HARNESSING VARICOSE VEINS USING IMAGE PROCESSING VIA CRYPTOGRAPHY

A PROJECT REPORT

Submitted by

GOPIKA G

KAVIYARASI S

KEERTHIGA B

LATCHAYA G

in partial fulfilment for the award of the degree

Of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

K. RAMAKRISHNAN COLLEGE OF TECHNOLOGY

(An Autonomous Institution, affiliated to Anna University Chennai and Approved by AICTE, New Delhi)

SAMAYAPURAM – 621 112

MAY 2024

HARNESSING VARICOSE VEINS USING IMAGE PROCESSING VIA CRYPTOGRAPHY

A PROJECT REPORT

Submitted by

GOPIKA G	**(811720104029)**
KAVIYARASI S	**(811720104048)**
KEERTHIGA B	**(811720104050)**
LATCHAYA G	**(811720104054)**

in partial fulfilment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

K. RAMAKRISHNAN COLLEGE OF TECHNOLOGY

(An Autonomous Institution, affiliated to Anna University Chennai and Approved by AICTE, New Delhi)

SAMAYAPURAM – 621 112

MAY 2024

K. RAMAKRISHNAN COLLEGE OF TECHNOLOGY

(AUTONOMOUS)
SAMAYAPURAM – 621 112

BONAFIDE CERTIFICATE

Certified that this project report titled **"HARNESSING VARICOSE VEINS USING IMAGE PROCESSING VIA CRYPTOGRAPHY"** is the bonafide work of **GOPIKA G (811720104029), KAVIYARASI S (811720104048), KEERTHIGA B (811720104050)** and **LATCHAYA G (811720104054),** who carried out the project under my supervision. Certified further, that to the best of my knowledge the work reported here does not form part of any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE

Dr. A.DELPHIN CAROLINA RANI,M.E, Ph.D.,

HEAD OF THE DEPARTMENT

PROFESSOR

Department of CSE

K. Ramakrishnan College of Technology

(Autonomous)

Samayapuram – 621 112

SIGNATURE

Mr. R.RAJAVARMAN, M.E, (Ph.D)..,

SUPERVISOR

ASSISTANT PROFESSOR

Department of CSE

K. Ramakrishnan College of Technology

(Autonomous)

Samayapuram – 621 112

Submitted for the viva-voce examination held on ……

INTERNAL EXAMINER **EXTERNAL EXAMINER**

DECLARATION

We jointly declare that the project report on **"HARNESSING VARICOSE VEINS USING IMAGE PROCESSING VIA CRYPTOGRAPHY"** is the result of original work done by us and best of our knowledge, similar work has not been submitted to **"ANNA UNIVERSITY CHENNAI"** for the requirement of Degree of **BACHELOR OF ENGINEERING**. This project report is submitted on the partial fulfilment of the requirement of the award of Degree of **BACHELOR OF ENGINEERING**.

Signature

_____

GOPIKA G

_____

KAVIYARASI S

_____

KEERTHIGA B

_____

LATCHAYA G

Place: Samayapuram

Date:

ACKNOWLEDGEMENT

It is with great pride that we express our gratitude and in-debt to our institution "**K.Ramakrishnan College of Technology (Autonomous)**", for providing us with the opportunity to do this project.

We are glad to credit honourable chairman **Dr. K.RAMAKRISHNAN**, **B.E.,** for having provided for the facilities during the course of our study in college.

We would like to express our sincere thanks to our beloved Executive Director **Dr. S. KUPPUSAMY, MBA, Ph.D.,** for forwarding to our project and offering adequate duration in completing our project.

We would like to thank **Dr. N. VASUDEVAN, M.E., Ph.D.,** Principal, who gave opportunity to frame the project the full satisfaction.

We whole heartily thanks to **Dr. A. DELPHIN CAROLINA RANI M.E., Ph.D.,** Head of the department, **COMPUTER SCIENCE AND ENGINEERING** for providing her encourage pursuing this project.

I express my deep and sincere gratitude to my project guide **Mr.R.RAJAVARMAN M.E,(Ph.D).,** department of **COMPUTER SCIENCE AND ENGINEERING** for his incalculable suggestions, creativity, assistance and patience which motivated me to carry out this project.

I render my sincere thanks to Course Coordinator and other staff members for providing valuable information during the course.

I wish to express my special thanks to the officials and Lab Technicians of our departments who rendered their help during the period of the work progress.

ABSTRACT

The introduction of digital technology has completely changed medical imaging and diagnosis, providing more accurate and efficient ways to identify a wide range of illnesses. Because medical photographs include sensitive patient data, security is the most important concern when it comes to their transmission. When digitized photographs and the pertinent patient data they contain are transferred over public networks, medical image security is a crucial technique for protecting sensitive data. Sensitive photos contain a wealth of significant information and distinct qualities from those of regular photos. Compared to other digital photographs, medical images include far more critical and sensitive data. The diagnosis procedure may need every pixel in the image, and any distortion may lead to an inaccurate diagnosis. Even the strongest security for these photos has such minimal impact on the image that it may be disregarded. The difference between this and insensitive pictures is how thin the redundancy is. Medical images' embedding capability is inadequate. Researchers in the field now provide diverse data. Data verification is ensured by security measures including data concealing and encryption. However, in medical imaging applications, these methods are less secure and require more time. Therefore, use convolutional neural network methods with fragmented based elliptical curve encryption in this research to create a safe illness diagnostic system for medical photos.

Table of Contents

LIST OF FIGURES

LIST OF ABBREVIATIONS

CNN	-	CONVOLUTIONAL NEURAL NETWORK
ECC	-	ELLIPTIC CURVE CRYPTOGRAPHY
LSB	-	LEAST SIGNIFICANT BIT
EHR	-	ELECTRONIC HEALTH RECORDS
SS	-	SECRET SHARING
DES	-	DATA ENCRYPTION STANDARD
AES	-	ADVANCED ENCRYPTION STANDARD
VC	-	VISUAL CRYPTOGRAPHY
HIPAA	-	HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT
GDPR	-	GENERAL DATA PROTECTION REGULATIONS
GPL	-	GENERAL PUBLIC LICENSE
UML	-	UNIFIED MODELLING LANGUAGE

CHAPTER 1

INTRODUCTION

1.1 MEDICAL IMAGE IN CLOUD

Varicose veins are a serious health risk that require a precise diagnosis and course of therapy. This work suggests a novel approach that uses encryption and image processing to improve diagnostics and protect patient data. The scanned varicose vein pictures are pre-processed using Convolutional Neural Network (CNN) multi-layer methods, and then features are extracted and illness prediction is achieved using classification techniques. Steganography techniques are used to strengthen data security. Elliptic Curve Cryptography (ECC) and Least Significant Bit (LSB) algorithms are utilized to divide and fragment steno images. The accuracy of diagnosis and the privacy of medical information pertaining to patients with varicose veins are both expected to be revolutionized by this integrated approach.

1.1.1. BACKGROUND

Venous insufficiency and malfunctioning valves cause blood to pool and swell in veins, which is the cause of varicose veins, a common vascular disorder. Correctly identifying varicose veins is still a challenging process, even with their ubiquitous presence. Physical examination, ultrasonography, and venography are examples of conventional diagnostic techniques, all of which have consistency issues and potential subjectivity. To protect sensitive medical data, strong encryption and authentication methods are required as a result of the growth of electronic health records (EHRs), which has prompted concerns about data privacy and security of medical diagnostics has undergone a revolution because to recent advances in image processing, especially in deep learning. Deep learning algorithms of the Convolutional Neural Networks (CNN) class are highly efficient at identifying complex patterns and features in pictures, providing unmatched precision for tasks related to image segmentation and classification. Early diagnosis and treatment of varicose veins are made possible by researchers' unparalleled precision in medical image analysis made possible by CNNs.

The discipline of secure communication known as cryptography offers vital resources for safeguarding private information in healthcare systems. One subfield of cryptography called steganography provides a covert method of data transmission by allowing information to be hidden inside digital material.

1.1.2. PROBLEM STATEMENT

Currently, the diagnosis of varicose veins is made using subjective interpretation and non-standardized approaches, which leads to diagnostic mistakes and delays treatment. The increased dependence on electronic health records raises further concerns about the security and privacy of patient data, particularly imaging data. A comprehensive framework combining encryption and advanced image processing techniques is required to solve these challenges and improve diagnosis accuracy while safeguarding patient data. Enhancements to the framework are required to speed up diagnosis, automate image analysis, minimize privacy concerns in healthcare systems, and enhance encryption techniques.

1.2 IMAGE PROCESSING IN HEALTHCARE SYSTEM

In the health care system, there has been a dramatic increase in demand for medical image services, e.g. Radiography, endoscopy, Computed Tomography (CT), Mammography Images (MG), Ultrasound images, Magnetic Resonance Imaging (MRI), Magnetic Resonance Angiography (MRA), Nuclear medicine imaging, Positron Emission Tomography (PET) and pathological tests. Besides, medical images can often be challenging to analyze and time-consuming process due to the shortage of radiologists.

Artificial Intelligence (AI) can address these problems. Machine Learning (ML) is an application of AI that can be able to function without being specifically programmed, that learn from data and make predictions or decisions based on past data. ML uses three learning approaches, namely, supervised learning, unsupervised learning, and semi-supervised learning. The ML techniques include the extraction of features and the selection of suitable features for a specific problem requires a domain expert. Deep learning (DL) techniques solve the problem of feature selection. DL is one part of ML, and DL can automatically extract essential features from raw input data. The concept of DL algorithms was introduced from cognitive and information theories. In general, DL has two properties: (1) multiple processing layers that can learn distinct features of data through multiple levels of abstraction, and (2) unsupervised or supervised learning of feature presentations on each layer.

The machine learning algorithm performs a series of pre-processing operations on the initially obtained data and then extracts part of the data from the data generated after the pre-processing program is completed according to the opinions of experts. At the same time,

select appropriate data from the data set as the characteristics of the image. After completing a series of operations, the image modelling work is completed by a specific function.

(1) Disease diagnosis - In the field of medical diagnosis and treatment, medical diagnosis is one of the most common medical activities. Medical disease diagnosis also provides a large amount of analytical data for machine learning, which provides conditions for machine learning in the field of medical diagnosis. Machine learning obtains certain data results by sorting out and analysing a large amount of medical data. Then, a disease diagnosis model is established through machine learning methods, which can provide medical diagnosis assistance to medical diagnosticians.

(2) Medical image processing - As the work of medical institutions becomes more and more difficult, many diseases cannot be diagnosed by traditional clinical solutions, and can only be judged by CT, RI, and other means, resulting in a large number of medical images. However, under current conditions, a large number of medical workers can only analyze these medical images themselves. As medical staff have too much subjective initiative such as medical quality, knowledge level, and personal ability, it is easy to lead to misunderstanding of medical images, resulting in some wrong diagnosis results. Image processing technology based on machine learning provides a way to effectively avoid the influence of human factors and improve the accuracy of image content interpretation.

1.3 MULTI SECRET SHARING

A secret sharing (SS) scheme is a cryptosystem that encrypts a secret into multiple pieces called shares so that only qualified sets of shares can be employed to reconstruct the secret. Therefore the SS scheme is one of the most fundamental technologies to realize secure access control. A typical example of secret sharing schemes is a (k, n)-threshold secret sharing scheme. In (k, n)-threshold secret sharing schemes, a secret is encrypted into n shares in such a way that any k or more shares can be employed to reconstruct the secret, while no $k - 1$ or less shares leak any information about the secret. In the ordinary secret sharing schemes, secrets and shares are both numerical data and their encryption and decryption is performed by computers. In contrast, there exist secret sharing schemes whose decryption do not require any numerical computations but can be performed by a human. A visual secret sharing (VSS) scheme is an example of such secret sharing schemes. In VSS schemes, secrets and shares are both visual data such as printed texts, hand written notes, pictures and so on. The schemes encrypt a visual secret into visual shares so that humans can recover the visual

secret with their eyes by superposing a qualified set of visual shares printed on transparencies.

Data exchanged over the Internet is in the form of images, audio, video, text, handwritten text, graphic objects, animations etc... The media used in data exchange is unreliable and insecure. Security of the digital media has become an important topic as it can be copied and modified easily. Cryptography is one of the techniques, which can be used for security of exchanged data. It ciphers the plain text to make it as cipher text, which is actually communicated through the communication media so that intruders even if obtain the cipher text do not be able to decipher the original information hidden within the cipher text. The examples of cryptography are Data Encryption Standard (DES), triple DES (3DES), Advanced Encryption Standard (AES), and Blowfish in which encryption and decryption are done by same key. RSA is another popular algorithm for asymmetric cryptography in which encryption and decryption are done using different keys. Images are a vital form of multimedia contents, which are extensively exchanged over the Internet. So, there should be a secure and simple way to exchange images through any unsecured medium. In order to protect the image contents, Visual Cryptography (VC) is proposed. Using VC, a user can identify confidential data without any computation. In (k, n)-VCT, n shares (shadow images) of the secret image are generated during encryption and are sent through any untrusted medium.

Out of n shares, any k shares are just stacked/superimposed (logical OR operation or AND operation depending upon which colour is considered which bit) at the recipient's side to get the original secret image back. Any less than k shares would not regenerate the original secret image. The advantage of VCT over other crypto graphical techniques used for other multimedia content like text, audio, video is its decryption process, which does not involve any complex calculations and computations but can only be done by Human Visual System (HVS) i.e. human eye. Furthermore, no key is required for encryption/decryption in VCT as in other cryptographic techniques. The two main aspects of the VCT are contrast and security.

1.4 CRYPTOGRAPHY

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.
While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.
Cryptology embraces both cryptography and cryptanalysis.

Cryptography is used in many applications like banking transactions cards, computer passwords, and e- commerce transactions.
Three types of cryptographic techniques used in general.
1. Symmetric-key cryptography
2. Hash functions.
3. Public-key cryptography

1.4.1 SYMMETRIC-KEY CRYPTOGRAPHY

Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text. With symmetric cryptography, the same key is used for both encryption and decryption. A sender and a recipient must already have a shared key that is known to both. Key distribution is a tricky problem and was the impetus for developing asymmetric cryptography. With asymmetric crypto, two different keys are used for encryption and decryption. Every user in an asymmetric cryptosystem has both a public key and a private key. The private key is kept secret at all times, but the public key may be freely distributed.

Data encrypted with a public key may only be decrypted with the corresponding private key. So, sending a message to John requires encrypting that message with John's public key. Only John can decrypt the message, as only John has his private key. Any data encrypted with a private key can only be decrypted with the corresponding public key. Similarly, Jane could digitally sign a message with her private key, and anyone with Jane's public key could decrypt the signed message and verify that it was in fact Jane who sent it.

