Journal of Information Systems and Telecommunication
Vol.12, No.4, October-December 2024, 300-312
http://jist.acecr.org
ISSN 2322-1437 / EISSN:2345-2773

Design and Analysis of a Secure Intelligent Blood Management Information System

Hessah Alhajri[1], Mostafa Abd El-Barr[2], Kalim Qureshi[1*]

[1].Department of Information Science, College of Life Sciences, Kuwait University, Kuwait
[2].Department of Electrical Engineering, College of Engineering, Badr University in Cairo, Egypt.

Received: 15 Feb 2024/ Revised: 04 Nov 2024/ Accepted: 11 Dec 2024

Abstract

The need for blood and the blood donors are on the rise continuously. Poor communication between blood banks and hospitals results in improper management and wastage of available blood inventory and can cause life threats. Therefore, there is an urgent need for coordination between blood banks, hospitals, and blood donors. The Design of a Secure Intelligent Blood Bank Information System (SIBBIS) is a way to align blood banks and hospitals with the help of the Internet. SIBBIS is a web application through which registered hospitals can check the availability of required blood, send a request for blood to the nearest blood bank or donor that matches the blood requirements, and order blood online as requested. A blood bank can also send a request to another blood bank in case of unavailable blood. The person willing to donate blood can find the nearest blood banks using SIBBIS. The location of the blood bank can be traced using maps. The life of the hardware, software, refrigerator cleaning of refrigerator and vaccination of employees are monitored intelligently. For this system, we developed a standard process-oriented information System analysis methodology using use case, activity, system sequence, entity relationship, and class diagrams. The usability of the developed system was evaluated, and it was 93.39%.

Keywords: Blood Bank; Information System; Security of Information System; Blood Donation.

1- Introduction

The need for blood is increasing due to the increase in the population. Humans can suffer from serious and significant health issues and even die from blood deficiency. Blood cannot be produced in the laboratory by medical science, but it can be transferred from one person to another with the guidance of medical science [1]. An ailing patient can go through several serious emergencies that cause bleeding and, hence, blood loss, which could be accidents, anemia attacks, surgical operations, and pregnancy, to name a few.

The traditional NACO blood bank management system requirement of paperwork is inefficient and error-prone, which cannot be tolerated in the time of emergency. Existing systems were designed to meet the incredibly huge and urgent demand for blood. Modern blood storage systems have been constructed to bridge the gap between blood recipients in need of blood and blood donors. It was observed that most patients who are in urgent need of blood do not get blood on time due to the lack of communication between the blood recipients and blood donors. Improper management between the blood banks, blood donors, and hospitals lead to waste of the available blood inventory. There is a critical need for an efficient, real-time management system for communication and synchronization among the different constituents of the blood system stage players. This serious issue prompted us to devise a plan to build a secured intelligent blood bank information system to ensure that blood is always available in emergencies and that the appropriate donor is available [2]. Through the proposed system, the blood seeker should be able to view all information they need. Such information could be related to the donor, blood bank, and hospital. When the new user accesses the system. When a new user logs in to the system as a seeker or donor, they must provide valid information to prove their identity, such as their civil ID, driver's license, to authenticate the blood type [3].

✉ **Kalim Qureshi**
Kalimuddinqureshi@gmail.com

The most serious concern in our proposed system is security. Sensitive information, such as patient information, must be kept secure and private when stored in a database. Users that use the proposed system are identified and their identities should be properly verified. Communication within the proposed system should be treated with confidentiality and not intentionally corrupted.

1-1- Objectives

In cases of epidemics, disasters, and wars, the need for large quantities of blood is critical. Large quantities of blood cannot be stored, so the presence of a system for preserving the data of all donors is required. Such a system should facilitate communication with these donors in the event of a need for blood donation [4]. Hence, this growth motivates build a system able to acquire the following objectives and innovations:

- *track* the quantities of blood and track the requests.
- *analyz*e the standards from the World Health Organization regarding blood donation.
- *monitor* the devices specified for storing blood.
- *match* the suitable blood types automatically.
- *allow* the administrator to monitor the health/life of all connected equipment.
- *monitor* the health of all staff and the health status of all registered employees.
- *work* according to the guidelines of the World Health Organization for all blood transfusions.
- *allow* the staff to know all related information about the packages of blood.
- *manage* the components of blood and display all related information.
- *track* donors and contact them easily (after getting their acceptance).
- *check* all documents that certify that the donated blood is clear of viruses.

The Research Questions (RQs) of our research work are set to be the following:

RQ1: What are the current functional requirements of building a blood bank information system?

RQ2: What are the current non-functional requirements of building a blood bank information system?

RQ3: How to ensure the availability of a blood bank information system's equipment?

RQ4: How to manage the hygiene level of a blood bank information system employee?

RQ5: How to manage the blood donor's availability in a blood bank information system?

This article is organized as follows: Section 1 includes an introduction, motivation, and an outline of the article. Section 2 gives an overview of the current related work that investigates the efforts of other researchers to develop SIBBIS application. Section 3 provides an analysis of the proposed system and determines the system requirements. We provide a table of other related system features compared to existing and innovative features, in addition to the intelligence of the system and functional requirements. We follow the WHO (World Health Organization) guidelines to build our system in this part. Moreover, we provide illustrative design models of the proposed IS application and applied different models such as analysis diagrams and design diagrams.

Table 1: Summary of the key contributions of the related researchers' work.

Reference	***Blood Bank Development Contributions***
[2], [24]	Donors, patients, and hospitals can register into the system, and donors can access information about the various blood banks on the system and blood donation campaigns held by blood banks.
[9], [25]	This system brings voluntary blood donors and patients need blood into the same platform—together with Raspberry Pi to send messages to the corresponding blood donor via GSM modem
[13], [26]	Hospitals can check the availability of blood and send requests for blood to the nearest blood bank or donor matching the blood requirement
[22], [27]	Users can instantly view nearby hospitals and blood banks and hospitals online by tracing their location using GPS. An alert system for severe guiding ambulance to the patient's destination
[23], [28]	The system lists of records donors and blood group information, Ahere contact details will appear in alphabetical order, finds a matching blood type, and reaches the nearby by city/area.

