cloud with the help of encryption key along with the development of protocols which ensures that data is stored only on trusted servers. However,this enhances integrity of the data within the cloud this is according to (Grabelkovsky, 2015) (Priya, 2015) Argues that strong encryption of file systems protects data integrity but in some circumstances encryption accidents can make data useless and end up complicating the availability of data.

### **Trusted Platform Module**

The trusted platform module is a computer microchip or a micro controller, which is installed on the motherboard of computer to perform various security tasks and cryptography. (Haeger, 2015) This technique provides the tools such as certificates, encryption keys, passwords and integrity metrics to authenticate the cloud platform. (Carter, 2015) Each TPM chip contains an RSA key called the endorsement key. The pair is maintained inside the chip and cannot be accessed by software. Furthermore, the storage root key is created when a user or administrator takes ownership of the system. Moreover, the key pair is generated by the TPM based on the endorsement key and an-owner specified password (Carter, 2015) Second key called an attestation identity key protects the device against unauthorized firmware and software modification by hashing critical sections of firmware and software before they are executed. However when the systems attempts to connect to the network the hashes are sent to a server that verifies that they match expected values this is according to (Haegar, 2015) TPM is widely underused and yet has best information security methods. However TPM limits user to a single computer that has been fitted with the microchip due to store of keys moreover this makes other devices impractical.

### **Data security using Kerberos operation**

Kerberos uses the technique of strong encryption method and complex ticket granting algorithm. This ensures the gets authenticated on network and it also uses a session key which allow encrypted data stream over an IP network for each user registering with Kerberos. Moreover, the user will get his user ID and password which is stored on server database, this is described in details by (Sharma, 2014).

Kerberos employs client-server architecture and provides user-to-server authentication rather than host-to-host authentication. Moreover Kerberos security model and authentication is solely based on secret key sharing technology.in cloud every host network owns its own secret key therefore it would be irrational if every host had to know the key of all other hosts. However, there is in existence a key distribution center, which knows all keys, Kerberos, fixes the problems of configuring new node on a network by providing single sign-on, which lets user log into the system and access multiple systems and applications. Kerberos has various benefits that makes it outstanding, Kerberos, does not transmit unencrypted passwords over the network, it protects against replay attacks (misuse of intercepted credentials) (Plotnik, 2017), it also do not require the user to repeatedly enter a password to access routine services. On the other hand Kerberos also has various drawbacks hence (Carter, 2017) argues that the system always depends on passwords for user authentication if the pass codes are stolen the possibility of the system being attacked is very high.

### **System Overview of Cloud Proof**

This technique presents a secure storage system specifically designed for cloud clients. Using cloud proof customers can detect integrity of customers data is violated. Cloud proof operates in line with four goals. Firstly, Customers should know if service provider has violated the integrity of the data, furthermore client’s data must be private and confidential from outsiders. This can be achieved by encrypting data stored on the cloud. Secondly, customers should be able to prove cloud violations from their end. Thirdly, cloud proof should provide for read and write access control in a scalable way. Lastly, cloud proof should maintain the performance, scalability, and availability of cloud services despite adding security.

## **2.2.2 Methods of testing cloud securities**

### Code reviews

Source code review also known as static analysis is the process of manually checking source code for security weakness. (Khan, 2016). According to serious security, any other form of analysis cannot detect vulnerabilities or testing .with the source code a tester can actually trace errors. (Aljawarneh, 2017). Code review is productive when identifying security vulnerabilities. Automated code reviewing facilitates systematic testing of source code for potential trouble such as buffer overflows, race conditions, memory leakage, size violations and duplicate statements. May be especially productive for identifying security vulnerabilities. However, it is so hard to ensure code review quality and promptness due the many lines of codes to review

### Source code fault injection

This is a testing technique used to induce stress in the software, and create interoperability problems among components. This technique also simulate faults in the execution environment and thereby reveal safety-threatening faults that are not made. (Rao, 2017) This technique automatically extends fault injection by adding errors, thus enabling testers to analyze security of the state changes of the software when it is exposed to the cloud environment. . (Khan, 2016)

### Fuzzy testing

This is a mechanism of injecting random data in to the cloud based Application do determine whether it can run normally under the jumbled input. This testing technique helps in discovering security vulnerabilities moreover it’s a very effective way of testing and it detects hidden flaws which are difficult for other testing modes to detect.(khan, 2016) Fuzzy testing is also used by hackers seeking to gain information about systems and system responses to use in formulating attacks. Therefore, it is important to identify and evaluate vulnerabilities and risk using tools that can be utilized to attack your application in a cloud platform. (Chang, 2016) Fuzzy testing enhances software security testing. On the other hand, data from fizzers can be difficult to interprete and it takes a lot of time to complete its testing circles.