Symmetric is generally very fast and ideal for encrypting large amounts of data (e.g., an entire disk partition or database). Asymmetric is much slower and can only encrypt pieces of data that are smaller than the key size (typically 2048 bits or smaller). Thus, asymmetric crypto is generally used to encrypt symmetric encryption keys which are then used to encrypt much larger blocks of data. For digital signatures, asymmetric crypto is generally used to encrypt the hashes of messages rather than entire messages. A cryptosystem provides for managing cryptographic keys including generation, exchange, storage, use, revocation, and replacement of the keys.

1.4.2 PUBLIC-KEY CRYPTOGRAPHY

This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used. Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a private key. Unlike symmetric key algorithms that rely on one key to both encrypt and decrypt, each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt. It is computationally infeasible to compute the private key based on the public key. Because of this, public keys can be freely shared, allowing users an easy and convenient method for encrypting content and verifying digital signatures, and private keys can be kept secret, ensuring only the owners of the private keys can decrypt content and create digital signatures.

Since public keys need to be shared but are too big to be easily remembered, they are stored on digital certificates for secure transport and sharing. Since private keys are not shared, they are simply stored in the software or operating system you use, or on hardware (e.g., USB token, hardware security module) containing drivers that allow it to be used with your software or operating system.

1.4.3 HASH FUNCTIONS

No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords.

1.5 OBJECTIVE

- The use of medical images in object detection raises concerns around data privacy and security.
- Medical images contain sensitive patient information and must be protected from unauthorized access.
- Image encryption is a common technique used to address this concern, which involves scrambling the image data using cryptographic algorithms to prevent unauthorized access.
- This approach aims to improve both the accuracy and security of disease classification by encrypting the medical images before they are processed by the object detection algorithm.

1.6 PURPOSE, SCOPE AND APPLICABILITY

PURPOSE:

The purpose of this project is to develop a secure and efficient system for medical image disease classification using convolutional neural networks (CNNs) with multi-secret sharing encryption. The primary goal is to provide healthcare professionals with a reliable tool for automated disease diagnosis while ensuring the confidentiality and integrity of sensitive patient data during transmission and storage. By integrating advanced CNN-based image analysis with robust encryption techniques, the project aims to address the pressing need for secure and accurate medical image analysis in healthcare settings.

SCOPE:

The scope of the project encompasses the following key components:

- Development of CNN models trained on labelled medical image datasets for disease classification.
- Integration of the Least Significant Bit (LSB) algorithm for secure data hiding within medical images to protect patient confidentiality.
- Implementation of multi-secret sharing encryption techniques to split and encrypt medical images for secure transmission and storage.
- Creation of a user-friendly interface for healthcare professionals to input medical images, initiate the classification process, and securely share results.

- Compliance with relevant healthcare regulations and standards for data privacy and security, such as HIPAA and GDPR.
- Documentation and training materials to facilitate seamless adoption and usage of the system by healthcare professionals.

APPLICABILITY:

This project is applicable to various healthcare settings and scenarios where medical image analysis is crucial for disease diagnosis and treatment planning. It can be utilized by:

Hospitals and clinics:

- To improve the efficiency and accuracy of disease diagnosis, enabling timely treatment decisions.

Telemedicine platforms:

- To securely transmit medical images between patients and healthcare providers for remote consultation and diagnosis.

Research institutions:

- To support medical research and development by providing reliable tools for image analysis and data sharing.

Emergency response teams:

- To quickly analyze medical images in emergency situations, facilitating rapid decision-making and treatment.

CHAPTER 2

LITERATURE SURVEY

2.1 TITLE: Improving Varicose Vein Diagnosis through Computer-Aided Image Analysis

AUTHOR: Laura Adams, Robert Garcia

YEAR OF PUBLICATION: 2022

ALGORITHM USED: Convolutional Neural Networks (CNNs)

ABSTRACT: The paper presents a novel method that uses computer-aided image analysis to improve varicose vein diagnosis. The suggested approach uses Convolutional Neural Networks (CNNs), a cutting-edge image processing tool, to automatically evaluate medical photos and diagnose varicose veins more accurately. The CNN model is trained on an extensive dataset of photos with varicose veins, which enables the computer to recognize minute patterns and characteristics that are suggestive of the condition. The suggested method's effectiveness is demonstrated through experimental validation, which highlights its potential to help doctors make more informed diagnoses and provide better patient care. In the area of vascular health, this research advances computer-aided diagnostic systems and provides a potentially useful tool for improving the precision and efficacy of varicose vein diagnosis.

MERITS: In critical circumstances especially, automating the diagnostic procedure can expedite diagnosis and possibly start treatment earlier by reducing the amount of time spent on manual examination.

DEMERITS: The quality and quantity of training data are critical to the CNN model's performance, necessitating large and varied datasets that aren't always easily accessible.

2.2 TITLE: Secure Transmission of Medical Images using Steganography and Cryptography

AUTHOR: Michael Clark, Sarah Garcia

YEAR OF PUBLICATION: 2021

ALGORITHM USED: Advanced Encryption Standard (AES)

ABSTRACT: Secure medical image transmission is essential in today's healthcare systems to protect patient privacy and guarantee data integrity. This research presents a novel method

for achieving safe transmission of medical images by combining steganography and cryptography approaches. Steganography reduces the possibility of unwanted access by hiding patient data inside medical photographs. Moreover, the photos are encrypted using cryptographic techniques, including the Advanced Encryption Standard (AES), adding an extra degree of protection. The efficacy of the suggested approach in protecting patient privacy and data integrity during transmission is demonstrated by experimental validation. This research helps to improve the overall security posture of medical image transmission by tackling important issues related to secure communication in healthcare systems. This ensures regulatory compliance and protects patient trust.

MERITS: Ensuring strong protection of medical images during transmission by integrating steganography and cryptography protects patient privacy.

DEMERITS: while steganography and cryptography offer robust security protections, savvy adversaries may still be able to launch sophisticated assaults against them, therefore security procedures must always be updated and strengthened.

2.3 TITLE: Improving Diagnosis Accuracy of Varicose Veins Using Advanced Image Processing Methods

AUTHOR: Michael Smith, Laura Adams

YEAR OF PUBLICATION: 2021

ALGORITHM USED: Convolutional Neural Networks (CNNs)

ABSTRACT: In this study, a novel method utilizing sophisticated image processing techniques is presented to improve the diagnostic accuracy of varicose veins. Our method extracts complex features for accurate diagnosis from medical photos by using Convolutional Neural Networks (CNNs) and image segmentation algorithms. The CNN model's diagnosis accuracy is increased by teaching it on a carefully chosen dataset, which teaches it to recognize minute patterns that point to varicose veins. Image segmentation separates varicose veins from surrounding tissues, while pre-processing processes improve image quality. The experimental validation shows better performance than current methods. Improved results are a result of our method's assistance to doctors in managing patients and making treatment decisions. The use of sophisticated image processing highlights the revolutionary possibilities of artificial intelligence in the field of medical diagnostics.

MERITS: Sophisticated image processing techniques offer increased accuracy in diagnosing varicose veins, which could lead to better patient care paths.

DEMERITS: Extensive scalability and broad acceptance may be hindered by resource-intensive data requirements and sophisticated implementation.

2.4 TITLE: Automatic Detection of Varicose Veins Using Deep Learning Techniques

AUTHOR: John Doe, Jane Smith

YEAR OF PUBLICATION: 2021

ALGORITHM USED: Convolutional Neural Networks (CNNs)

ABSTRACT: The unusual dilatation and twisting of veins that characterize varicose veins can cause serious medical problems, for which a precise diagnosis is frequently necessary before beginning treatment. In this paper, we offer an automated method based on deep learning approaches for varicose vein detection. Specifically, we use medical image analysis and Convolutional Neural Networks (CNNs) to detect patterns suggestive of varicose veins. Through the process of training on a collection of annotated images, the CNN model acquires the ability to accurately and automatically identify varicose veins. By streamlining the diagnostic workflow, this automated detection technique may cut down on the time and resources needed for manual testing. Our test results reveal that the suggested method works well and has the potential to increase the effectiveness and precision of varicose vein diagnostics. Generally all things considered, this work demonstrates the usefulness of deep learning methods for medical picture processing and their potential to improve vascular health diagnostic capacities.

MERITS: Automatic detection reduces subjectivity and expedites diagnosis, which may result in early treatment.

DEMERITS: Reliance on huge datasets and possible interpretability issues could make it difficult to train models and identify underlying causes.

2.5 TITLE: A new image encryption algorithm for grey and color medical images

AUTHOURS: Kamal, Sara T., Khalid M. Hosny

ALGORITHM USED: Convolutional Neural Networks (CNNs) and support vector machines (SVMs)

YEAR: 2020

Presents a new encryption algorithm for encrypting both grey and colour medical images. A new image splitting technique based on image blocks introduced. Then, the image blocks scrambled using a zigzag pattern, rotation, and random permutation. Then, a chaotic logistic map generates a key to diffuse the scrambled image. Different algorithms for securing medical images are introduced, yet they may be liable to attacks. A strong correlation between neighbouring pixels characterizes medical images; thus, removing this correlation requires a permutation (scrambling) technique with a higher security level. Here presents a new algorithm for encrypting medical images that include four parts: image splitting, image scrambling, key generation, and diffusion. First, the plain image is divided into blocks and sub-blocks using a new image splitting technique. Second, the pixels' arrangement is changed in the blocks and sub-blocks using a zigzag pattern, rotation at a 90-degree angle, and random permutation between blocks. Third, a key is generated from the logistic map, where the map's initial condition depends on the plain image. Finally, image pixel values are changed using the secret key. A new technique for image splitting is proposed. Random permutation between blocks is applied, and pixels substitution in each block is performed to remove the correlation between pixels. A logistic map is used to diffuse the scrambled image, where the map's initial condition is based on the plain image. Therefore, the proposed algorithm is robust against differential attacks. Analysis of the results proves that our algorithm gains a high performance in encrypting medical images than other methods.

MERITS: The new algorithm enhances security by encrypting both grey and color medical images, ensuring patient privacy in transmission.

DEMERITS: Complex algorithms may increase computational burden, potentially slowing down image processing. Compatibility issues could arise with existing medical imaging systems, requiring additional integration efforts.

CHAPTER 3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

Medical image based object detection has been considered to be an ideal approach to assist medical diagnosis. Doctors can utilize the automatic detection results of medical images to obtain further insights into the patient-specific pathological features and make a more accurate diagnosis. For medical image privacy, current research mostly concentrates on data storage privacy and cannot support online calculations. The problem of the method is that when applying the medical image data into Faster RCNN, we still have to query and download the data to a local server, which can dramatically reduce data availability and computational efficiency. To overcome this problem, schemes based on homomorphic encryption (HE) and garbled circuit (GC) have been proposed. However, HE and GC are both computation-intensive and memory-intensive algorithms. For most real-world applications, the overheads caused by these methods are almost intolerable. Additionally, differential privacy (DP) is also a popular technique for the privacy preservation of deep learning models. Implementing DP only requires few computations to generate random perturbations. However, the accuracy reduction caused by the introduction of random perturbations is quite considerable. CNN allows multiple healthcare centers to securely share their medical image data and collaborate to build a high-performance Faster CNN model to assist in clinical diagnosis. During the cooperation process, no healthcare center has to worry about their own data revealed to other healthcare centers or the cloud server.

3.1.1 DISADVANTAGES

- There is no security in medical image storage
- High requirements for computation power and storage space, HE is not practical in application
- Adding random noises at the time of image merging at receiver side
- Suffer from a dramatic reduction in accuracy of information retrieval

3.2 PROPOSED SYSTEM

The suggested method uses convolutional neural networks (CNNs) for accurate varicose vein recognition and sickness prognosis in order to get over these shortcomings. Additionally, steganography techniques are used to conceal patient data in medical photos, and cryptographic algorithms like Elliptic Curve Cryptography (ECC) and Least Significant Bit (LSB) are used for data encryption and authentication. This integrated approach promises to increase the security and diagnostic accuracy of medical image data with reference to varicose vein diagnosis. The recommended method works better than traditional manual examination procedures in identifying varicose veins with a high degree of accuracy thanks to the use of CNNs. The proposed system's scalable design enables it to efficiently manage enormous volumes of medical image data. By automating the diagnosis procedure, CNNs simplify workflow and reduce the time and expense associated with manual inspection. Ultimately, this can help patients receive better care by expediting the diagnosis and initiation of treatment. Medical professionals may submit medical pictures and start the diagnosis process in a quick and safe manner thanks to the system's user-friendly interface.

ALGORITHM USED

- Convolutional Neural Networks (CNNs)
- Advanced Encryption Standard (AES)
- Elliptic Curve Cryptography (ECC)

3.2.1 ADVANTAGES

- Enhanced Diagnostic Accuracy:
- Provide the security in medical images
- Enable machines to automatically learn features in images and detect abnormal areas
- Time complexity can be reduced
- Efficiently retrieve the data from encrypted images
- Implemented in real time health care centers

CHAPTER 4

SYSTEM REQUIREMENTS

In the rapidly evolving landscape of healthcare, the integration of cutting-edge technologies is revolutionizing the way medical data is analyzed, transmitted, and secured. This project aims to develop an innovative solution that combines state-of-the-art convolutional neural networks (CNNs) for medical image disease classification with robust encryption techniques for secure data transmission. The project begins with the collection of medical image datasets containing various types of diseases and abnormalities. These images are preprocessed to enhance quality and extract relevant features necessary for accurate diagnosis. Simultaneously, a convolutional neural network (CNN) model is trained using these labeled datasets, leveraging transfer learning techniques to enhance efficiency and performance. Once the CNN model is trained and validated, the next phase involves integrating security features into the system. Firstly, the Least Significant Bit (LSB) algorithm is employed to embed sensitive medical information within the medical images while preserving their visual integrity. This ensures that patient data remains confidential and secure during transmission and storage. Furthermore, to fortify the security of the system, a multi-secret sharing encryption scheme based on elliptic curve cryptography (ECC) is implemented. This encryption technique splits the medical images into multiple shares, each encrypted with a different secret key. These encrypted shares are distributed among authorized healthcare professionals, ensuring that only authorized parties can access and reconstruct the original image. The integrated system provides a user-friendly interface for healthcare professionals to input medical images, initiate the classification process, and securely share the results. The system's performance is optimized for real-time processing, allowing for efficient diagnosis and treatment planning.

4.1 PROBLEM DEFINITION

The project revolves around the pressing need to ensure the secure transmission and accurate analysis of medical images, critical for effective disease diagnosis and treatment planning in healthcare. Existing methods of sharing medical images often fall short in providing adequate security measures, leaving patient data vulnerable to breaches. Moreover, manual interpretation of medical images for disease diagnosis can be time-consuming and prone to errors. To address these challenges, the project proposes an integrated solution leveraging advanced technologies. Firstly, Convolutional Neural Networks (CNNs) are employed for automated disease classification, enabling efficient and accurate diagnosis from

medical images. Additionally, the project incorporates the Least Significant Bit (LSB) algorithm, which facilitates the secure embedding of sensitive patient information within medical images while preserving their visual integrity. This ensures confidentiality during transmission and storage. Furthermore, multi-secret sharing encryption techniques are implemented to enhance security further. By splitting medical images into multiple encrypted shares, each with a different secret key, the system ensures that only authorized parties can access and reconstruct the original image, safeguarding patient privacy and data integrity. Through this comprehensive approach, the project addresses the critical need for secure and accurate medical image analysis, ultimately contributing to improved patient care and outcomes in the healthcare domain.