2- Related Work

In this part, we investigate the efforts of other researchers to develop similar nature systems. Recent references were chosen, and a brief comparison was made. Two tables

were provided: one presents a summary of the key contributions of the related researchers's work (Table 1). The other Table prenents the key features of the three systems that we had chosen to present some similar systems to determine their functions and their roles in blood bank information systems.

In [2], [5], the authors aimed to provide a list of donors in the neighboring city/region when an urgent blood transfusion is needed. The user's contact information appears alphabetically on the screen and promptly connects them with a specific or related blood group via the Blood Bank Website. Another project component is an Android-based location-based app that will assist users in accessing blood donors' phone numbers for immediate assistance.

Online Blood Bank System (OBBS) was proposed in [6]. [9]. It provides a central repository for all available blood deposits and the accompanying information. Blood type, location, and storage date are all included in the report. This web-based system allows users to see if their specific category is available in the blood bank. Additional features include patients' names and contact information, booking, and even a requirement for a specific blood group listed on the website to locate willing donors in case of a blood emergency.

The work in [7], [13] granted the administrator access to all donor-related information in the system. The blood donor/recipient can promptly locate blood banks or hospitals matching a specific blood type or group, where they can request specific amounts of blood.

Creating a cloud-based blood bank system is the primary goal for the work of [4] to ensure that those in need have access to blood as quickly as possible, especially during times of emergency. As a part of this initiative, a mobile Android app has been utilized, containing all donor and adjacent hospital information, besides GPS capacity to locate blood banks and hospitals nearby. Health checkup drives, blood donation camps, and other similar facilities will be advertised to all registered users.

In [8], the authors aimed to create cloud storage connecting all blood banks. This cloud should deliver live information about blood supply availability. If there is insufficient blood available, the system will list blood donors' names and contact information belonging to different blood groups.

An automated blood bank system, using Raspberry Pi, was built by [9]. This system was used in the proposed project to send a message to the appropriate blood donor through a GSM modem when the user enters the requisite blood group details, bridging the donor–recipient communication gap via a low-cost and low-power Raspberry Pi kit as a communication bridge.

In [10], [22[, a blood bank mobile application was created that sources a list of blood banks near the user, linking blood banks with potential donors, displaying maps, and tracking locations while also estimating the time to reach the recipient.

In [11], [23], the Ublood System was built, an online blood donation system. It offers a quick and easy way to connect with donors and find nearby organ donors in emergencies like car accidents. A web application and an Android mobile application are both being considered. Table 2 shows the cross-list features with the proposed SIBBIS.

Table 2: Existing and innovation features

Existing features from other researchers' work	***Added innovative features in SIBBIS***
• Create user profile Login • Define-blood banks/hospitals • Submit blood request • Find nearby donors • Send notifications • Search for donors • Map navigation • Blood type matching • Monitor blood storage and validity • Validate-donors availability	• Real-time notification for blood donation • Search for nearby donors • Smart matching process • Control blood donation attempts • Life of hardware checking • Employees' health monitoring in the blood bank

The related work provided an overview of recent developments in this field. It was discovered that improper management between blood banks, blood donors, and hospitals resulted in the waste of available blood inventory. There is a critical need for an efficient, real-time management system for communication and synchronization among the different constituents of the blood system stage players. This serious issue motivated us to plan to create a secured intelligent blood bank information system to ensure that blood is always available in emergencies and that the appropriate donor is available [2].

3- Secure Intelligent Blood Bank Information System (SIBBIS)

SIBBIS is a web-based information system. Its main functions include users (blood donors and blood recipients) who can create their profile, search and find the requested blood type/amount, and request/donate blood. The system's transparency is evident in its tracking tool, enabling users to follow and monitor the process and condition of their requests. Additionally, the

system automatically directs the request to the right user. All records are maintained in a centralized database to ensure fast information retrieval and accuracy. Figure 1 displays a summary of the proposed system features, whether they exist in similar systems or innovation features.

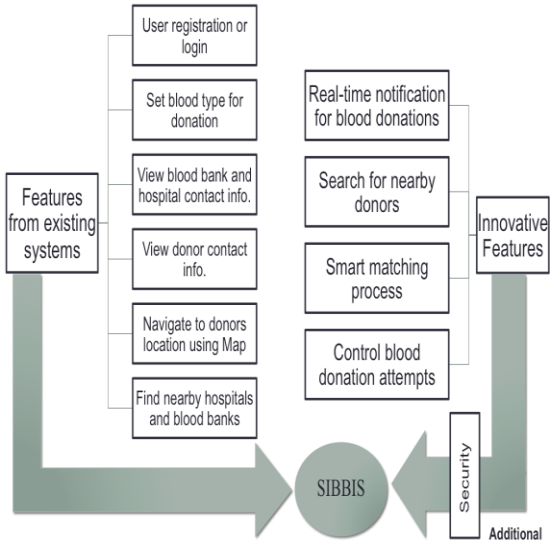


Fig. 1 SIBBIS component contract diagram

3-1- Functional Requirements of SIBBIS

Below is the list of functions that are needed to be support by the proposed SIBBIS system. The proposed SIBBIS system supported innovative features are listed in Table 2 (see above).

1. Users' registration or login
2. Finding nearby hospitals and blood banks
3. Viewing donor's contact information
4. Viewing hospitals and blood banks' contact information
5. Setting blood type for donation
6. Navigating to donor's location using maps

3-2- Comparison with similar Blood Information Management Systems

The purpose of presenting some similar systems is to know their functions and their roles in blood bank information systems. This should facilitate the designing of the SIBBIS in this research, projected to be utilized in the blood banks in Kuwait and other countries.