## Vulnerability scanning testing

This technique tests space scanning, by running the application to determine leakage that the application might have created. (Khan, 2016). There are two types of approaches for vulnerability scanning, authenticated and unauthenticated scans. In the unauthenticated method, the tester performs the scan, as an intruder would scan without trusted access into the network hence this type of scans reveals vulnerabilities that are accessible to a trusted user, or an intruder that has gained access into the system. Vulnerability systems should be patched or updated if possible to address the identified vulnerabilities. . (Chang, 2016) On the other hand for flaws that don’t have an applicable patch the identified risk should be taken into account and additional mitigation procedures should be taken to minimize the exposure of the vulnerable system. However intruders and attackers have advanced by attacking and infiltrating scanners hence the scanners get too weak to detect vulnerable.

### Risk based testing

To review security requirements and to identify security risks. (Chang, 2016) This is done in design phase of development. Threat modelling is a methodological process that is used to identify threats and vulnerabilities in a software. This helps system designers to analyze and think about the security threat that the system might face. . (Khan, 2016) Therefore, threat development is carried out as risk assessment for software development. Hence, this helps the developer to develop mitigations for future threats and vulnerabilities.

# CONCLUSION

This paper has made major contribution on cloud computing security. Firstly, it has presented major techniques of securing cloud infrastructure and ways to implement cloud based application. This research has also mapped methods used to test cloud security. Finally, the ultimate goal for this research study is to provide a basis on further reaction to cloud insecurity. This research recommends use of cloud security techniques to mitigate future attacks.

# Chapter 3

### 3.0 SYSTEM ANALYSIS AND DESIGN

### 3.1Introduction

## 3.2 Feasibility Study

The purpose of this study is to examine in depth the ability of the proposed system based on its workability, operability, meeting user requirements, and cost effectiveness. Feasibility study is categorized into several types that include the following

### 3.2.1 Legal feasibility

The aim of this legal study is to determine whether the proposed system conforms to the legal requirements set. This proposed system strictly conforms to the law and intends not to violate any law set. Furthermore, it complies with the local data protection act, intellectual properties laws and access to information law.

### 3.2.2 Operational feasibility

The study was carried out to determine whether the proposed system was meeting the requirements, which were gathered during the survey. This feasibility also included setting up of schedules of system implementation. The system initiates a plan of easing the operation process by solving problems like blood drives and help management improve the process of blood matching and blood searching as the cloud based mobile application will be able to link the blood donors and procurers online. Moreover, for the proposed system to be operationally feasible the organization will have to incur some cost in educating the users on how to work with system

### **3.2.2.1 Operational feasibility report**

For the proposed system to be operationally feasible, the organization will have to incur some cost in educating the users on how to work with the new system. The departmental structure will hardly change since the system will be designed to suite the structure of the department. The system will be developed in such a way that it becomes very easy even for a person with little web knowledge to operate it.

### **3.2.3Economic feasibility**

Purpose of the economic feasibility is to perform a cost benefit analysis. This is an analysis of the of the costs to be incurred in the system. This includes cost of design, development and implementation.

### **3.2.3.1 Economic feasibility report**

According to the analysis done, the organization will incur some cost in purchasing some hardware equipment’s according to the system architecture and also in training of the users although due to the computer literacy level of the employees the training will be very minimal. However, despite the costs, the organization is able and willing to invest in this project since the major problems they face will be minimized. Moreover, the way of working will be highly improved, and thus this project will be economically feasible.

### **3.2.4 Schedule feasibility**

The proposed system will involve evaluating to what extent the system will take to develop and in the event that it tends to be finished in a given timespan. The system will take roughly 3months to be developed. Fundamentally, this will proportion out of how sensible the task timetable will be consequently feasible.