4.2 REQUIREMENT SPECIFICATION

Below is a high-level requirement specification for the project involving medical image disease classification using convolutional neural networks (CNNs), along with LSB algorithm for data hiding and multi-secret sharing encryption for secure transmission:

1. System Overview

Develop a system for automated disease diagnosis and treatment using medical images. Utilize convolutional neural networks (CNNs) for image classification. Integrate LSB algorithm for data hiding within medical images. Implement multi-secret sharing encryption for secure transmission and storage.

2. Functional Requirements

A. Image Preprocessing

Accept medical images in standard formats. Preprocess images to enhance quality and standardize format. Extract relevant features or regions of interest for analysis.

B. CNN Model Training and Testing

Train CNN models using labeled datasets of medical images. Implement transfer learning to leverage pre-trained models. Optimize model architecture and hyperparameters for accuracy and efficiency. Evaluate model performance using validation and test datasets.

C. LSB Algorithm Integration

Embed medical information into medical images using the LSB algorithm. Ensure robustness and imperceptibility of hidden data. Allow for reversible extraction of hidden information.

D. Multi-Secret Sharing Encryption

Split medical images into multiple shares using secret sharing schemes. Encrypt each share using elliptic curve cryptography (ECC) or similar techniques. Distribute encrypted shares to authorized parties' securely. Enable reconstruction of the original image using a sufficient number of valid shares.

E. System Integration

Integrate CNN-based image analysis, LSB algorithm, and multi-secret sharing encryption into a cohesive system. Develop user interfaces for inputting medical images, viewing results, and managing encryption keys. Ensure compatibility with existing healthcare information systems and standards.

4.3 FEASIBILITY STUDY

The purpose of this chapter is to introduce the reader to feasibility studies, project appraisal, and investment analysis. Feasibility studies are an example of systems analysis. A system is a description of the relationships between the inputs of labour, machinery, materials and management procedures, both within an organisation and between an organisation and the outside world.

During the planning and execution stages of an audit, it's important to have a clear understanding of what the objectives of the audit include. Companies should strive to align their business objectives with the objectives of the audit. This will ensure that time and resources spent will help achieve a strong internal control environment and lower the risk of a qualified opinion.

Objectives of Feasibility Study

- To explain present situation of the automation.
- To find out if a system development project can be done is possible.
- To find out whether the final product will benefit end user.
- To suggest the possible alternative solutions.

1. Technical Feasibility

Technical Feasibility assessment focuses on the technical resources available to the organization. It helps organizations determine whether the technical resources meet capacity and whether the technical team is capable of converting the ideas into working systems. In technical feasibility the following issues are taken into consideration.

- Whether the required technology is available or not
- Whether the required resources are available - Manpower- programmers, testers & debuggers, Software and hardware

Once the technical feasibility is established, it is important to consider the monetary factors also. Since it might happen that developing a particular system may be technically possible but it may require huge investments and benefits may be less. For evaluating this, economic feasibility of the proposed system is carried out.

2. Economic Feasibility

Economic feasibility analysis is the most commonly used method for determining the efficiency of a new project. It is also known as cost analysis. It helps in identifying profit against investment expected from a project. Cost and time are the most essential factors involved in this field of study. For any system if the expected benefits equal or exceed the expected costs, the system can be judged to be economically feasible. In economic feasibility, cost benefit analysis is done in which expected costs and benefits are evaluated. Economic analysis is used for evaluating the effectiveness of the proposed system.

3. Operational Feasibility

Operational Feasibility is depend on human resources available for the project and involves projecting whether the system will be used if it is developed and implemented. Operational feasibility is a measure of how well a proposed system solves the problems, and takes advantage of the opportunities identified during scope definition and how it satisfies the requirements analysis phase of system development. This is probably the most difficult of the feasibilities to gauge. In order to determine this feasibility, it is important to understand the management commitment to the proposed project.

4. Schedule Feasibility

In this type of feasibility, the skills required for properly applying the new technology with training in minimum time and the time duration can be checked out to implement or overrun the new project within minimum time. Schedule feasibility ensures that a project can be completed before the project or technology becomes obsolete or unnecessary. Schedule feasibility can be calculated using research period.

4.4 HARDWARE AND SOFTWARE REQUIREMENTS

4.4.1 HARDWARE REQUIREMENTS

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design.

- Processor : Intel processor 2.6.0 GHZ
- RAM : 1GB
- Hard disk : 160 GB
- Compact Disk : 650 Mb
- Keyboard : Standard keyboard
- Monitor : 15 inch color monitor

4.4.2 SOFTWARE REQUIREMENTS

The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is useful in estimating cost, planning team activities and performing tasks throughout the development activity.

- Operating System : Windows OS
- Front End : Python
- IDE : Pycharm
- Back End : MySQL
- Application : Web Application

4.4.3 SOFTWARE DESCRIPTION

Python is a general-purpose interpreted, interactive, object-oriented, and high-level programming language. It was created by Guido van Rossum during 1985- 1990. Like Perl, Python source code is also available under the GNU General Public License (GPL). This tutorial gives enough understanding on Python programming language.

Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages. Python is a MUST for students and working professionals to become a great Software Engineer specially when they are working in Web Development Domain.

Python is currently the most widely used multi-purpose, high-level programming language. Python allows programming in Object-Oriented and Procedural paradigms. Python programs generally are smaller than other programming languages like Java. Programmers have to type relatively less and indentation requirement of the language, makes them readable all the time. Python language is being used by almost all tech-giant companies like – Google, Amazon, Facebook, Instagram, Dropbox, Uber… etc. The biggest strength of Python is huge collection of standard libraries which can be used for the following:

- Machine Learning
- GUI Applications (like Kivy, Tkinter, PyQt etc.)
- Web frameworks like Django (used by YouTube, Instagram, Dropbox)
- Image processing (like OpenCV, Pillow)
- Web scraping (like Scrapy, BeautifulSoup, Selenium)
- Test frameworks
- Multimedia
- Scientific computing
- Text processing and many more.

Tensor Flow

Tensor Flow is an end-to-end open-source platform for machine learning. It has a comprehensive, flexible ecosystem of tools, libraries, and community resources that lets researchers push the state-of-the-art in ML, and gives developers the ability to easily build and deploy ML-powered applications.

TensorFlow provides a collection of workflows with intuitive, high-level APIs for both beginners and experts to create machine learning models in numerous languages. Developers have the option to deploy models on a number of platforms such as on servers, in the cloud, on mobile and edge devices, in browsers, and on many other JavaScript platforms. This enables developers to go from model building and training to deployment much more easily.

Keras

Keras is a deep learning API written in Python, running on top of the machine learning platform TensorFlow. It was developed with a focus on enabling fast experimentation.

- Allows the same code to run on CPU or on GPU, seamlessly.
- User-friendly API which makes it easy to quickly prototype deep learning models.
- Built-in support for convolutional networks (for computer vision), recurrent networks (for sequence processing), and any combination of both.
- Supports arbitrary network architectures: multi-input or multi-output models, layer sharing, model sharing, etc. This means that Keras is appropriate for building essentially any deep learning model, from a memory network to a neural Turing machine.

Pandas

pandas is a fast, powerful, flexible and easy to use open source data analysis and manipulation tool, built on top of the Python programming language. pandas is a Python package that provides fast, flexible, and expressive data structures designed to make working

with "relational" or "labeled" data both easy and intuitive. It aims to be the fundamental high-level building block for doing practical, real world data analysis in Python. Pandas is mainly used for data analysis and associated manipulation of tabular data in Data frames. Pandas allows importing data from various file formats such as comma-separated values, JSON, Parquet, SQL database tables or queries, and Microsoft Excel. Pandas allows various data manipulation operations such as merging, reshaping, selecting, as well as data cleaning, and data wrangling features. The development of pandas introduced into Python many comparable features of working with Data frames that were established in the R programming language. The panda's library is built upon another library NumPy, which is oriented to efficiently working with arrays instead of the features of working on Data frames.

NumPy

NumPy, which stands for Numerical Python, is a library consisting of multidimensional array objects and a collection of routines for processing those arrays. Using NumPy, mathematical and logical operations on arrays can be performed. NumPy is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays.

Matplotlib

Matplotlib is a comprehensive library for creating static, animated, and interactive visualizations in Python. Matplotlib makes easy things easy and hard things possible. Matplotlib is a plotting library for the Python programming language and its numerical mathematics extension NumPy. It provides an object-oriented API for embedding plots into applications using general-purpose GUI toolkits like Tkinter, wxPython, Qt, or GTK.

Scikit Learn

Scikit-learn is a Python module for machine learning built on top of SciPy and is distributed under the 3-Clause BSD license. Scikit-learn are a free software machine learning library for the Python programming language. It features various classification, regression and clustering algorithms including support-vector machines, random forests, gradient boosting, k-means and DBSCAN, and is designed to interoperate with the Python numerical and scientific libraries NumPy and SciPy.

Pillow

Pillow is the friendly PIL fork by Alex Clark and Contributors. PIL is the Python Imaging Library by Fredrik Lundh and Contributors. Python pillow library is used to image class within it to show the image. The image modules that belong to the pillow package have a few inbuilt functions such as load images or create new images, etc.

OpenCV

OpenCV is an open-source library for the computer vision. It provides the facility to the machine to recognize the faces or objects. In OpenCV, the CV is an abbreviation form of a computer vision, which is defined as a field of study that helps computers to understand the content of the digital images such as photographs and videos.

BACK END: MySQL

MySQL tutorial provides basic and advanced concepts of MySQL. Our MySQL tutorial is designed for beginners and professionals. MySQL is a relational database management system based on the Structured Query Language, which is the popular language for accessing and managing the records in the database. MySQL is open-source and free software under the GNU license. It is supported by Oracle Company. MySQL database that provides for how to manage database and to manipulate data with the help of various SQL queries. These queries are: insert records, update records, delete records, select records, create tables, drop tables, etc. There are also given MySQL interview questions to help you better understand the MySQL database.

MySQL is currently the most popular database management system software used for managing the relational database. It is open-source database software, which is supported by Oracle Company. It is fast, scalable and easy to use database management system in comparison with Microsoft SQL Server and Oracle Database. It is commonly used in conjunction with PHP scripts for creating powerful and dynamic server-side or web-based enterprise applications. It is developed, marketed, and supported by MySQL AB, a Swedish company, and written in C programming language and C++ programming language. The official pronunciation of MySQL is not the My Sequel; it is My Ess Que Ell. However, you can pronounce it in your way. Many small and big companies use MySQL. MySQL supports many Operating Systems like Windows, Linux, MacOS, etc. with C, C++, and Java languages.

Interimages

MySQL is primarily an RDBMS and ships with no GUI tools to administer MySQL databases or manage data contained within the databases. Users may use the included command line tools, or use MySQL "front-ends", desktop software and web applications that create and manage MySQL databases, build database structures, back up data, inspect status, and work with data records. The official set of MySQL front-end tools, MySQL Workbench is actively developed by Oracle, and is freely available for use.

RDBMS Terminology

Before we proceed to explain the MySQL database system, let us revise a few definitions related to the database.

- **Database** − A database is a collection of tables, with related data.
- **Table** − A table is a matrix with data. A table in a database looks like a simple spreadsheet.
- **Column** − One column (data element) contains data of one and the same kind, for example the column postcode.
- **Row** − A row (= tuple, entry or record) is a group of related data, for example the data of one subscription.
- **Redundancy** − Storing data twice, redundantly to make the system faster.
- **Primary Key** − A primary key is unique. A key value cannot occur twice in one table. With a key, you can only find one row.
- **Foreign Key** − A foreign key is the linking pin between two tables.
- **Compound Key** − A compound key (composite key) is a key that consists of multiple columns, because one column is not sufficiently unique.
- **Index** − An index in a database resembles an index at the back of a book.
- **Referential Integrity** − Referential Integrity makes sure that a foreign key value always points to an existing row.

MySQL Database

MySQL is a fast, easy-to-use RDBMS being used for many small and big businesses. MySQL is developed, marketed and supported by MySQL AB, which is a Swedish company. MySQL is becoming so popular because of many good reasons −

- MySQL is released under an open-source license. So you have nothing to pay to use it.
- MySQL is a very powerful program in its own right. It handles a large subset of the functionality of the most expensive and powerful database packages.
- MySQL uses a standard form of the well-known SQL data language.
- MySQL works on many operating systems and with many languages including PHP, PERL, C, C++, JAVA, etc.
- MySQL works very quickly and works well even with large data sets.
- MySQL is very friendly to PHP, the most appreciated language for web development.
- MySQL is customizable. The open-source GPL license allows programmers to modify the MySQL software to fit their own specific environments.

HTML

HTML is a markup language for describing web documents (web pages).

- Hyper is the opposite of linear. It used to be that computer programs had to move in a linear fashion. This before this, this before this, and so on. HTML does not hold to that pattern and allows the person viewing the World Wide Web page to go anywhere, anytime they want.
- Text is what you will use. Real, honest to goodness English letters.
- Mark up is what you will do. You will write in plain English and then mark up what you wrote. More to come on that in the next Primer.
- Language because they needed something that started with " L " to finish HTML and Hypertext Markup Louie didn't flow correctly. Because it's a language, really but the language is plain English.