System-1 [12]: One of the software systems that are used in blood banks is called the Blood Donation Management System, comprising web and mobile applications to help patients and donors communicate. People who want to donate blood must create an account by entering basic information. Google Map is connected with this application to locate a donor's exact location. An appointment is set only after a donor agrees to donate. After that, the system will notify the donor 12 hours before the donation is scheduled to take place.)

System-2 [13]: This is another similar system called Blood Bank Management System. It is a web application enabling registered hospitals to check the availability of requested blood and send blood requests to the nearest blood bank or donor matching the blood criteria. The blood bank could also be found via maps, and the mobile application is only available to donors.

System-3 [2]: CBBR Blood Bank System is another system that stores and manages donated blood that has been collected through a donation or a blood-collecting program. Donors and other recipients, such as patients and hospitals, can register in the Centralized Blood Bank Repository (CBBR). System administrators will have access to critical information like the type of blood available and locating the nearest blood center. A summary of the key features of all the three systems is shown in Table 3. Table 3: Key features of all the three systems [12,13, 2]. The table clearly shows that essential features are still missing in the literature and that more innovative work is needed in the current literature. This, in addition to what we have been through the difficult crisis of COVID-19 urges the need for innovative and intelligent blood management tools in the field. As a result of our research's aspects and studies discussed beforehand, we came out with a list of features that we will incorporate into our application.

A comparison was made between some of the highest-rated blood bank information systems, presenting their features, functions, and differences. Previous systems have deficiencies despite their several features: There is no connection between a blood donor and blood recipients, between hospitals, and hospitals with blood donors. There is no user (blood donor, blood recipient) role in the system, so the staff adds their information to the system manually. Our proposed system will bridge a connection between them to improve the donation process.

Table 3: Key features of all the three systems [12,13, 2]

System's Features	System 1 [12]	System 2 [13]	System 3 [2]
User registration and login	✕	✕	✓
Donors add blood type for donation	✕	✓	✕
Blood seekers search for nearby donors	✓	✕	✕
Finding nearby blood banks and hospitals	✕	✕	✕
Navigating directions through Google map	✕	✓	✓
Smart matching between blood types	✓	✕	✕

4- Secure Blood Bank Information System (SIBBIS)

The proposed SIBBIS aims to acquire, transmit, store, and manage various user-related information and the activities of the health departments that use it. There are various security mechanisms in health information systems to protect data access, collection, transmission, and storage [17]. The security measures in our system help in achieving the following objectives:

- Identify the system's users and their access rights.
- Maintain an operating environment for authorized users and the processing system by protecting the system from different attacks.
- Protect the information in the systems' database and during transmission in internal and external networks.

4-1- Access Controls

Access controls represent a vital security aspect as they limit access to the system's resources to specified users [16]. A health system that enables electronic and remote access sharing of medical data must employ users' identity proofing and authentication procedures before allowing any individual to perform activities, securing the system's safeguards against unauthorized users and operations. Our system has multiple user groups, and each of them will use the system to perform predefined roles. Therefore, it is essential to correctly identify users before assigning them a role in the system. In the following, we elaborate on our system's security mechanisms:

4-1-1- User Identification

Identifying the users that our system is targeting is the first step in the development of access controls [15]. In the case of the proposed SIBBIS, our targets are the following:

- System Administrator: A person who manages the operation of a computer system
- Blood Donor: A person who is willing to donate blood
- Blood Recipient: A person who is seeking blood
- Staff: A person who works in blood banks or hospitals
- After identifying the system's users, we start the process of developing the access controls to prohibit users from accessing unnecessary resources.

4-1-2- User Registration

To access the system, users must complete the registration process by providing their identification information. To correctly identify new users' registration requests, the system requests them to provide the following credentials:

- Soft copy of a government-issued ID
- Demographic information including first and last names, birth date, nationality, gender, marital status, phone number, current address, and email address
- Indication of the group they belong to (blood donor, blood recipient, system administrator, staff)
- For blood recipient: provide information about blood type and medical history
- For staff: Provide information about specialty, certifications, years of experience, department, and location.

4-1-3- Identity Proofing

After receiving a complete registration request, the system checks the new account requests against existing ones to avoid duplications. After that, the

system administrators complete processing requests by:

- Verifying valid IDs
- Verifying that submitted demographics are valid and accurate

- Verifying that healthcare providers' documents are certified and valid
- Verifying eligible requests and notifying the system

4-1-4- User Authentication

After proofing eligible users' identities, the system generates users' IDs. The system requests said users to provide authentication information, which is a critical process as it verifies that a user is correctly identified and that a user can access the system and is eligible to perform specific functions [16]. Having a secure and efficient authentication secures the system. A user will not be able to access the system without using a valid authentication factor assigned by the system or chosen by them. Identity authentication is done by using one or more of these factors:

- Something you know, such as password, PIN, and secret answers
- Something you have, such as ID cards, mobile device, or a cryptographic key
- Something you are, such as a piece of biometric data.

Choosing a strong authentication factor is necessary for preventing unauthorized access attempts to information systems [15]. Most security breaches occur due to weak or stolen authentication information, leading to the leak of sensitive information and, in turn, leading to huge financial costs [16]. In our system, we have incorporated a Two-Factor Authentication process (2FA) to overcome the risks associated with using a single factor. Through a 2FA system, users must provide two authentication factors to access the system, thus, significantly reducing phishing attacks by adding an extra protection layer to the system. For our system, we have chosen an efficient and friendly 2FA

method. The first authentication factor is the most common factor, which is the password. For the second authentication factor, the authentication manager in our system will generate a One-Time Password (OTP) to authenticate users further. The user can receive the OTP via SMS or email. The generated password will be valid for one time only:

- Create a password.
- Choose the method of the second authentication step (SMS, email).
- Fill up the required information.
- Confirm the request.