### **3.2.5 Behavioral feasibility**

Behavioral feasibility determines how much exertion will go in selling the proposed system, and in education and training the account staff (the admin) on the new system, along with the new ways of conducting the business. Behavioral study strives on ensuring that the equilibrium of the organization is not disturbed. The staff should readily accept the changes.

## **3.3 Requirement Elicitation**

Thefollowing data collection and sampling techniques were used

### **3.3.1 Stratified Sampling**

This method first divides population who share similar characteristics into subgroups called strata hence this helps to capture representation from all subgroups. However, this method does not require equal sample sizes from the strata groups created. Therefore, for every strata created one choose randomly the population size to work with. This research chose to work with three groups of the population, which are Blood donors, patients, and KNBTS staff.

**KNBTS staff**

|  |  |  |
| --- | --- | --- |
| Staff type | operational | managerial |
| Number of staff | 200 | 50 |
| Randomly selected | 20 | 10 |

**Blood Donors**

|  |  |
| --- | --- |
| Possible number of donors | 100 |
| Randomly selected | 10 |

**Patients**

|  |  |
| --- | --- |
| Possible number of Patients | 30 |
| Randomly selected | 10 |

### **3.3.2 Questionnaires**

Formulated questions were used to help facilitate the process of data collection. Furthermore, the question used were open-ended and close ended and were issued to the stakeholders who complied by giving their responses. This tool helped in the collection of data from both blood donors and the KNBTS staffs this process took place at the blood donation centers and KNBTS offices.

**Questionnaire questions**

**Summary**

**Section 1**

1. Do you own a smartphone or a tablet? yes or no
2. Have you ever heard of computer cloud technology before? Yes or No
3. Any cloud services that you know-------------------------.
4. How secure do you think the cloud services are? A.Very secure B. Not secure C. Not sure
5. Can you trust any cloud operating company with your data? Yes or No, if yes how flexible do you think the cloud services are? A. Very flexible B. Not flexible C. Not sure

**Section 2**

1. Are you a registered donor? Yes or No?
2. Have you ever received or donated blood before? Yes or No, if YES how often----------?
3. How easy is the process of finding your blood match? A.Very easy, B.Very hard, C.Takes sometime
4. How efficient is the process of blood donation? A.Very slow, B.Very fast, C. None
5. What recommendations would you give in the process of blood procurement for patients and blood donations by donors--------------------------------------------------------------?

### **3.3.2.1 Questionnaire report**

**KNBTS staff questionnaire report**

### **3.3.2.2Report from blood donors**

## **3.3.3 Interviews**

In this technique, data was collected from different patients with each of the patient in intervals of approximately 10 -15 minutes. The content of the interview was involved in asking questions and capturing any necessary information that pertained cloud knowledge of cloud security, cloud flexibility as well as current blood management system and the improvements that should be made if need be. This research chose to interview the patients due to their conditions. This process took place in hospitals, Kenyatta National hospital and Mbagathy hospital.

**Interview questions**

**Summary**

**Section 1**

1. Do you own a smartphone or a tablet? yes or no
2. Have you ever heard of computer cloud technology before? Yes or No
3. Any cloud services that you know-------------------------.
4. How secure do you think the cloud services are? A.Very secure B. Not secure C. Not sure
5. Can you trust any cloud operating company with your data? Yes or No, if yes how flexible do you think the cloud services are? A. Very flexible B. Not flexible C. Not sure

**Section 2**

1. Are you a registered donor? Yes or No?
2. Have you ever received or donated blood before? Yes or No, if YES how often----------?
3. How easy is the process of finding your blood match? A.Very easy, B.Very hard, C.Takes sometime
4. How efficient is the process of blood donation? A.Very slow, B.Very fast, C. None
5. What recommendations would you give in the process of blood procurement for patients and blood donations by donors--------------------------------------------------------------?

### 3.3.3.1 Interview report

## **3.3.4 Observation**

It involves the study of the environment, people and objects to obtain information and data. The main aim of using this type of data collection was to get close as possible to the real system. Observation helped to see how people relate with the current system. The reason why the researcher used this type of data collection is that one can observe what people actually do or say. Observation can be strong validity and in-depth understanding of the current system. As well, enable access to situation and people where questionnaire and interviews are impossible to use. The information gathered was very meaningful since there was no biasness.