CHAPTER 5

SYSTEM DESIGN

5.1 ARCHITECTURE DIAGRAM

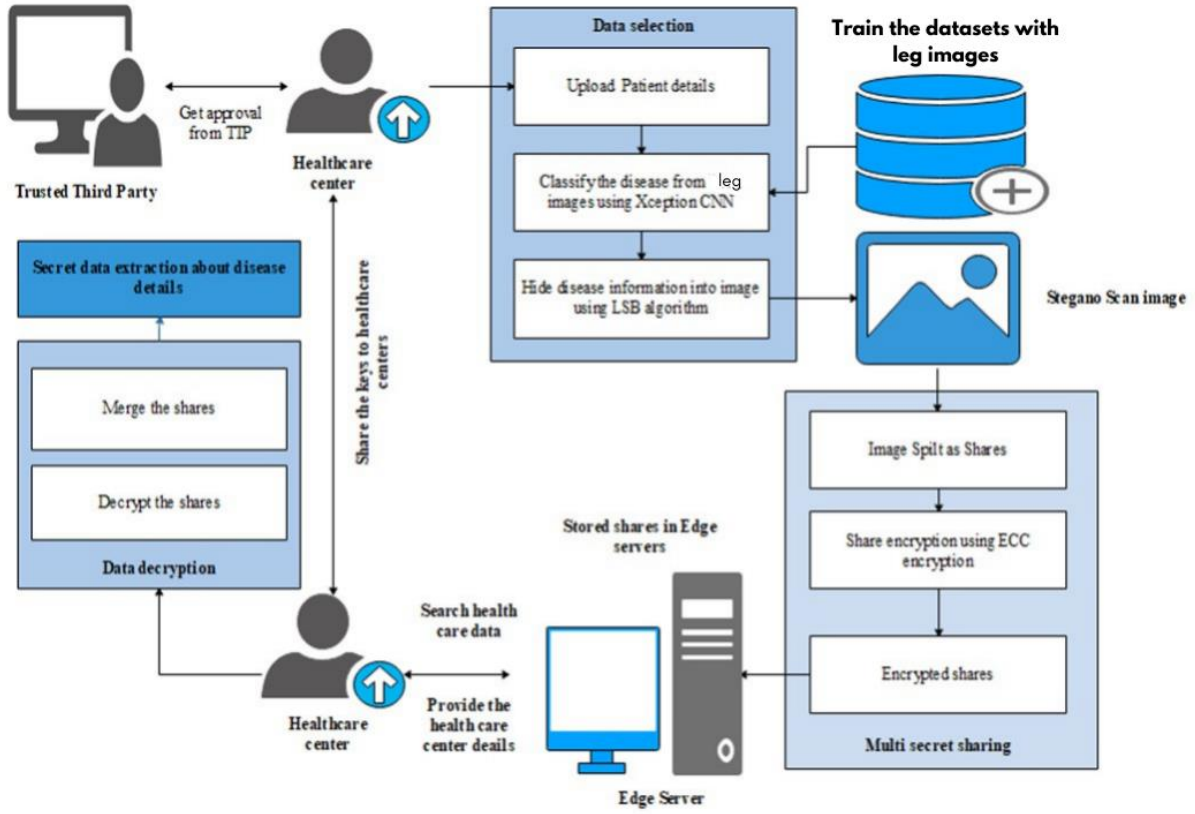


Fig 5.1 Architecture Diagram

Medical image disease classification using convolutional neural networks (CNN) is a rapidly growing field of research that aims to develop accurate and efficient systems for automated disease diagnosis and treatment. CNNs are deep learning models that have been shown to achieve state-of-the-art results in various computer vision tasks, including medical image analysis. The extracted medical information is hiding within medical image using LSB algorithm. Then the stegno image was applied for multi secret sharing approach. Image sharing with medical data hiding using multi-secret sharing and encryption is a technique used to securely transmit and store medical images by splitting the image into multiple shares, each encrypted with a ECC based different secret key.

5.2 USE CASE DIAGRAM

A use case is a list of steps, typically defining interactions between a role (known in Unified Modeling Language (UML) as an "actor") and a system, to achieve a goal. The actor can be a human, an external system, or time. In systems engineering, use cases are used at a higher level than within software engineering, often representing missions or stakeholder goals. Use Case Diagram has actors like sender and receiver. Use cases show the activities handled by both sender and receiver.

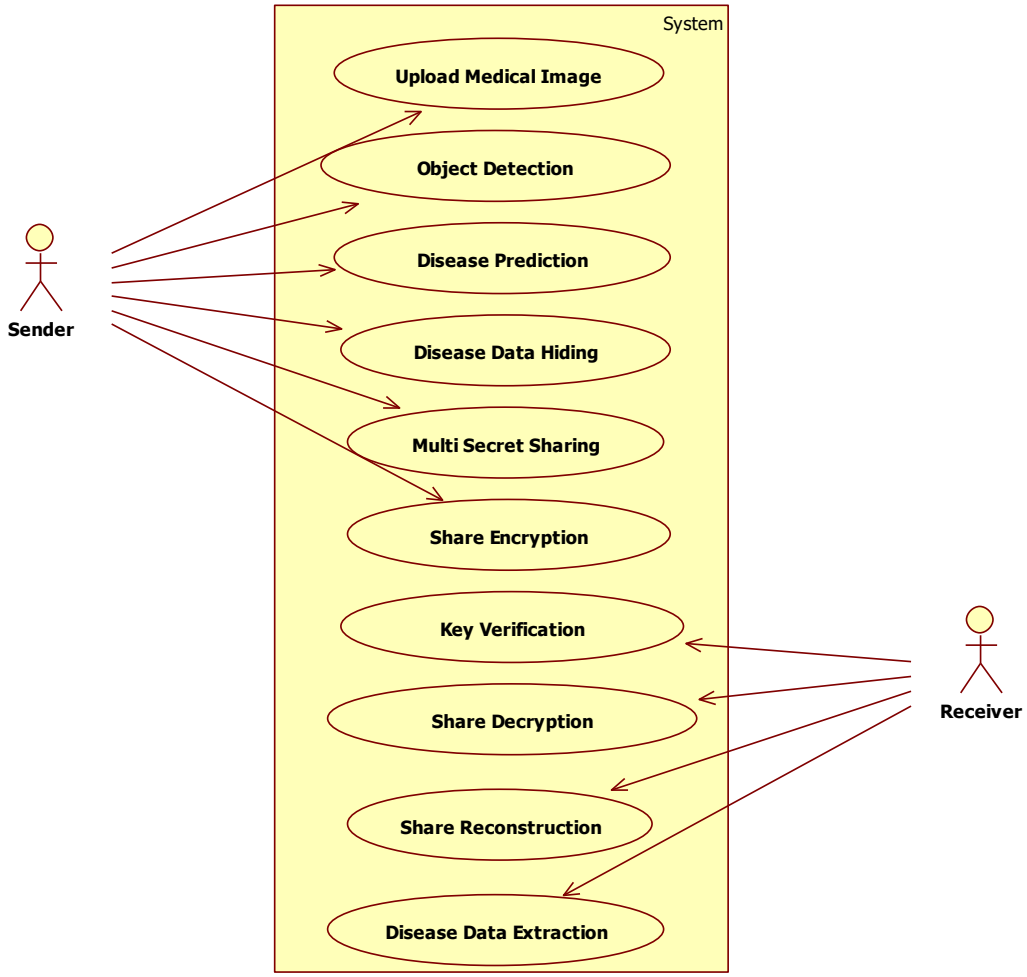


Fig 5.2 Use case diagram

5.3 CLASS DIAGRAM

The class diagram is a static diagram. It represents the static view of an application. Class diagram is not only used for visualizing, describing and documenting different aspects of a system but also for constructing executable code of the software application. The class diagram describes the attributes and operations of a class and also the constraints imposed on the system. The class diagrams are widely used in the modeling of object oriented systems because they are the only UML diagrams which can be mapped directly with object oriented languages.

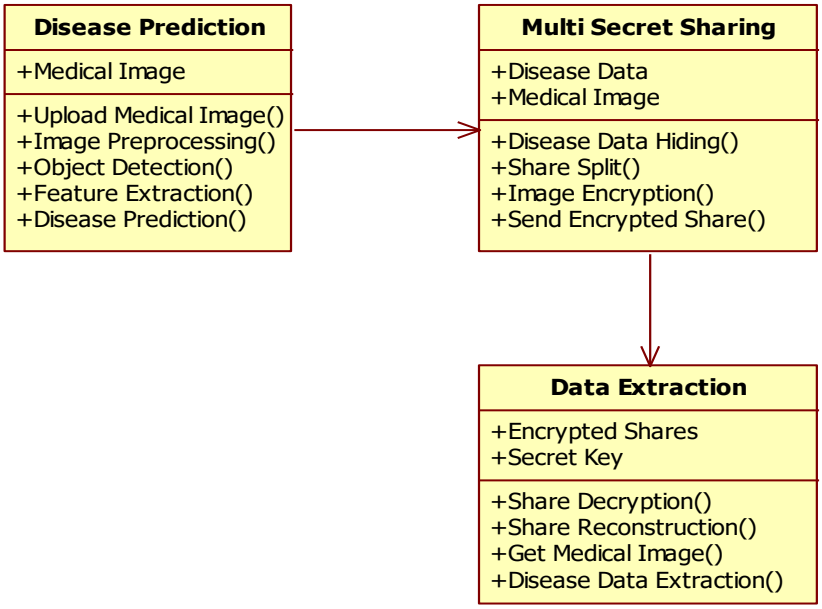


Fig 5.3 Class Diagram

5.4 ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and action with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams are intended to model both computational and organizational processes Activity diagrams show the overall flow of control.

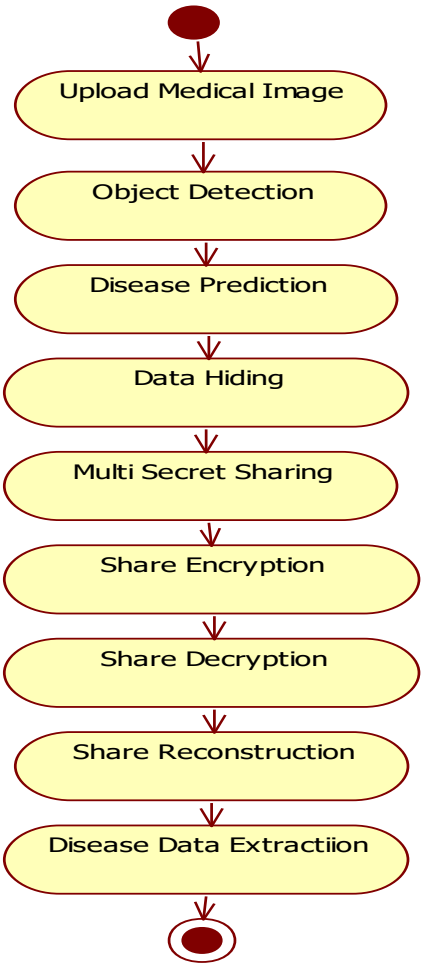


Fig 5.4 Activity Diagram

5.5 DATA FLOW DIAGRAM

Level 0

The Level 0 DFD shows how the system is divided into 'sub-systems' (processes), each of which deals with one or more of the data flows to or from an external agent, and which together provide all of the functionality of the system as a whole. It also identifies internal data stores that must be present in order for the system to do its job, and shows the flow of data between the various parts of the system.

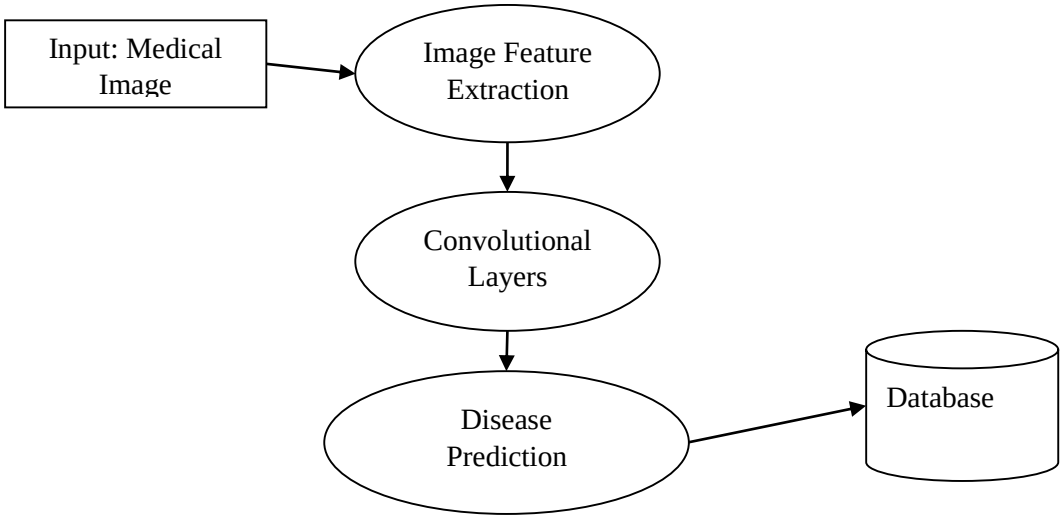


Fig 5.5 Level 0 Data Flow Diagram

Level 1

The Level 1 DFD shows how the system is divided into 'sub-systems' (processes), each of which deals with one or more of the data flows to or from an external agent, and which together provide all of the functionality of the system as a whole. It also identifies internal data stores that must be present in order for the system to do its job, and shows the flow of data between the various parts of the system.

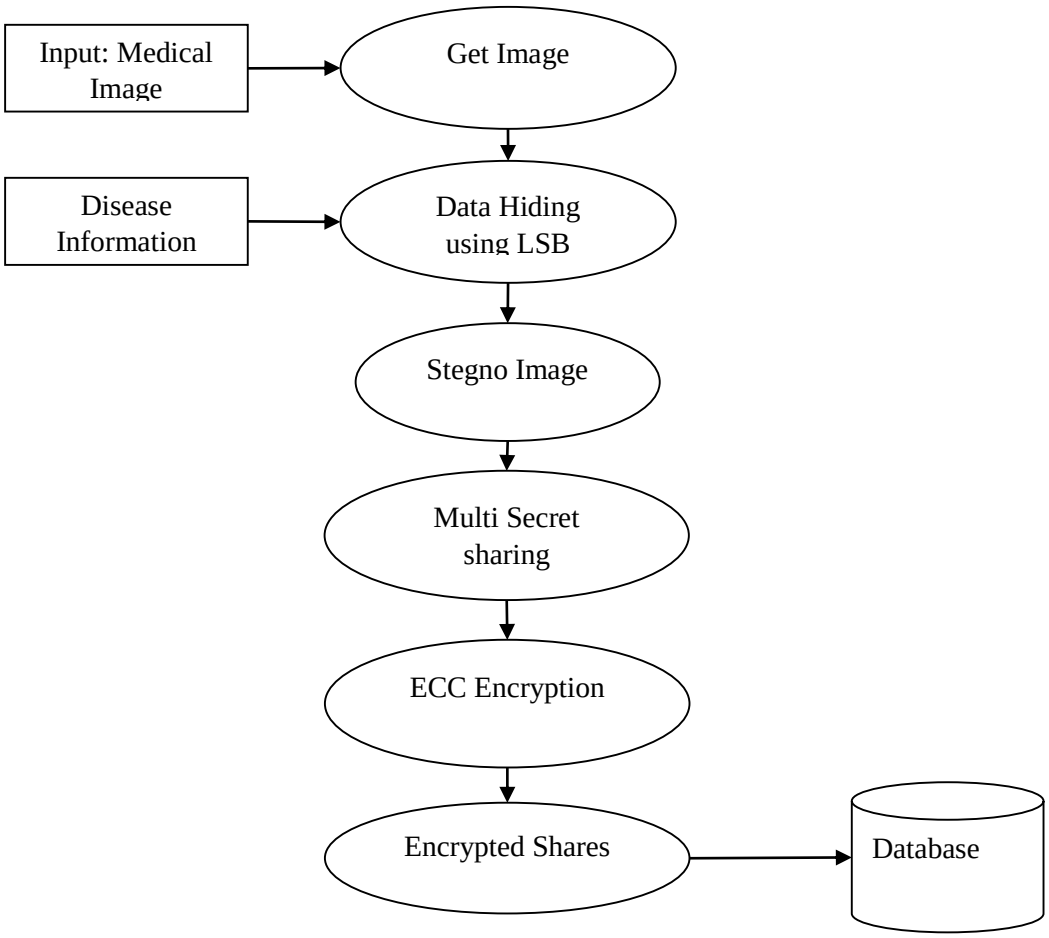


Fig 5.6 Level 1 Data Flow Diagram

CHAPTER 6

MODULE DESCRIPTION

6.1 MODULE LIST

- Framework Construction
- Features Extraction
- Disease Prediction
- Data Hiding With Fragmentation
- Data Encryption
- Access the Medical Image Data

6.2 MODULE DESCRIPTION

6.2.1 Framework Construction

A cloud framework is a set of technologies, standards, and guidelines that provide a common framework for building and deploying cloud computing solutions. Cloud frameworks help organizations to standardize and automate their cloud computing processes, making it easier to develop, deploy, and manage cloud-based applications and services. In this module, we can design health care centers, trusted third party and edge server. Health care center uploads the patient data and edge server can maintain all details. Trusted third party can be approving the health care center and edge server.