When a user attempts to access the system, the system starts by checking the inserted ID in the user's database. If the ID exists, the system retrieves the corresponding password in a decrypted form. Next, the user is requested to insert their password. The provided password will be compared against the retrieved password. If the entered password is correct, the system generates the OTP code and sends it to the desired user method for the second authentication step. The user receives the code and inserts it to access the system.

4-1-5- Access Control List

Authenticating eligible users alone is not enough to protect information systems. Internal users can cause threats to the system by exploiting the system's resources for illegal acts [15]. Therefore, it is crucial to define the system's access controls. The users of the system and subjects perform different actions on the system's objects. These objects of a system include files, hardware devices, network connections, and processes. Depending on the user role and the object, we define the access mode. Access modes include, but are not limited to, read, write, delete, create, and modify. Creating an access control list is the most convenient method of preventing subjects from performing unauthorized activities [16]. With this list, unwanted access will be immediately denied. Groups must be assigned roles that apply the following standards:

- Roles are designed and implemented based on the principle of least privileged.
- Permissions are to be defined based on role authority and responsibilities within a job function.
- A user account is assigned to a role that allows it to perform only what is required for that role.
- A user can only access an object based on an assigned role.
- The object is only to be concerned with the user's role and not the user.

The access rights lists define the access rights to the system's resources allowed or denied for authorized users [15]. When a user attempts to access any resource, the system checks this list to determine the
user's type. The accesses provided for users are as follows:

- Create: The user can create new entities and upload folders into the system.
- Delete: The user can delete entities and folders in the system.
- Read: The user can view the entities and folders in the system.

- Write: The user can edit and modify the contents of entities and folders in the system.

When an authenticated user provides the correct authentication mean (ID, password, and OTP), the system grants the user access to the system resources. However, there is no full access to the system's resources for all users. The system checks the permission level of each user by checking the access rights list and then grants the appropriate access to each user.

4-2- Data Security Mechanism

The sensitive data incorporated in our system is projected to be diverse. The attractive nature of the health information system makes it more exposed to threats like eavesdropping, forgery, and manipulation [14]. These threats could lead to huge damages and, in some cases, life threats. If attackers gain access to health systems, they might modify the stored data or change the system's configuration. This would lead to threatening the lives of patients and low-quality services causing financial losses. Hence, it is important to consider the system's information security when stored in the database and when it is in the transmission phases.

4-2-1 Database Security

Storing tremendous amounts of data in a central database server bears many threats and risks that must be considered [19]. The system's database must be sufficiently protected. In addition to access controls, we incorporate other mechanisms to increase the system's security significantly. Via encryption, we prevent interceptors or intruders from accessing the plaintext form of data in the system's databases. Additionally, authorized users will be prevented from accessing unauthorized resources through the application of cryptography architectures to the stored data is a primary method to keep the database secure. In cryptography, data would be altered to a format that unauthorized users cannot view. Using it is very effective in protecting files and sensitive data in the database. The database of our system will be encrypted using different sets of rules that would be defined in the system's configuration phase [18].

4-2-2- Backup and Recovery

Planning for database backup and recovery are adequate safeguards against data loss and software errors. It is an important security measure to protect the system's data against crashes and network and disk failures. With it, the process of reconstructing the system's database would be faster and easier. Therefore, making copies and archives of the system's data and processes is crucial for a successful backup [17].

The transaction logging technique would be incorporated into our database server to back up the system. With it, we keep track of the updates to the system's database. Modifications on the stored data are recorded with the details of who, when, and how the update was performed. By this, we create an audit trail of all updates to the database that can trace any error or suspicious activity. This technique is important in safeguarding the system's security by keeping evidence of the source of changes. Hence detecting unauthorized actions that authorized users could conduct. Moreover, this logging can assist in detecting the source of error if there is a failure in the system or a part of it.

4-2-3 Data Transmission Security

In our proposed blood bank information system, data would travel, whether via wired or wireless means, between the different components of our system and to other health systems, if necessary.
Along with the transmission medium, unauthorized users can intercept this data. Data in transmission levels targets attract many threats such as spying, altering information, interrupting communication, sending extra signals to block the base station, and networking traffic. As in database security, the most effective solution is to encrypt information during transmission to preserve confidentiality [20, 21]. The transmission of some of the system's data is over insecure public networks, such as the Internet. Therefore, encryption would be necessary to ensure confidentiality. This involves the use of algorithms and secret keys. Many protocols, such as Internet Protocol Security (IPsec), Transport Layer Security (TLS), and Secure Socket Layer (SSL), have been proposed to achieve protected communication data over insecure channels. In the system implementation phase, we will select the most appropriate protocol to achieve the system's security needs.

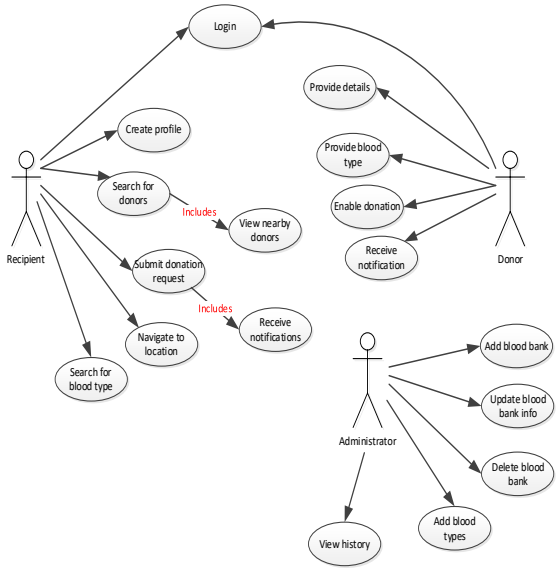


Fig..2 SIBBIS use case diagram

5- The Intelligence of the SIBBIS

- The following are the intelligent features supported by SIBBIS:
- Real-time notification for blood donation
- Searching for nearby donors
- Smart matching process
- Controlling blood donation attempts
- Life of hardware checking
- Employees' health monitoring in the blood bank (Blood banks and hospitals are required to ensure all employees have the needed certification (such as a COVID-19 vaccination certificate), and that safety and hygiene are always considered.
- Our proposed system asked staff members to upload the COVID-19 vaccine certification or a PCR test that ensures they are not infected as an alternative. In addition, medical history was required.