## **3.4 Functional Requirements**

**Login**

The system provides security features through username-password matching where only authorized user can access the system with different authorization level.

**Advertisements of blood donation event**

This function allows the blood bank staff to publicize the blood donation events online. The public can view the venue and time of the blood donation programs to be held.

**Donor Profile Registration**

This allows healthy public to register as volunteer donor.

**Online Request for fresh blood**

This allows the probable recipients to make online request to the donor. After the request has been filed, donors are matched and the request is sent via SMS with necessary details.

**Blood Stock Management**

The blood bank staffs can manage the bloodstock starting from the blood collection, to blood screening, processing, storage, transference and transfusion through this system. Each process or workflow can be traced from the database. The system will also raise alert to the staff whenever the blood quantity is below its par level or when the blood in stock has expired.

**Donor/Recipient Management**

The records of all donors/recipient and their history are kept in one centralized database and thus reducing duplicate data in the database. The record of donation is maintained by the system.

**Reporting**

The system is able to generate pre-defined reports such as the list of donors, recipients,

## 3.5 Non-functional requirements

The non- functional requirements are follows

**Adaptability**

The system will be easy to adapt from one type of environment to another without any difficulties.

**Maintainability**

The experts should have the ease of maintaining the system by, correcting errors, preventing breakdown, perfecting the system and ensuring that it adapts to the changing technology and needs of the user.

**Usability;** The system will be friendly to all users with or without much computer knowledge due to simple user interfaces and proper documentation of the system.

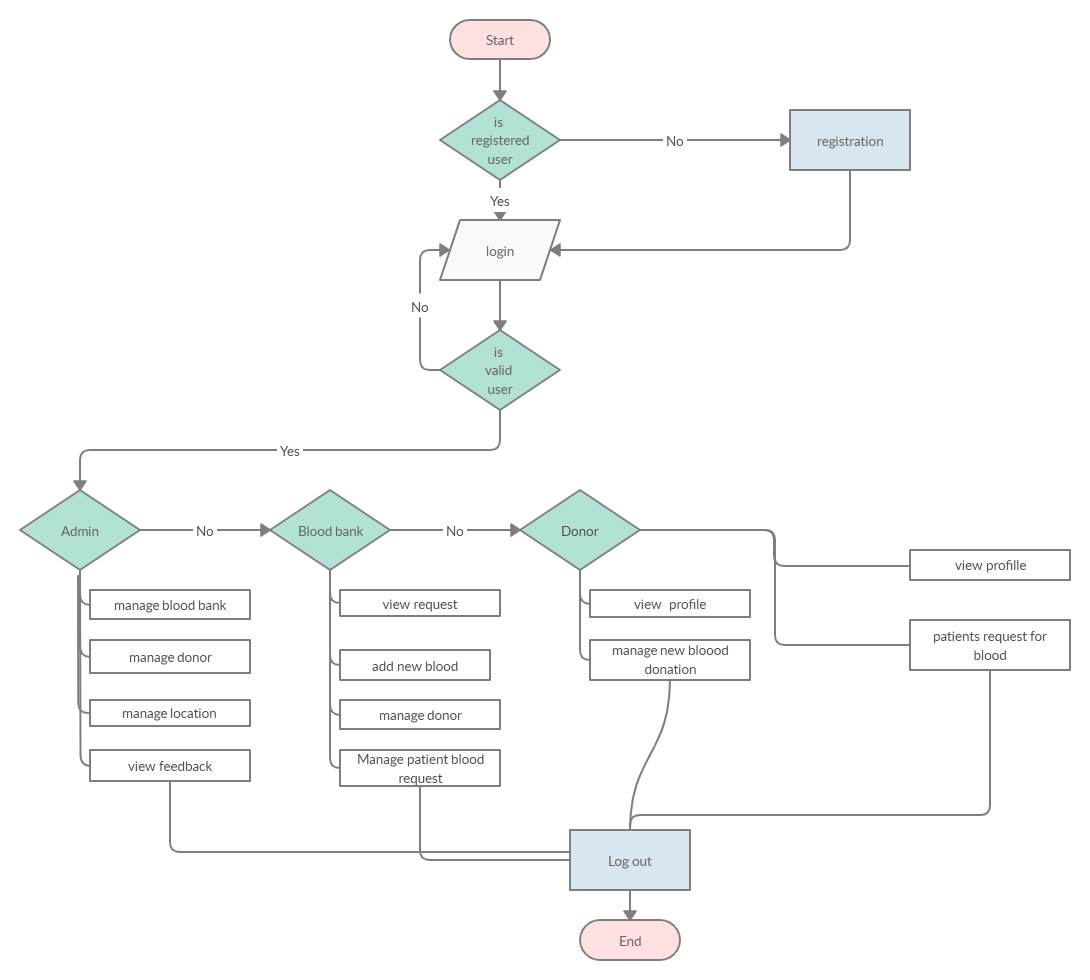
**Economy;** The system will be affordable and within the budget specified