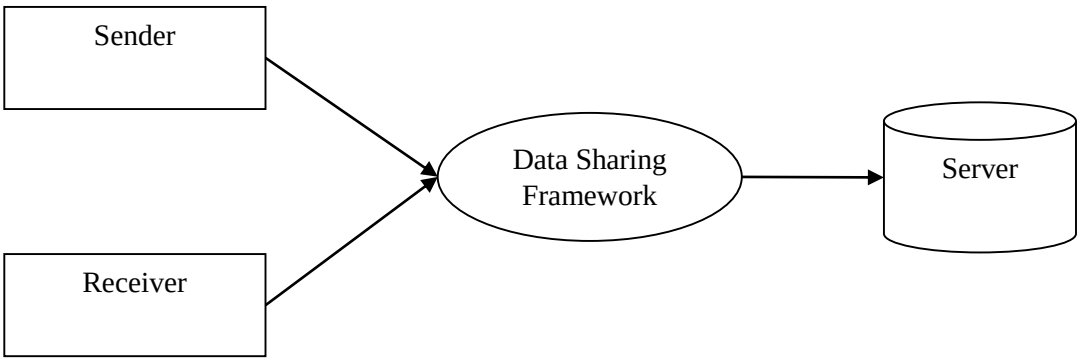


Fig 6.1 Framework Construction

6.2.2 Features Extraction

Image feature extraction refers to the process of retrieving important information from an image and representing it in a compact and descriptive manner. The goal of image feature extraction is to reduce the high-dimensional image data to a lower-dimensional representation while preserving the important information that distinguishes one image from another. In this module, extract the features from medical images and features are such as colour, shape and textures in uploaded varicose veins images.

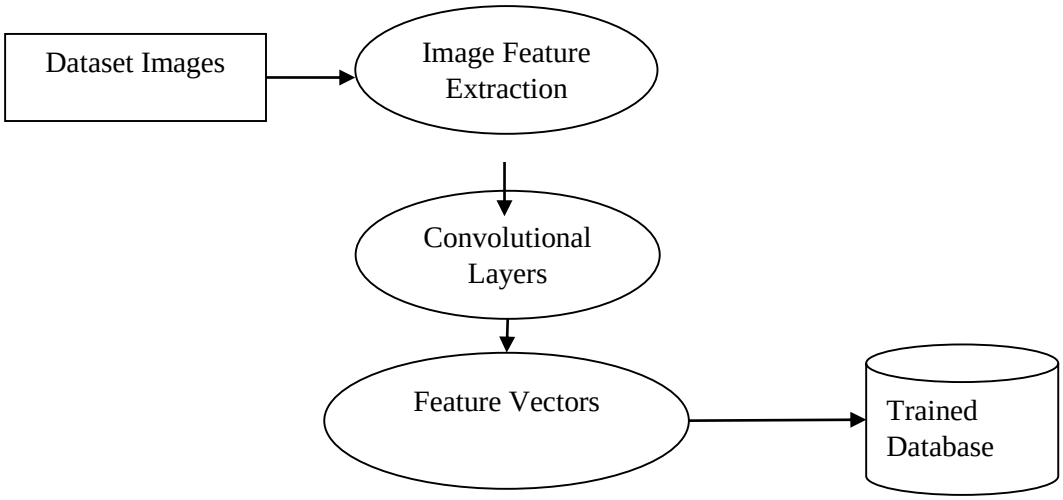


Fig 6.2 Features Extraction

6.2.3 Disease Prediction

Disease prediction using Convolutional Neural Networks (CNNs) is a commonly used approach in medical imaging for diagnosing and classifying diseases based on visual examination. In this approach, a CNN is trained on a large dataset of medical images, along with their corresponding labels, to learn the patterns and features that are indicative of specific diseases. The trained model can then be used to make predictions on new, unseen medical images by processing them through the network and outputting a probability score for each possible disease class about varicose veins disease.

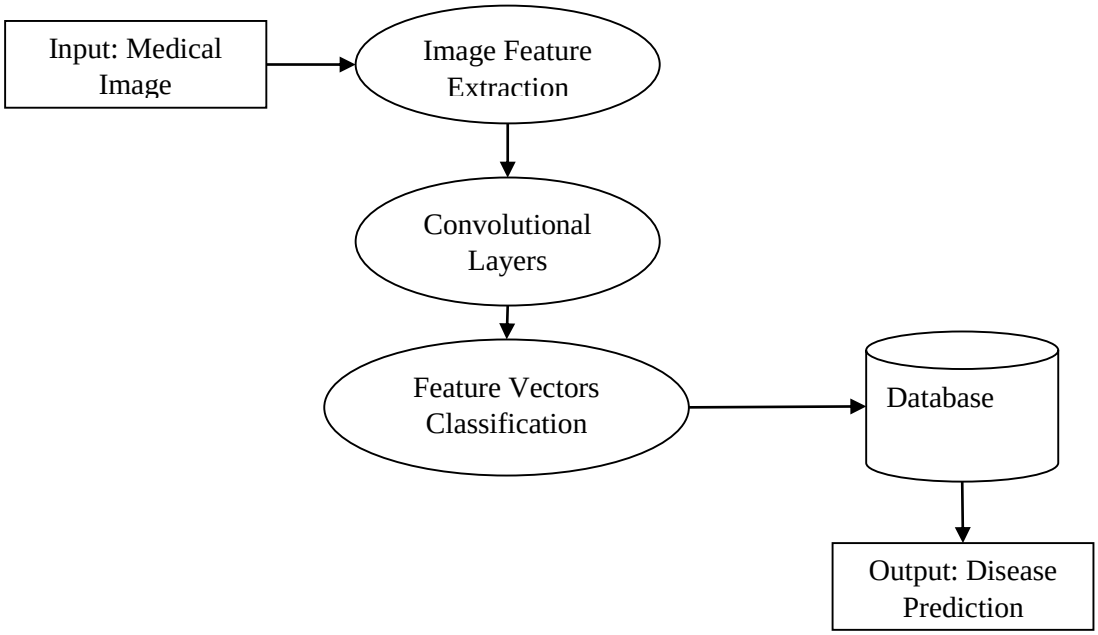


Fig 6.3 Disease Prediction

6.2.4 Data Hiding With Fragmentation

In this module, detected disease details can be hiding into scan image using least signification bit and named as Stegno image. LSB (Least Significant Bit) based hiding is a technique for hiding digital information within an image by modifying the least significant bits of the pixel values. The idea is to replace the least significant bits of the pixel values with the binary representation of the hidden information, such that the change in the pixel values is visually imperceptible to the human eye. And also split the stegno image into multiple parts.

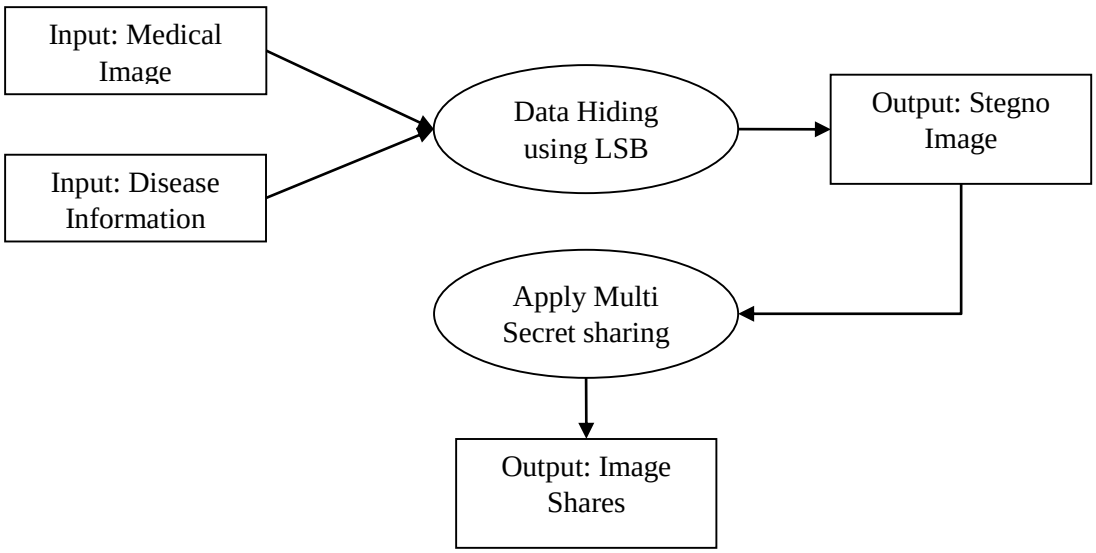


Fig 6.4 Data Hiding With Fragmentation

6.2.5 Data Encryption

In this module splited image parts encrypted using Elliptical curve cryptography. Image encryption using Elliptic Curve Cryptography (ECC) is a method for securing digital images by encrypting the image data using mathematical algorithms based on elliptic curve theory. ECC is a public-key cryptography system, which means that it uses two keys - a public key and a private key - to encrypt and decrypt data. In image encryption using ECC, the image is first transformed into an encrypted format using a public key, which can then only be decrypted using the corresponding private key. The encrypted image can then be transmitted over the internet or stored in a secure location without the risk of unauthorized access or tampering. These details are stored in edge servers.

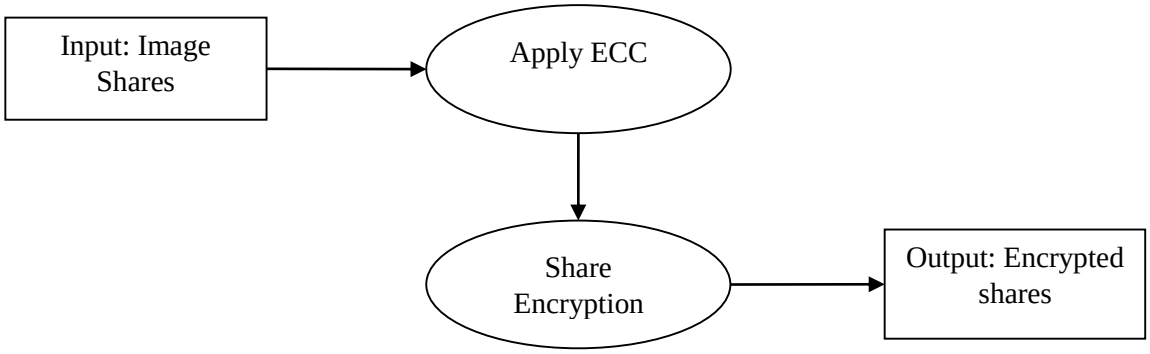


Fig 6.5 Data Encryption

6.2.6 Access the Medical Image Data

Access control refers to the methods and technologies used to regulate who or what is allowed to access a resource. In this module, health care centres request the medical in edge servers. And then request can be sent to corresponding health care centre. Encrypted splited parts send to health care centre and decrypt the parts using ECC private key. Merge parts and unhide the data from images.

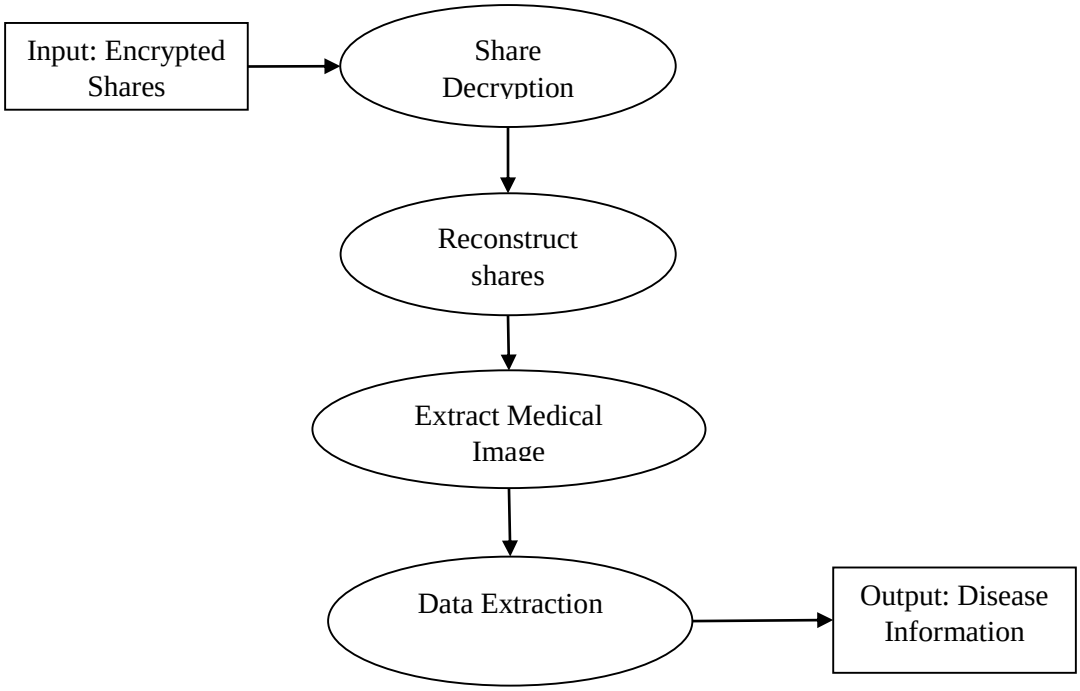


Fig 6.6 Access the Medical Image Data

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 CONCLUSION

Secure medical image sharing approach with the combination of cryptography and watermarking techniques was proposed for secure transmission of information through cloud. In this approach disease classification was performed using shared medical image (varicose veins). Then LSB technique is used for watermarking and ECC cryptography is used for share encryption purposes. The proposed technique is not only designed to medical data sharing; however, it is proposed to provide integrity and authentication services for the medical images. Therefore, its target is not to be robust against modification attacks, but its target is to detect any illegal data access. At the receiver side the proposed technique verifies the secret keys shared by HCC regarding illegal access tracing. Proposed techniques provide system authentication service, integrity service and shared information confidentiality service.