6- Analysis and Design Models of SIBBIS

In this section, we provide illustrative analysis and design models of the proposed system. Analysis diagrams include use case, sequence diagrams, activity diagram, entity relationship diagrams (ERD), and class diagrams. However, in this article, we will explain only the use case diagram, general activity diagram, and sequence diagrams.

6-1-Use Case Diagram

The use case diagram of the SIBBIS is shown in Figure 2. We have focused on the main actors of our system, which are users and system administrators. On the other hand, we have one database responsible for storing all the data. The use case diagram identifies how users interact with the system.

6-2- Activity Diagram of SIBBIS

As shown in Figure 3, the user starts by logging in to the system, then verifies the existence of the user in the system. Based on the success of the verification, the user will then be able to navigate proposed features such as creating a request for blood type, searching for donors, and navigating to the location through the map and finally through system usage.

6-3-Sequence Diagrams of SIBBIS

Figure 4 illustrates the sequence diagram of, which explains how objects and predefined actors are functioning starting from login as a base function to system usage until interacting with the backend to implement the required function.

6-4-ER Diagram of SIBBIS

In Figure 5, an entity–relationship diagram demonstrates the correlations between system objects or components. The ER model is composed of entity types and specifies relationships that can exist between these system-related entities. Some of these relations are described as one-to-one, many-to-many, and many-to-one. The system comprises seven entities: donors, donors' history, donation requests, recipients, recipients' history, blood centers or banks, and, finally, the map location details.

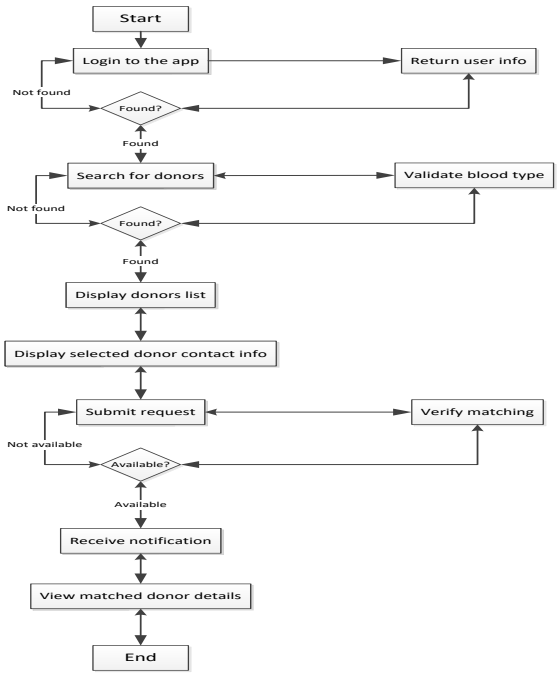


Fig. 3 General activity diagram

6-5-Class Diagram of SIBBIS

The class diagram is a type of static diagram that describes the structure of the system by visually representing the main classes defined in the system, objects, related attributes, and the relationships between these objects. As shown in Figure 6, the

application includes mainly five objects: donors, which includes information about the donors, this object is correlated to the object of location which includes the information about the location of each donor, which is also correlated with the object blood bank that includes the information of blood banks and
their locations, and, finally, the recipient object, which includes the basic information of users projected to receive blood donations. As evident, the recipient object has no direct relationships with any other objects since they can search for donors and request blood donations, which can be implemented in the application without the need to build a backend relationship.

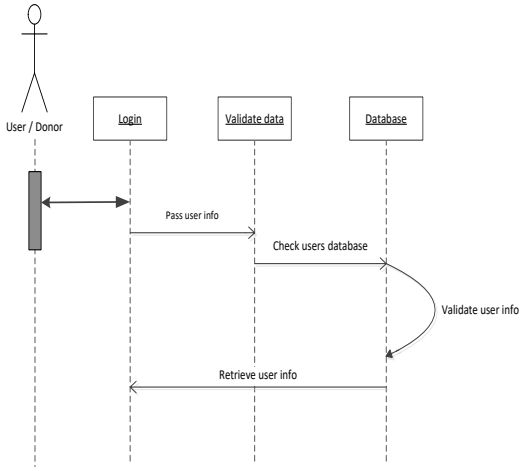


Fig. 4 Sequence diagram

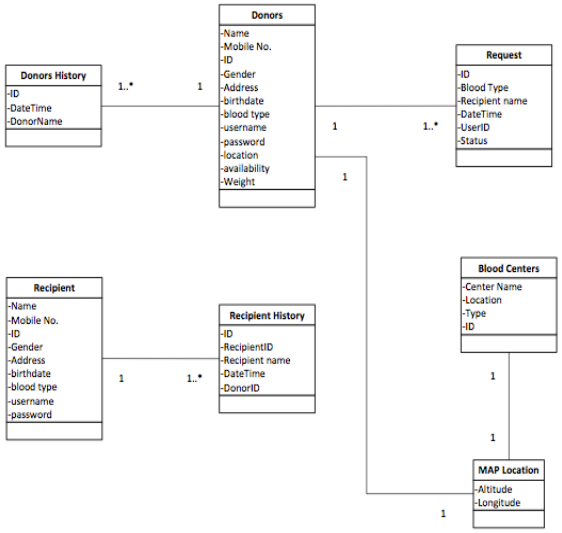


Fig. 5 Entity Relationship diagram

7- Implementation

This section is dedicated to explaining the proposed system user interface and SIBBIS usability evaluation.