## 3.6 System design

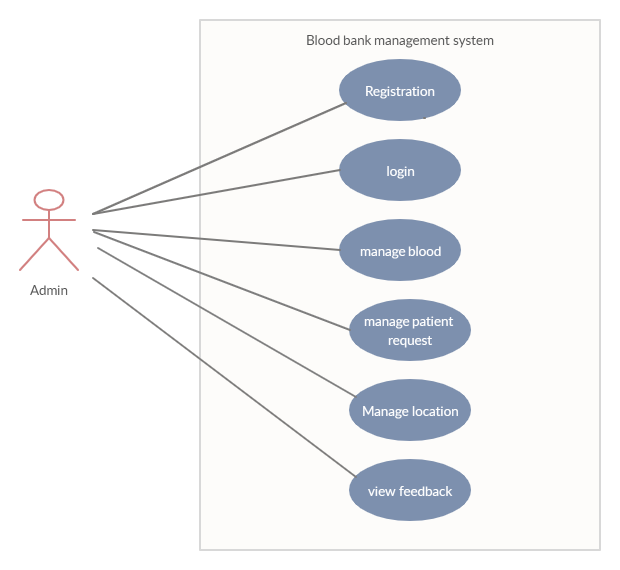
System design is the process of defining the architecture, components, modules, interfaces and data for a system to satisfy specified requirements. System design is therefore the process of defining and developing systems to satisfy specified requirements of the user.