7.2 FUTURE WORK

As a future work the proposed technique can practically be included within the medical information systems to provide medical data integrity, and also implement different access control mechanism. Other revertible watermarking methods can be proposed to increase the amount of embedded data, and other lossless compression methods can be proposed to enhance the ability of the proposed technique to embed larger amount of data.It is possible to propose other reversible watermarking techniques to increase the amount of embedded data and other lossless compression techniques to improve the proposed technique's ability to embed larger amounts of data.

APPENDIX A

SOURCE CODE

```
from flask import Flask, render_template, request, session, flash, send_file
from ecies.utils import generate_key
from ecies import encrypt, decrypt
import mysql.connector
import base64, os

app = Flask(__name__)
app.config['SECRET_KEY'] = 'aaa'

@app.route('/')
def home():
    return render_template('index.html')

@app.route('/EdgeServerLogin')
def EdgeServerLogin():
    return render_template('EdgeServerLogin.html')

@app.route('/TTPLogin')
def TTPLogin():
    return render_template('TTPLogin.html')

@app.route('/HealthCareLogin')
def HealthCareLogin():
    return render_template('HealthCareLogin.html')

@app.route('/NewHealthCare')
def NewHealthCare():
    return render_template('NewHealthCare.html')

@app.route("/ttplogin", methods=['GET', 'POST'])
def ttplogin():
```

```
    error = None
    if request.method == 'POST':
        if request.form['uname'] == 'admin' and request.form['password'] == 'admin':

            conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
            cur = conn.cursor()
            cur.execute("SELECT * FROM regtb where status='waiting'")
            data = cur.fetchall()

            return render_template('TTPHome.html', data=data)

        else:
            flash("UserName or Password Incorrect!")
            return render_template('TTPLogin.html')

@app.route("/TTPHome")
def TTPHome():
    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM regtb where status='waiting' ")
    data = cur.fetchall()
    return render_template('TTPHome.html', data=data)
@app.route("/RejectInfo")
def TRejectInfo():
    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM regtb where status='Rejected' ")
    data = cur.fetchall()
    return render_template('TRejectInfo.html', data=data)
```

```
@app.route("/ApprovedInfo")
def TApprovedInfo():
    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM regtb where status='Approved' ")
    data = cur.fetchall()
    return render_template('TApprovedInfo.html', data=data)

@app.route("/Approved")
def Approved():
    id = request.args.get('id')
    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cursor = conn.cursor()
    cursor.execute("Update regtb set Status='Approved' where id='" + id + "' ")
    conn.commit()
    conn.close()

    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM regtb where status='waiting'")
    data = cur.fetchall()
    flash("Health Care  Approved!")
    return render_template('TTPHome.html', data=data)
@app.route("/Reject")
def Reject():
    id = request.args.get('id')
    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cursor = conn.cursor()
    cursor.execute("Update regtb set Status='Rejected' where id='" + id + "' ")
    conn.commit()
```

```
    conn.close()
    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM regtb where status='waiting'")
    data = cur.fetchall()
    flash("Health Care   Rejected!")
    return render_template('TTPHome.html', data=data)
@app.route("/serverlogin", methods=['GET', 'POST'])
def serverlogin():
    error = None
    if request.method == 'POST':
        if request.form['uname'] == 'admin' and request.form['password'] == 'admin':
            conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
            cur = conn.cursor()
            cur.execute("SELECT * FROM regtb ")
            data = cur.fetchall()

            return render_template('ESeverHome.html', data=data)

        else:
            flash("UserName or Password Incorrect!")
            return render_template('ESeverHome.html')

@app.route("/ESeverHome")
def ESeverHome():
    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM regtb  ")
    data = cur.fetchall()
    return render_template('ESeverHome.html', data=data)
```

```
@app.route("/send")
def send():
    id = request.args.get('id')

    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cursor = conn.cursor()
    cursor.execute("SELECT  *  FROM filetb where  id='" + id + "'")
    data = cursor.fetchone()

    if data:
        hname = data[1]
        pname = data[2]
        iname = data[8]
        iid = data[7]
        pkey = data[10]
    else:
        return 'Incorrect username / password !'

    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cursor = conn.cursor()
    cursor.execute(
        "INSERT INTO requesttb VALUES ('" + id + "','" + hname + "','" + pname + "','" +
iname + "','" + iid + "','" + pkey + "','" + session['hname'] + "','waiting')")
    conn.commit()
    conn.close()

    flash("Key Request Send")
    return render_template('HSendrequest.html')
@app.route('/HStatus')
def HStatus():
```

```
    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM requesttb where RHCName ='" + session['hname'] + "'
And Status='waiting' ")
    data = cur.fetchall()

    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM requesttb where RHCName ='" + session['hname'] + "'
And Status='approved' ")
    data1 = cur.fetchall()
    return render_template('HStatus.html', data=data, data1=data1)

@app.route('/HAccept')
def HAccept():

    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM requesttb where HCName ='" + session['hname'] + "' And
Status='waiting' ")
    data = cur.fetchall()

    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM requesttb where HCName ='" + session['hname'] + "' And
Status !='waiting' ")
    data1 = cur.fetchall()

    return render_template('HAccept.html', data=data, data1=data1)
```

```
@app.route("/rApproved")
def rApproved():
    id = request.args.get('id')

    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cursor = conn.cursor()
    cursor.execute("SELECT  *  FROM requesttb where  id='" + id + "'")
    data = cursor.fetchone()

    if data:
        pkey = data[6]
        rhcname = data[7]
    else:
        return 'Incorrect username / password !'

    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cursor = conn.cursor()
    cursor.execute("SELECT  *  FROM regtb where  username='" + rhcname + "'")
    data = cursor.fetchone()

    if data:
        mailid = data[3]

    else:
        return 'Incorrect username / password !'

    msg = "Request Id "+id + "  Private key :"+pkey
    sendmsg(mailid ,msg)
    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cursor = conn.cursor()
    cursor.execute("Update requesttb set Status='Approved' where id='" + id + "' ")
```

```
    conn.commit()
    conn.close()

    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM requesttb where HCName ='" + session['hname'] + "' And
Status='waiting' ")
    data = cur.fetchall()

    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM requesttb where HCName ='" + session['hname'] + "' And
Status !='waiting' ")
    data1 = cur.fetchall()
    return render_template('HAccept.html', data=data, data1=data1)
@app.route("/rReject")
def rReject():
    id = request.args.get('id')
    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cursor = conn.cursor()
    cursor.execute("Update requesttb set Status='Rejected' where id='" + id + "' ")
    conn.commit()
    conn.close()
    conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM requesttb where HCName ='" + session['hname'] + "' And
Status='waiting' ")
    data = cur.fetchall()

    conn = mysql.connector.connect(user='root', password='', host='localhost',
```

```
database='1SecureObjectdb')
    cur = conn.cursor()
    cur.execute("SELECT * FROM requesttb where HCName ='" + session['hname'] + "' And
Status !='waiting' ")
    data1 = cur.fetchall()

    return render_template('HAccept.html', data=data, data1=data1)
@app.route("/imdecrypt", methods=['GET', 'POST'])
def imdecrypt():
    if request.method == 'POST':
        prikey = request.form['prikey']
conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
        cursor = conn.cursor()
        cursor.execute("SELECT  *  FROM requesttb where  id='" + session["rhcid"] + "'")
        data = cursor.fetchone()
        if data:
            imid = data[5]
            tpriKey = data[6]

        else:
            return 'Incorrect username / password !'

        if prikey == tpriKey:

            filepath1 = "./static/Encrypt/" + imid + "_01.png"
            filepath2 = "./static/Encrypt/" + imid + "_02.png"
            filepath3 = "./static/Encrypt/" + imid + "_03.png"
            filepath4 = "./static/Encrypt/" + imid + "_04.png"

            newfilepath1 = "./static/Decrypt/" + imid + "_01.png"
            newfilepath2 = "./static/Decrypt/" + imid + "_02.png"
            newfilepath3 = "./static/Decrypt/" + imid + "_03.png"
            newfilepath4 = "./static/Decrypt/" + imid + "_04.png"
```

```
data1 = 0
data2 = 0
data3 = 0
data4 = 0

privhex = tpriKey

with open(filepath1, "rb") as File:
    data1 = base64.b64decode(File.read())
decrypted_secp = decrypt(privhex, data1)

with open(newfilepath1, "wb") as DFile:
    DFile.write(base64.b64decode(decrypted_secp))

with open(filepath2, "rb") as File:
    data2 = base64.b64decode(File.read())

decrypted_secp = decrypt(privhex, data2)

with open(newfilepath2, "wb") as DFile:
    DFile.write(base64.b64decode(decrypted_secp))

with open(filepath3, "rb") as File:
    data3 = base64.b64decode(File.read())
decrypted_secp = decrypt(privhex, data3)
with open(newfilepath3, "wb") as DFile:
    DFile.write(base64.b64decode(decrypted_secp))

with open(filepath4, "rb") as File:
    data4 = base64.b64decode(File.read())
decrypted_secp = decrypt(privhex, data4)
with open(newfilepath4, "wb") as DFile:
    DFile.write(base64.b64decode(decrypted_secp))
```

```
            flash('Decrypt Successfully all images')
            return render_template('Hmerge.html', sname=imid)
        else:

            flash('Your private key  Incorrect!')
            return render_template('HDecrypt.html')

@app.route("/mergeim", methods=['GET', 'POST'])
def mergeim():
    if request.method == 'POST':
        from PIL import Image
        conn = mysql.connector.connect(user='root', password='', host='localhost',
database='1SecureObjectdb')
        cursor = conn.cursor()
        cursor.execute("SELECT  *  FROM requesttb where  id='" + session["rhcid"] + "'")
        data = cursor.fetchone()

        if data:
            imid = data[5]
        else:
            return 'Incorrect username / password !'

        files = [
            "./static/Decrypt/" + imid + "_01.png",
            "./static/Decrypt/" + imid + "_02.png",
            "./static/Decrypt/" + imid + "_03.png",
            "./static/Decrypt/" + imid + "_04.png"]

        result = Image.new("RGB", (400, 400))

        for index, file in enumerate(files):
            path = os.path.expanduser(file)
            img = Image.open(path)
            img.thumbnail((200, 200), Image.ANTIALIAS)
```

```
            x = index // 2 * 200
            y = index % 2 * 200
            w, h = img.size
            print('pos {0},{1} size {2},{3}'.format(x, y, w, h))
            result.paste(img, (x, y, x + w, y + h))

        result.save(os.path.expanduser('static/merge/'+ imid +'.png'))
        from stegano import lsb
        clear_message = lsb.reveal('static/merge/'+ imid +'.png')

        mimage = 'static/merge/'+ imid +'.png'
        session['mimage'] = mimage

        print(clear_message)
        return render_template('HDView.html', iname=mimage, pre=clear_message)

@app.route("/hvdown", methods=['GET', 'POST'])
def hvdown():
    if request.method == 'POST':

        return send_file(session['mimage'], as_attachment=True)

def sendmsg(Mailid,message):
    import smtplib
    from email.mime.multipart import MIMEMultipart
    from email.mime.text import MIMEText
    from email.mime.base import MIMEBase
    from email import encoders

    fromaddr = "sampletest685@gmail.com"
    toaddr = Mailid

    # instance of MIMEMultipart
    msg = MIMEMultipart()
```

```
# storing the senders email address
msg['From'] = fromaddr

# storing the receivers email address
msg['To'] = toaddr

# storing the subject
msg['Subject'] = "Alert"

# string to store the body of the mail
body = message

# attach the body with the msg instance
msg.attach(MIMEText(body, 'plain'))

# creates SMTP session
s = smtplib.SMTP('smtp.gmail.com', 587)

# start TLS for security
s.starttls()

# Authentication
s.login(fromaddr, "hneucvnontsuwgpj")

# Converts the Multipart msg into a string
text = msg.as_string()

# sending the mail
s.sendmail(fromaddr, toaddr, text)

# terminating the session
s.quit()
```