7-1 Build System Screenshots

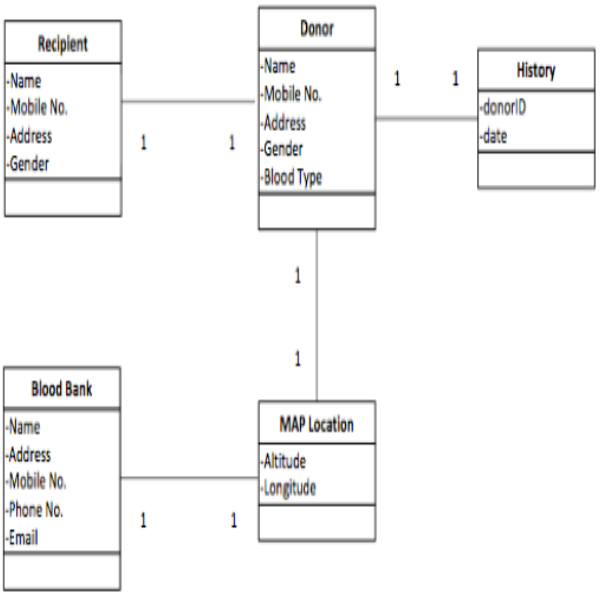
The screenshots of the developed SIBBIS are shown in Figures 8–17.

8- SIBBIS Usability Evaluation

To evaluate the usability of the developed system, we conducted a survey using the Computer System Usability Questionnaire (CSUQ), consisting of 19 questions

randomly distributed among 50 users. The user used the developed system and recorded their evaluation on the question paper. The user evaluates the system usability by answering the following items:

1. Overall, I am satisfied with how easy it is to use this system.



2. It was simple to use this system.
3. I can effectively complete my work using this system.
4. I am able to complete my work quickly using this system.
5. I am able to efficiently complete my work using this system.
6. I feel comfortable using this system.
7. It was easy to learn to use this system.
8. I believe I became productive quickly using this system.
9. The system gives error messages that clearly tell me how to fix problems.
10. Whenever I make a mistake using the system, I recover easily and quickly.
11. The information (such as online help, on-screen messages, and other documentation) provided with this system is clear.
12. It is easy to find the information I needed.
13. The information provided for the system is easy to understand.
14. The information is effective in helping me complete the tasks and scenarios.
15. The organization of information on the system screens is clear.
16. The interface of this system is pleasant.
17. I like using the interface of this system.
18. This system has all the functions and capabilities I expect it to have.
19. Overall, I am satisfied with this system.

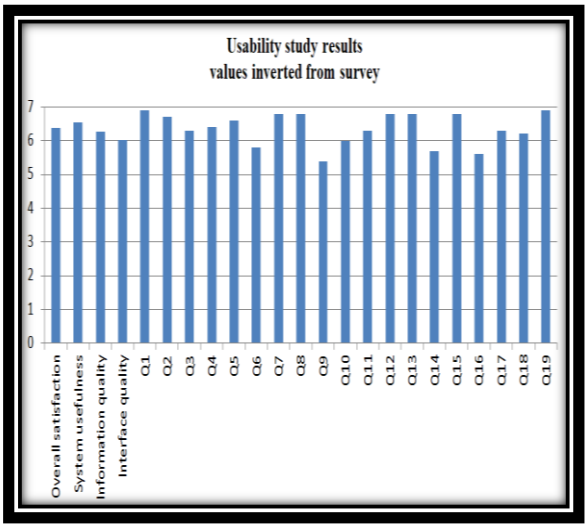


Fig. 6 Class Diagram

Fig. 7 CSUQ Results

Figure 7 shows the scores for general categories, together with the averages for all of the questions. While the study concluded that SIBBIS software recipients in the whole country by 93.39% (93.3%)

Fig. 8 Main page

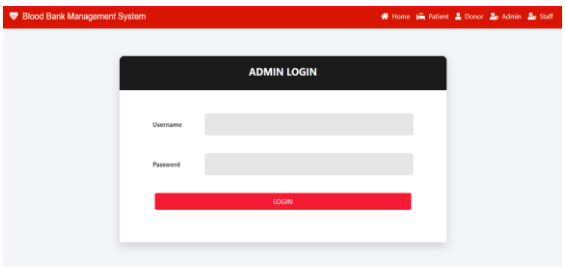


Fig. 9 Admin login page

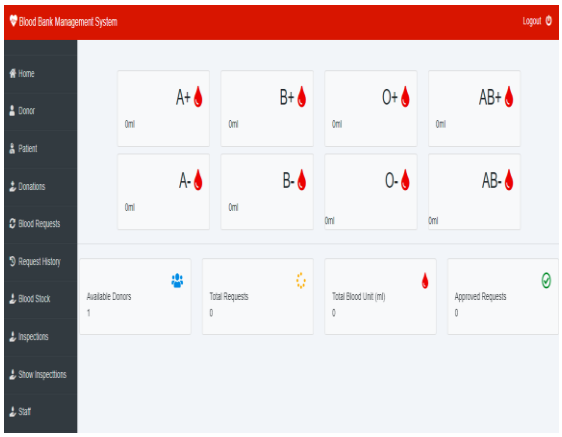


Fig. 10 Admin main page.

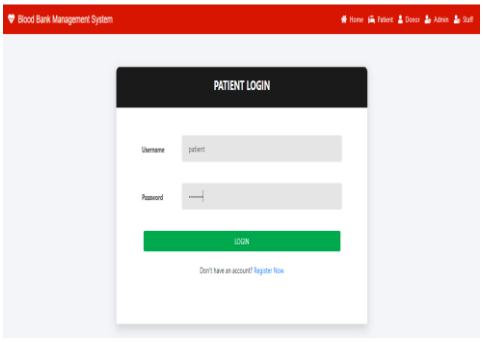


Fig.11 Patient login page.