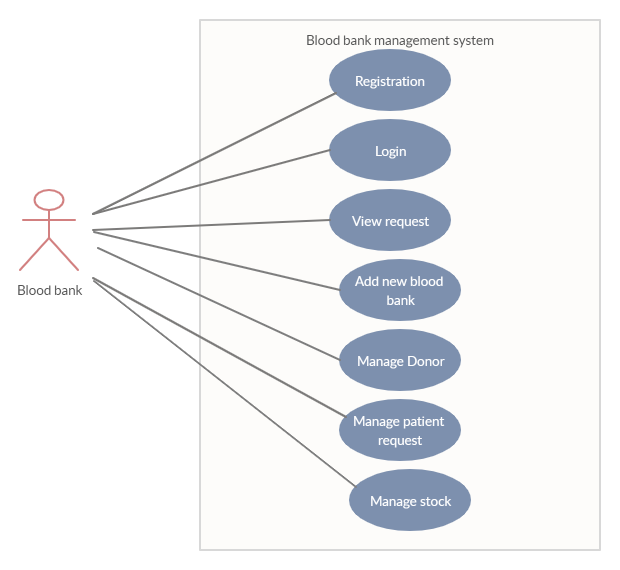
## **3.6.1 Logical Design**

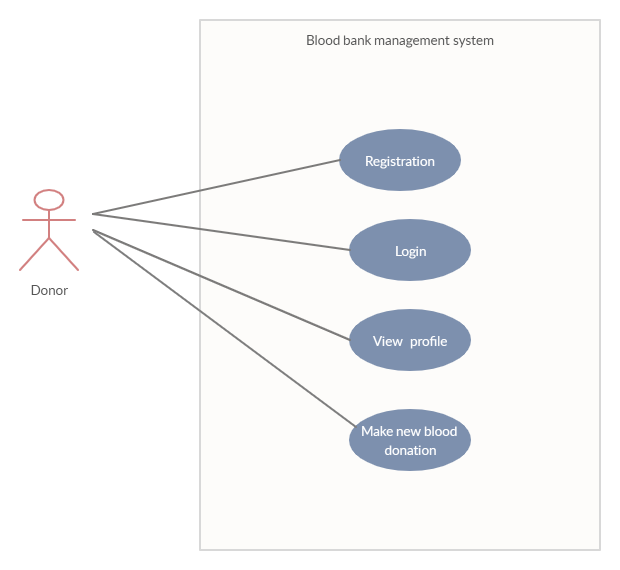
## **3.6.1.1 Flow chart diagrams**

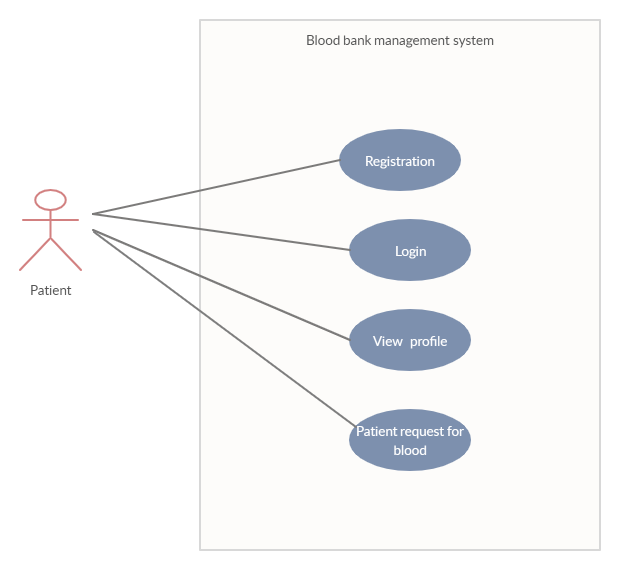


#### **3.6.1.2 USE CASES**









## 3.7Database Design

### **3.7.1 Normalization**

**The zero normal form (ONF)** the un-normalized/the zero-normal form data sets would be:

### Un-normalized Tables of Data

donor\_id, Username, User\_phone, Admin\_id, password

Location, Admin\_username, Admin\_password

**The First Normal Form (1NF)**

All columns must be atomic (no repeating groups). Once the un-normalized data set has been identified, it is converted into the first normal forms and primary keys are identified.

Table 1: donor\_id, donor\_name,donor\_bloodgroup, donor\_phone, location\_id

Table patient\_id, patient\_name, patient\_phone, patient\_ bloodgroup patientlocation\_id

**The second normal form (2nf)**

Patient\_name, patient\_bloodgroup

**The third normal form (3nf)**

Admin\_id=admin \_username, admin \_password, admin \_phone

The database system should have the following tables;

**Admin table**

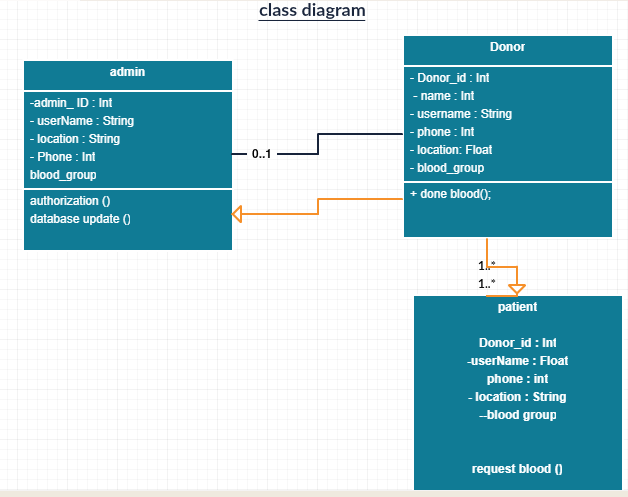
|  |  |  |  |
| --- | --- | --- | --- |
| **Field name** | **Data type** | **Primary key** | **null** |
| id\_admin | Int (10) | yess | no |
| username | Varchar (20) | no | no |
| password | Varchar (20) | no | no |
| Phone | Int (10 ) | no | no |
| location | Varchar(20) | no | no |
| Blood\_group | Varchar( 10) | no | no |