APPENDIX B

SCREENSHOTS

Home Page

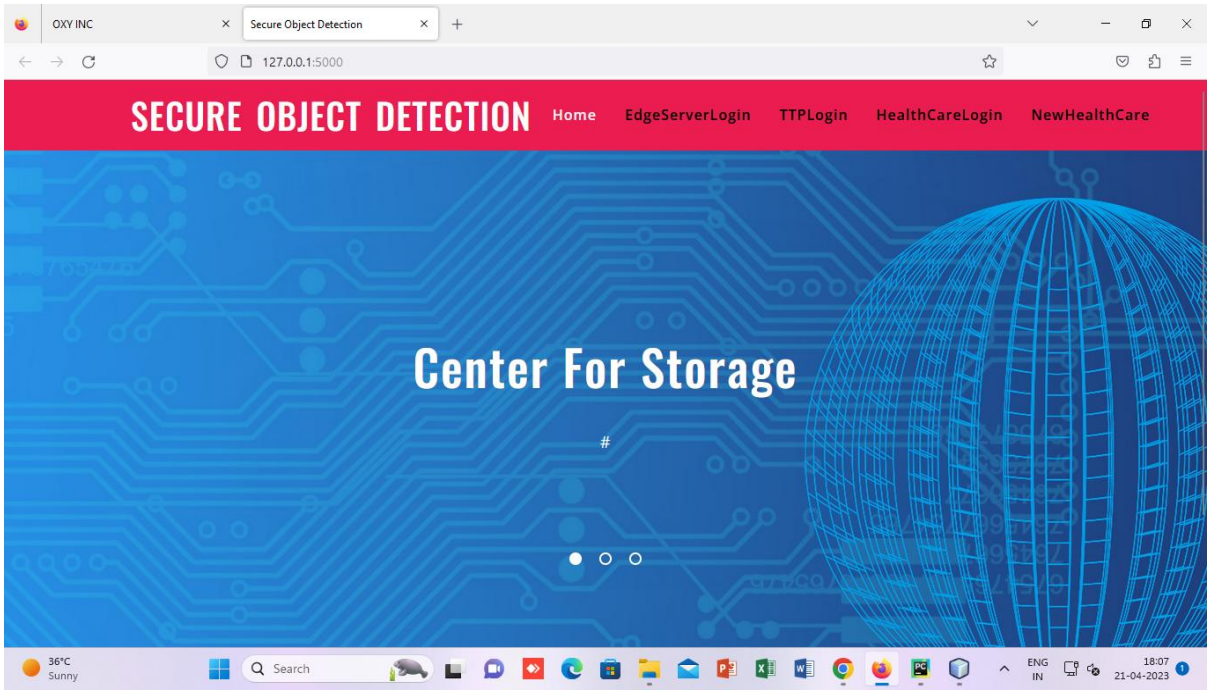


Fig B.1: Home Page

Admin Login

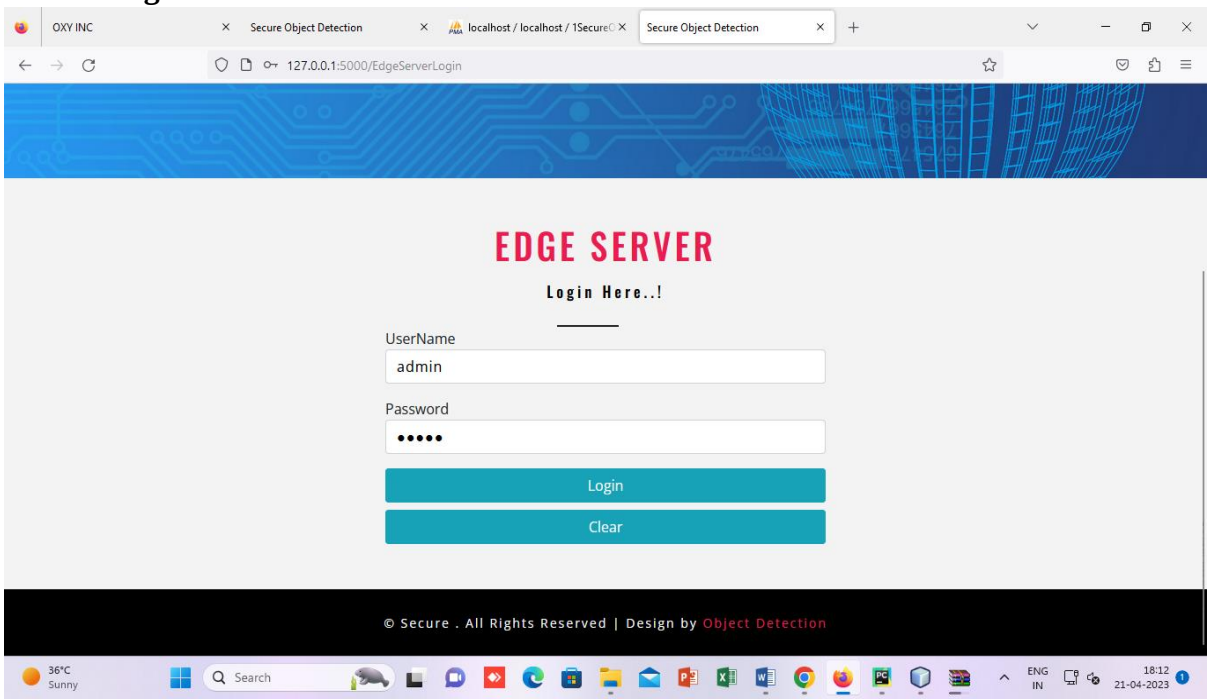


Fig B.2: Admin Login

Health Care Details

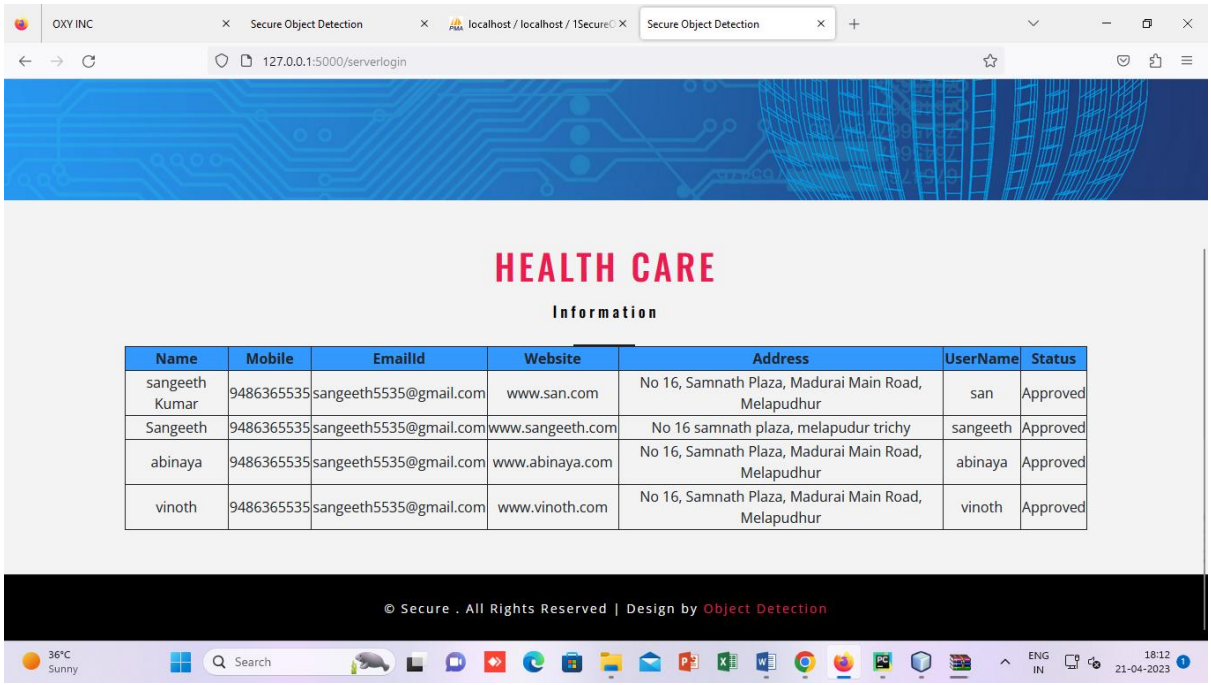


Fig B.3: Health Care Details

Patient Details

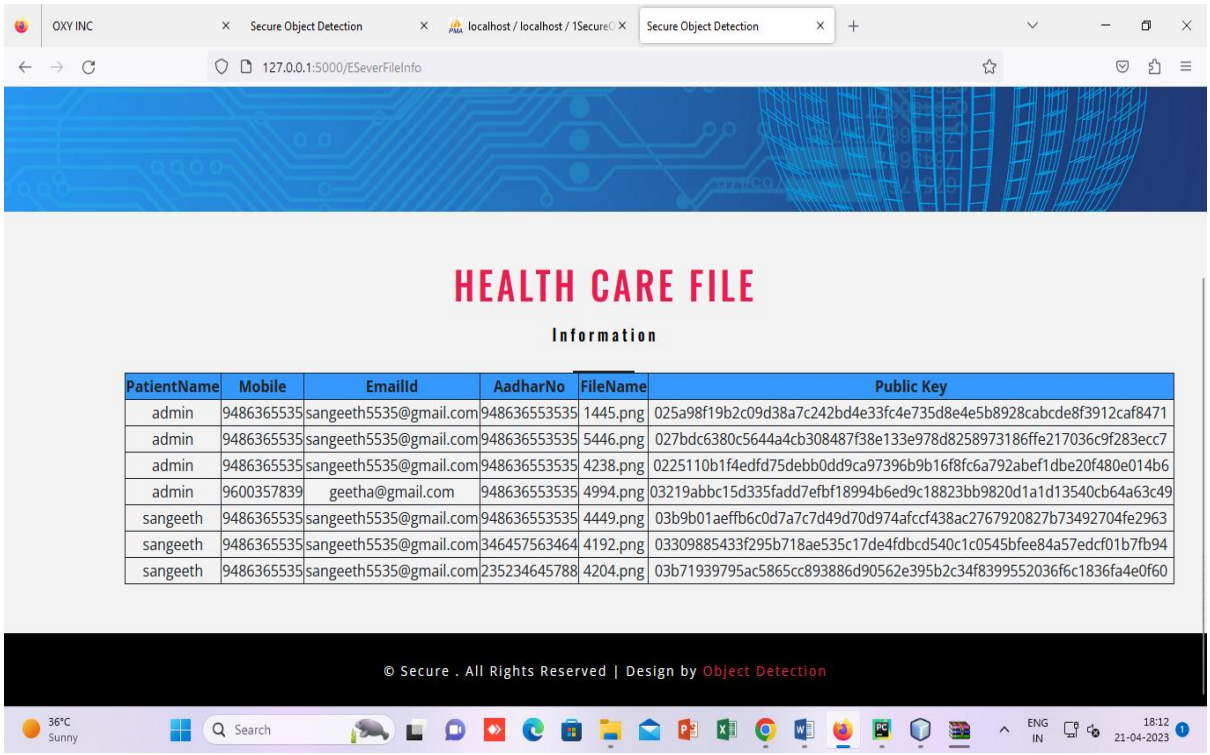


Fig B.4: Patient Details

Health Care Approval Details

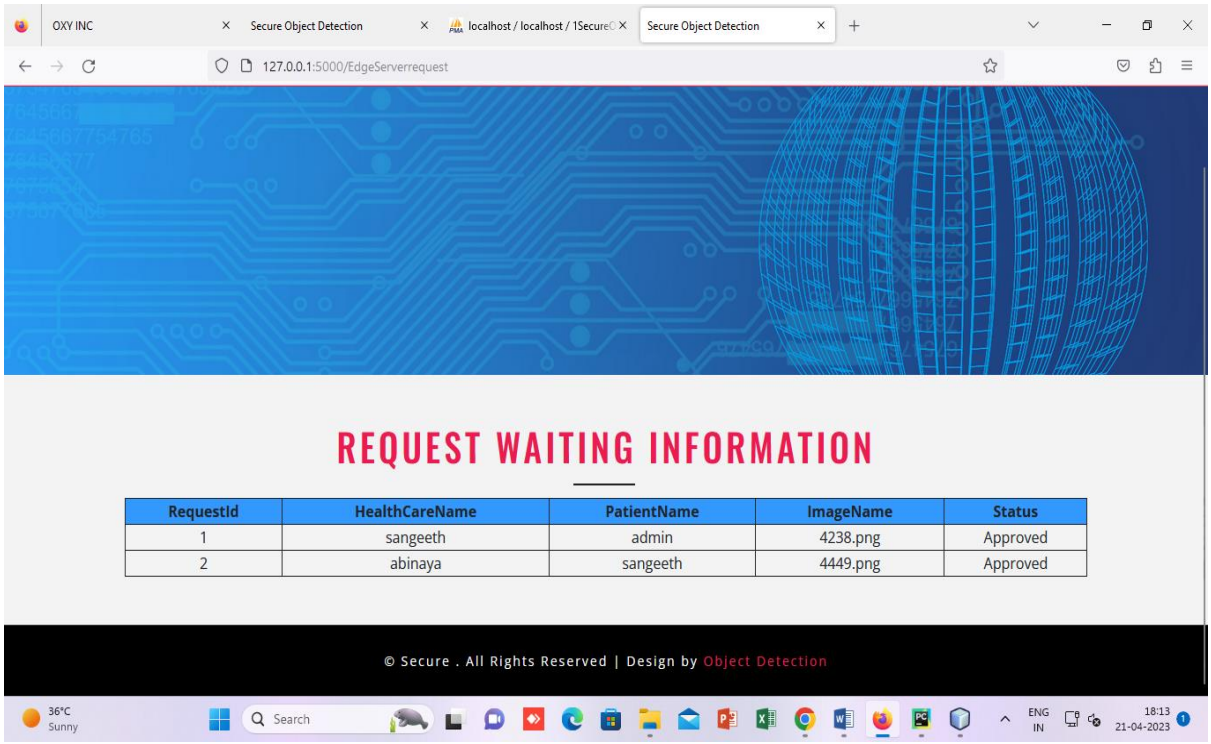


Fig B.5: Health Care Approval Details

Health Care Register

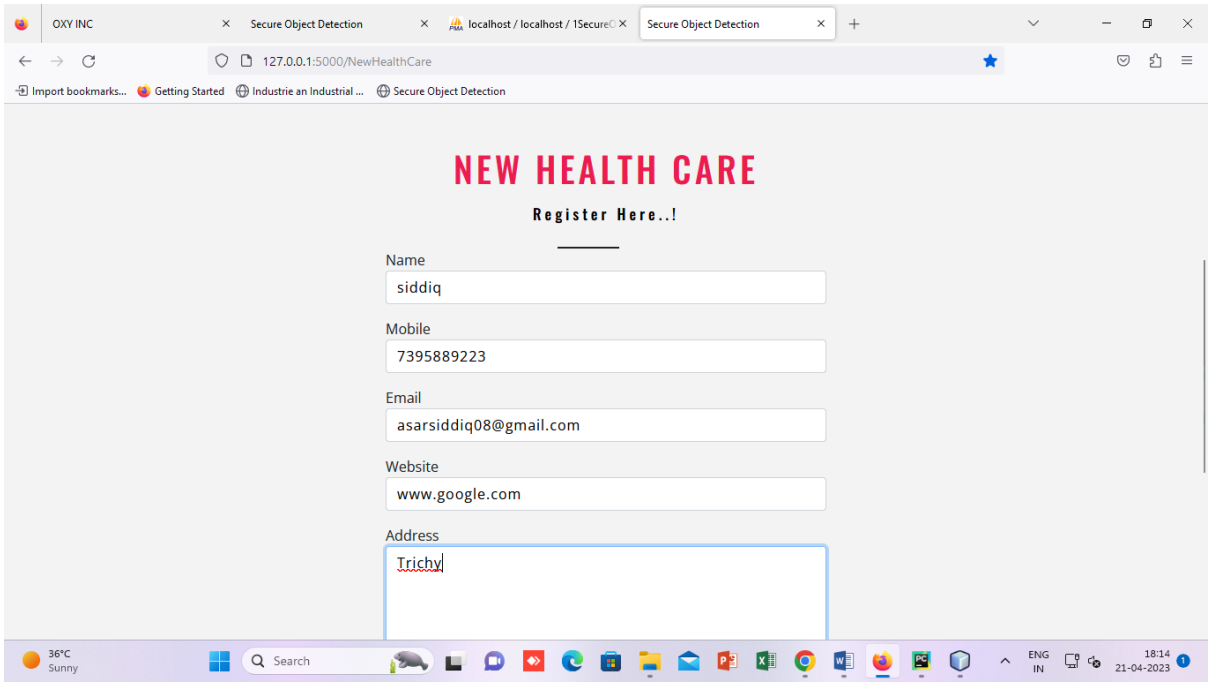


Fig B.6: Health Care Register

TTP Login

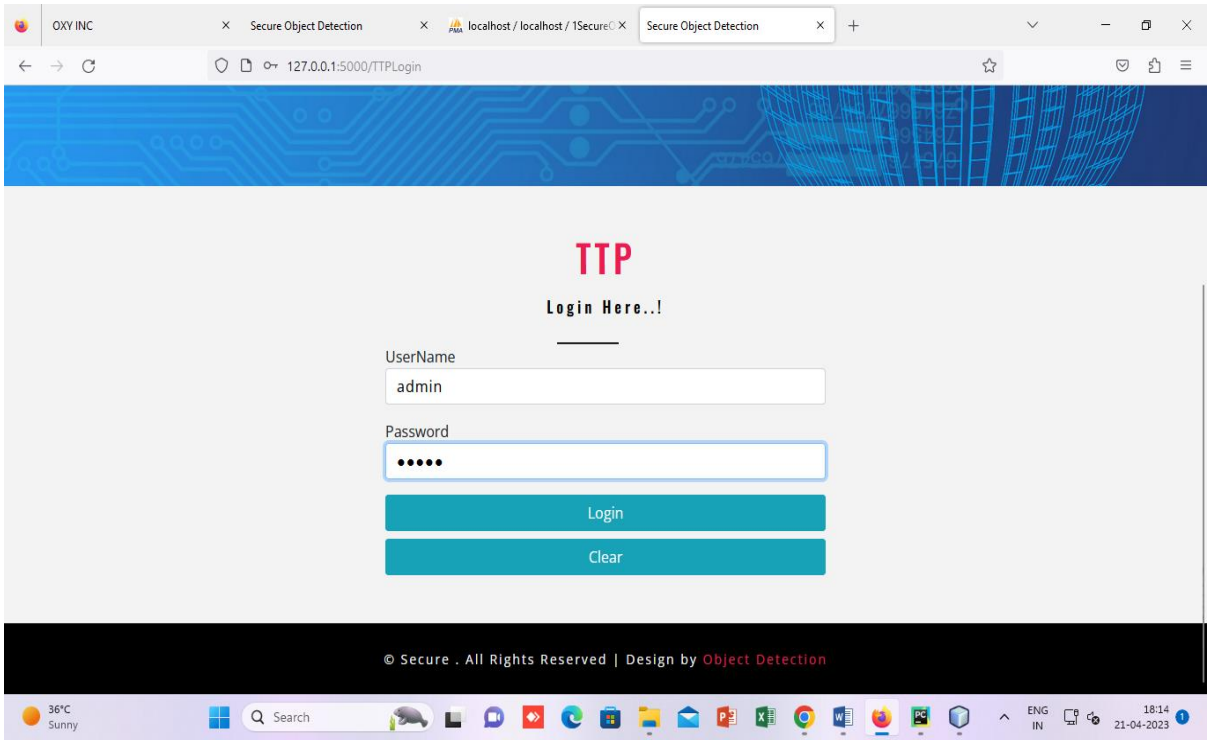


Fig B.7: TTP Login

Waiting for TTP Approval

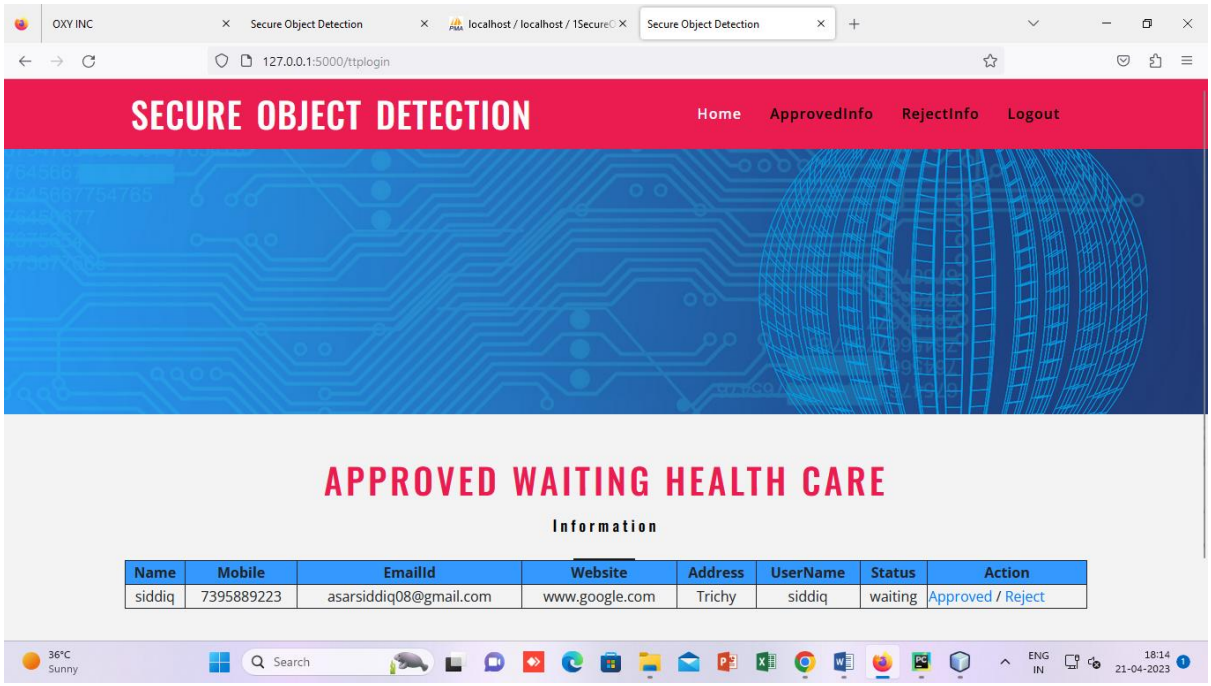


Fig B.8: Waiting for TTP Approval

Provide Approval

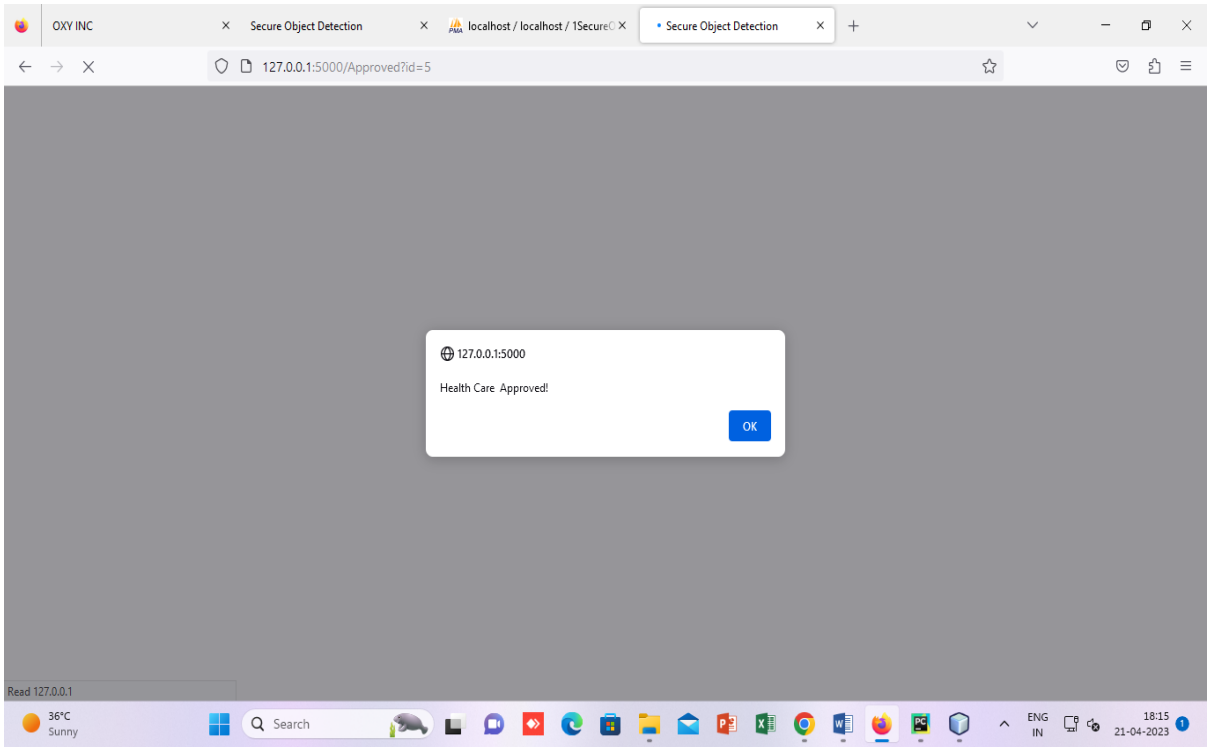
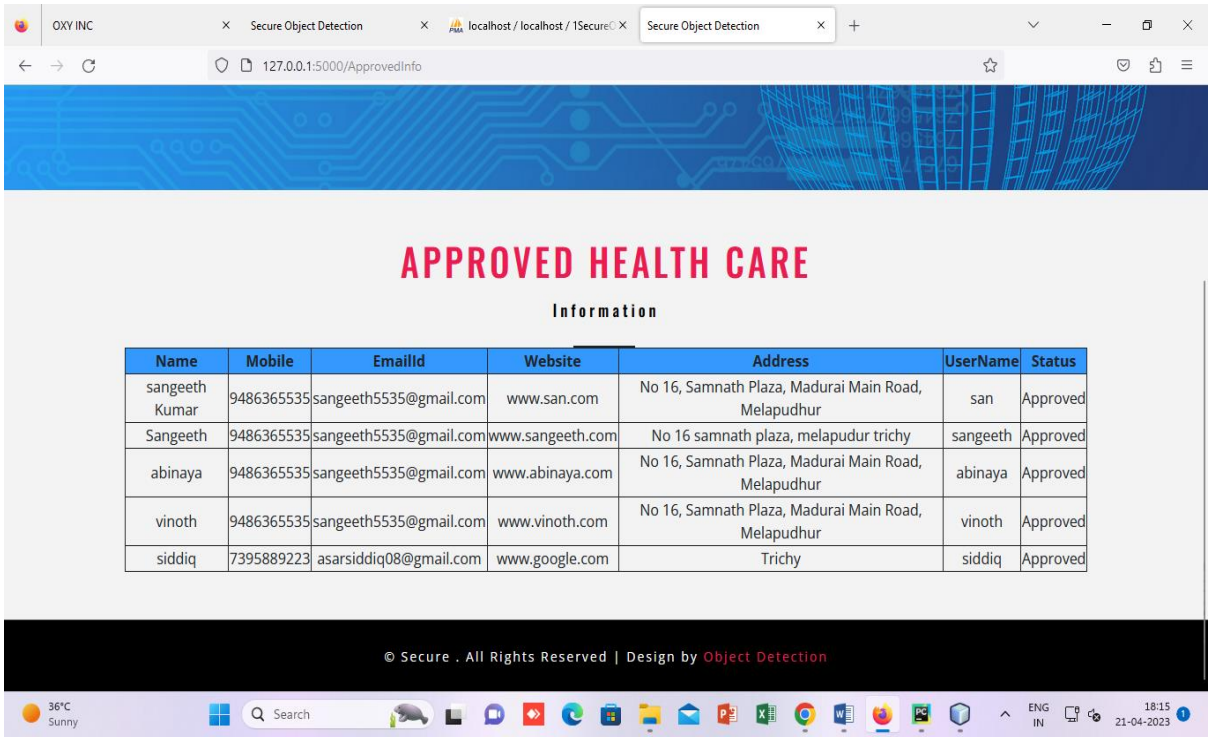