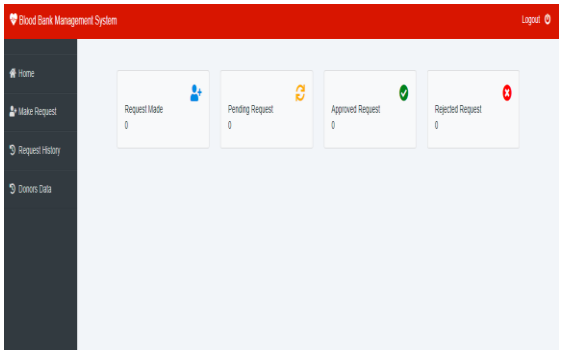


Fig. 12 Patient main page.

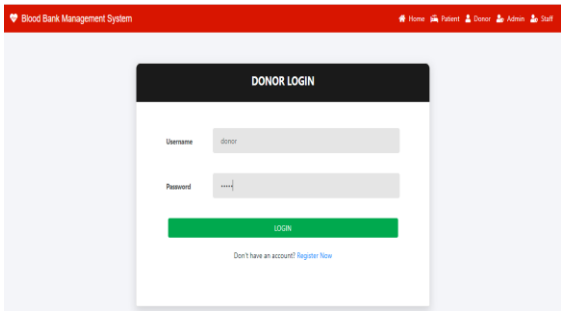


Fig. 13 Donor login page.

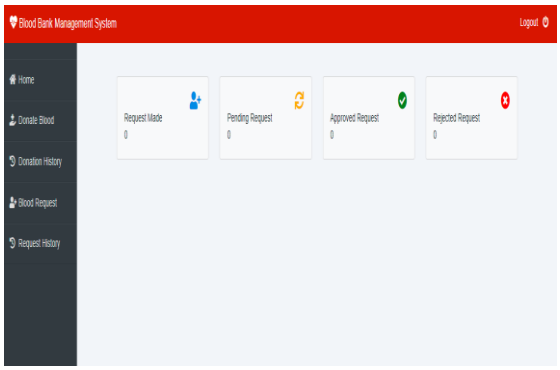


Fig.14. Donor main page

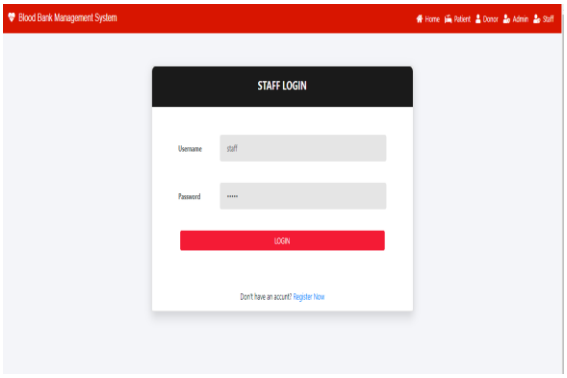


Fig.15 Staff login page

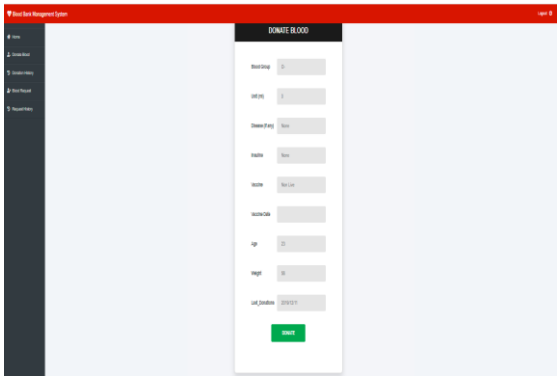


Fig. 16. Donor donating blood

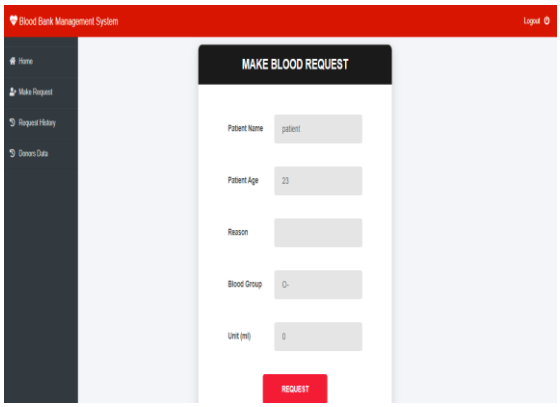


Fig. 17 Patient requesting blood

9- Conclusion

In conclusion, technology plays a vital part in improving the wellness and quality of life of people. This article presents the design and analysis of a standard process-oriented information System analysis methodology using use case, activity, system sequence, entity relationship, and class diagrams. SIBBIS is developed under the guidelines of the WHO. The proposed system is intelligent in terms of the real-time notification for blood donation, search for nearby donors, smart matching process, control of blood donation attempts, life of hardware checking, and employees' health monitoring in the blood bank. The system is an attempt to complement and add up what is missing in the current literature in terms of innovation and intelligence. The system was tested, and its usability was 93%. In addition, the system will be beneficial for blood banks, hospitals, clinics, and blood donors and blood seekers (patients). In the future, we have a plan to add more functions for the users and also make the system more intelligent and secure.

References

[1] Advisera Expert Solutions Ltd., "How to Implement NIST Cybersecurity Framework using ISO 27001", 2017, [Online] Available:http://www.infomania-services.fr/controle/file/181206101951000000_5892133709_1544091591.pdf

[2] Akar, I. F., Mohammad, T. A., & Ismail, M. "CBBR Centralized Blood Bank Repository", ResearchGate. Retrieved November 9, 2021, from https://www.researchgate.net/publication/319372139_CBBR_Centralized_Blood_Bank_Repository

[3] Ramachandran, P. Girija, N., Bhuvaneswari, T.,"Classification Blood Donors Using Data Mining Techniques", International Journal of Computer Science and Engineering, Vol.1, Issue 1, 2011, pp.10-13.