**Patients table**

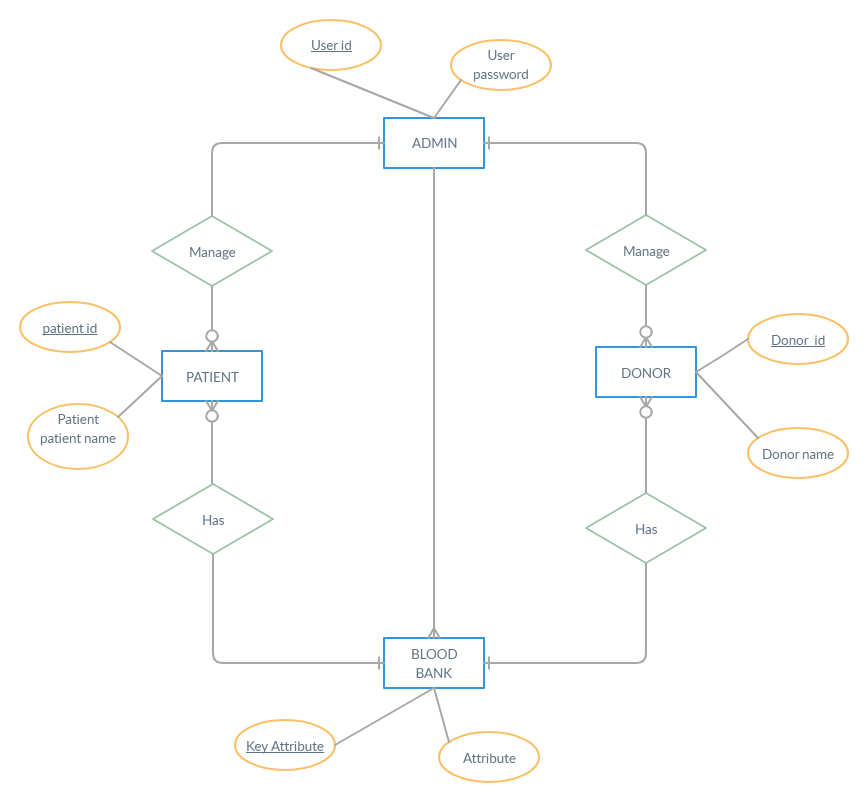
|  |  |  |  |
| --- | --- | --- | --- |
| **Field name** | **Data type** | **Primary key** | **null** |
| Member\_id | Int( 10) | yess | no |
| Username | Varchar (20 | no | no |
| password | Varchar (20 | no | no |
| Blood\_group | Varchar (20 | no | no |
| location | Varchar (20 | no | no |

**Donors table**

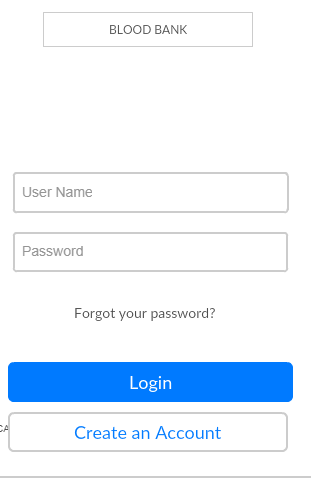
|  |  |  |  |
| --- | --- | --- | --- |
| **Field name** | **Data type** | **Primary key** | **null** |
| Donor\_id | Int (15) | yess | no |
| username | Varchar (20) | no | no |
| phone | Int(10) | no | no |
| password | Varchar (20) | no | no |
| Blood \_group | Varchar 20 | no | no |
| Location | Varchar (20) | no | no |
|  |  |  |  |

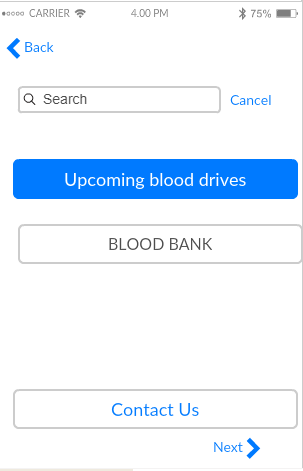
****

## 3.7.2 ERD- DIGRAM

**

## *3.7.3Phi*sical design





## 3.8 References

1. Abdallah, F., Mwanda, O. W., & Rana, F. (2005). Comparing walk-in and call-responsive donors in a national and a private hospital in Nairobi. *East African medical journal*, *82*(10).
2. Aljawarneh, S. A., Alawneh, A., & Jaradat, R. (2017). Cloud security engineering: Early stages of SDLC. *Future Generation Computer Systems*, *74*, 385-392.
3. Avram, M. G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*, *12*, 529-534.
4. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation computer systems*.
5. Beller, M., Bacchelli, A., Zaidman, A., & Juergens, E. (2014, May). Modern code reviews in open-source projects: Which problems do they fix?. In *Proceedings of the 11th working conference on mining software repositories* (pp. 202-211). ACM.
6. Chang, V., & Ramachandran, M. (2015). Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing*, *9*(1), 138-151.
7. Carter, S. R., Green, T. A., & Isaacson, S. A. (2015). *U.S. Patent No. 9,135,444*. Washington, DC: U.S. Patent and Trademark Office
8. Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless communications and mobile computing*, *13*(18), 1587-1611.
9. Grabelkovsky, M. (2015). *U.S. Patent No. 8,990,558*. Washington, DC: U.S. Patent and Trademark Office.
10. Haeger, E. S., Schurig, K., Cenname, M., Elliott, S., & Skowronski, A. (2015). *U.S. Patent No. 9,137,222*. Washington, DC: U.S. Patent and Trademark Office.
11. Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. *IEEE Security & privacy*, *9*(2), 50-57.
12. Hanssen, G. K., Bjørnson, F. O., & Westerheim, H. (2007, September). Tailoring and introduction of the rational unified process. In *European Conference on Software Process Improvement* (pp. 7-18). Springer, Berlin, Heidelberg.
13. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of internet services and applications*, *4*(1), 5.
14. Kimani, D., Mwangi, J., Mwangi, M., Bunnell, R., Kellogg, T. A., Oluoch, T., ... & Oduor, M. (2011). Blood donors in Kenya: a comparison of voluntary and family replacement donors based on a population‐based survey. *Vox sanguinis*, *100*(2), 212-218.Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial management & data systems*, *111*(7), 1006-1023.
15. Li, B. N., Chao, S., & Dong, M. C. (2007). SIBAS: A blood bank information system and its 5-year implementation at Macau. *Computers in Biology and Medicine*, *37*(5), 588-597.
16. Mao, M., & Humphrey, M. (2012, June). A performance study on the vm startup time in the cloud. In *2012 IEEE Fifth International Conference on Cloud Computing* (pp. 423-430). IEEE.
17. Njeru, D. G., Mwanda, W. O., Kitonyi, G. W., & Njagi, E. C. (2009). Prevalence of cytomegalovirus antibodies in blood donars at the National Blood Transfusion Centre, Nairobi. *East African medical journal*, *86*(12), 58-61.
18. Osaro, E., & Charles, A. T. (2011). The challenges of meeting the blood transfusion requirements in Sub-Saharan Africa: the need for the development of alternatives to allogenic blood. *Journal of blood medicine*, *2*, 7.
19. Pokorny, J. (2013). NoSQL databases: a step to database scalability in web environment. *International Journal of Web Information Systems*, *9*(1), 69-82.
20. Plotnik, I., Be'ery, T. A., Dolinsky, M., Plotnik, O., Messerman, G., & Krigsman, S. (2017). *U.S. Patent No. 9,729,538*. Washington, DC: U.S. Patent and Trademark Office.
21. Priya, A., Rana, Y. K., & Patel, B. P. (2015). Design and implementation of an algorithm to enhance cloud security. *International Journal of Computer Applications*,
22. Rajab, J. A., Muchina, W. P., Orinda, D. A. O., & Scott, C. S. (2005). Blood donor haematology parameters in two regions of Kenya. *East African medical journal*, *82*(3).
23. Ramollari, E., Dranidis, D., & Simons, A. J. (2007, June). A survey of service oriented development methodologies. In *The 2nd European Young Researchers Workshop on Service Oriented Computing* (Vol. 75).
24. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.
25. Sharma, R., & Trivedi, R. K. (2014). Literature review: cloud computing–security issues, solution and technologies. *International Journal of Engineering Research*, *3*(4), 221-225.
26. Trepalin, S. V., & Yarkov, A. V. (2001). CheD: chemical database compilation tool, internet server, and client for SQL servers. *Journal of chemical information and computer sciences*, *41*(1), 100-107.
27. Yao, K., & Luman, E. T. (2014). Evidence from 617 laboratories in 47 countries for SLMTA-driven improvement in quality management systems. *African journal of laboratory medicine*.