[4] Chaudhari, S., Walekar, S., Ruparel, K., and Pandagale, V., "A Secure Cloud Computing Based Framework for the Blood bank", International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 2018, pp. 1-7.

[5] Madan, T., Bharwai, N., Kumar, N., "Blood Donation Management with Modern Engineering", International Computational Engineering and Networking, 2016, vol. 9(8), pp.27-31.

[6] Chetan Masram, Arshad Mulani, Rasika Bhitale, Jidnesh Koli, "Online Blood Bank Management System", International Research Journal of Engineering and Technology, Vol. 8, issue 06, 2021, pp.4220-4226

[7] S Periyanagi, A Manikandan, M Muthukrishnan, M Ramakrishnan, "Bdoor App-Bood Donation Application using Android Studio", Journal of Physics: Conference Series, 2021, pp.1-12.

[8] AL-Kalbani, S. I. A. Kazmi and J. Pandey, "IoT Based Smart Network for Blood Bank," 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2018, pp. 732-736.

[9] A. C. Adsul, V. K. Bhosale and R. M. Autee, "Automated blood bank system using Raspberry PI," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2018, pp. 252-255.

[10] Fathima, M., A. Valarmathi, " Blood Bank Mobile Application", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 2, issue 2, 2017, pp. 1126-1130.

[11] Chawla, S., Dalal, T. "UBlood: Utilize every cell of Blood- A Proposed Mobile based Application Framework", International Journal of Computer Science and Information Technologies, Vol, 8(2), 2017, pp.292-294.

[12] Akkas Ali, K. M., Jahan, I., Islam, A., & Parvez, "Blood Donation Management System", American Journal of Engineering Research (AJER), 2015, Vol4(6), pp.123-136. [13] Raut, P., Parab, P., Suthar, Y., Narwani, S., & Pandey, "Blood Bank Management System", International Journal of Advance

[14] Appari, Ajit, Johnson, "Information Security and Privacy in Healthcare: Current State of Research", International Journal of Internet and Enterprise Management, 2020, Vol. 6. Pp.279-314.

[15] Athanase Nkunzimana, Boiko, Andrii & Shendryk, Vira, "System Integration and Security of Information Systems", Procedia Computer Science, 2017, Vol.104. pp.35-42.

[16] Boriev, Z & Sokolov, S & Nyrkov, "Review of modern biometric user authentication and their development prospects", IOP Conference Series Materials Science and Engineering. 2015, Vol. 91, pp.1-12.

[17] Leila Rikhtechi, Vahid Rafe, Afshin Rezakhani, "Secure Access Control in Security Information and Event Management System", Journal of Information Systems and Telecommunication, 2021, pp. 67-78.

[18] Pattanashetti, M. A., & Pilli, G. S, "Novel Transfusion parameters in Blood bank for Thalassemia patients", Indian

Journal of Pathology and Onco-logy, 2017, vol. 4(4), pp.396-399.

[19] M. Puppala, T. He, X. Yu, S. Chen, R. Ogunti and S. T. C. Wong, "Data security and privacy management in healthcare applications and clinical data warehouse environment," IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI), Las Vegas, NV, USA, 2016, pp. 5-8

[20] Zukime, M. & Mat Junoh, Mohd Zukime & Osman, Abdullah & Ab. Halim, M. Suberi & Halim, Ab & Safizal Abdullah, M.. Data Security: Issues And Challenges for Disaster Management In The New Millennium. International Journal of Scientific & Technology Research. 2014, 3.8.2277-8612.

[21] Siddiq Iqbal, Sujatha B. R, "Secure Key Management Scheme for Hierarchical Network Using Combinatorial Design", Journal of Information Systems and Telecommunication, Vol. 10, No.1, January-March 2022, pp. 20-27.

[22] Ashita Jain, Amit Nirmal, Nitish Sapre, Prof Shubhada Mone, "Online Blood Bank Management System using Android", International Journal of Innovative Studies in Sciences and Engineering Technology, Volume: 2 Issue: 2, 2016, pp.55-58.

[23] Mohit, "Review on Blood Bank Management Systems", International Research Journal of Modernization in Engineering Technology and Science, Volume:03/Issue: 04/April-2021, pp. 172-174.

[24] Ben Elmir, W., Allaoua Hemmak, A., and Senouci, B.,Smart Platform for Data Blood Bank Management: Forecasting Demand in Blood Supply Chain Using Machine Learning", Information January 2023, 14(1):1-31. https://doi.org/10.3390/info14010031

[25] Sri A., Pravallika, M. Kumar, O., Sridevi, K., Balaji, K., "A Systematic Review on Blood Bank Information Systems", International Journal of Scientific Research & Engineering Trends, Volume 10, Issue 2, Mar-Apr-2024, ISSN (Online): 2395-566X. https://doi.org/10.22214/ijraset.2023.49843

[26] Varghese A., Thilak, K., Saritha., M., "Technological advancements, digital transformation, and future trends in blood transfusion services", International Journal of Advances in Medicine, March-April 2024, Vol 11, Issue 2, pp. 147-152.

[27] Ghouri AM, Khan HR, Mani V, Ul Haq MA, De Sousa, ABL., "An Artificial-Intelligence-Based Omnichannel Blood Supply Chain., 2023;1-58. DOI:10.22214/ijraset.2023.49843

[28] Mohammed R., Al-zebari, A., "Proposed A Web-Based Intelligent System to Manage the Blood Bank in Zakho District, Vol 8 No.3, June 2023, PP. 1267-1284. DOI:10.25212/lfu.qzj.8.5.46