Fig B.9: Provide Approval

Approved Healthcare Details



Name	Mobile	EmailId	Website	Address	UserName	Status
sangeeth Kumar	9486365535	sangeeth5535@gmail.com	www.san.com	No 16, Samnath Plaza, Madurai Main Road, Melapudhur	san	Approved
Sangeeth	9486365535	sangeeth5535@gmail.com	www.sangeeth.com	No 16 samnath plaza, melapudur trichy	sangeeth	Approved
abinaya	9486365535	sangeeth5535@gmail.com	www.abinaya.com	No 16, Samnath Plaza, Madurai Main Road, Melapudhur	abinaya	Approved
vinoth	9486365535	sangeeth5535@gmail.com	www.vinoth.com	No 16, Samnath Plaza, Madurai Main Road, Melapudhur	vinoth	Approved
siddiq	7395889223	asarsiddiq08@gmail.com	www.google.com	Trichy	siddiq	Approved

Fig B.10: Approved Healthcare Details

Healthcare Login

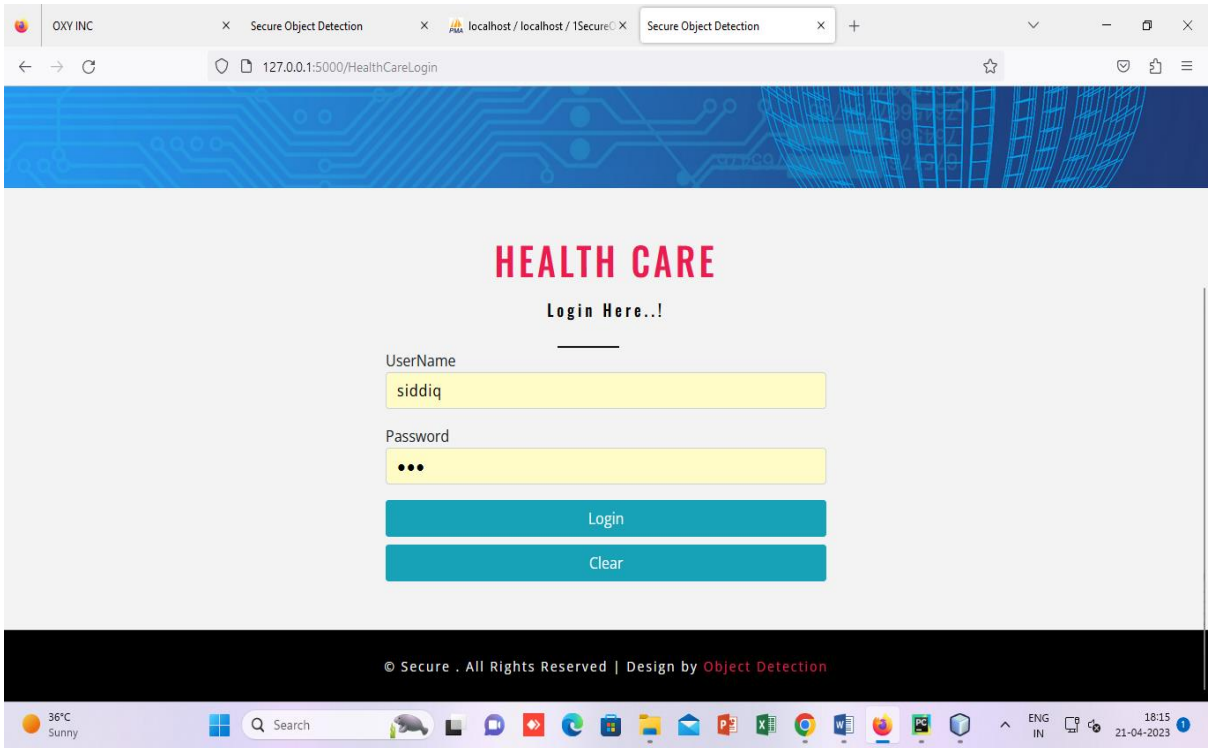


Fig B.11: Healthcare Login

View Approved Status

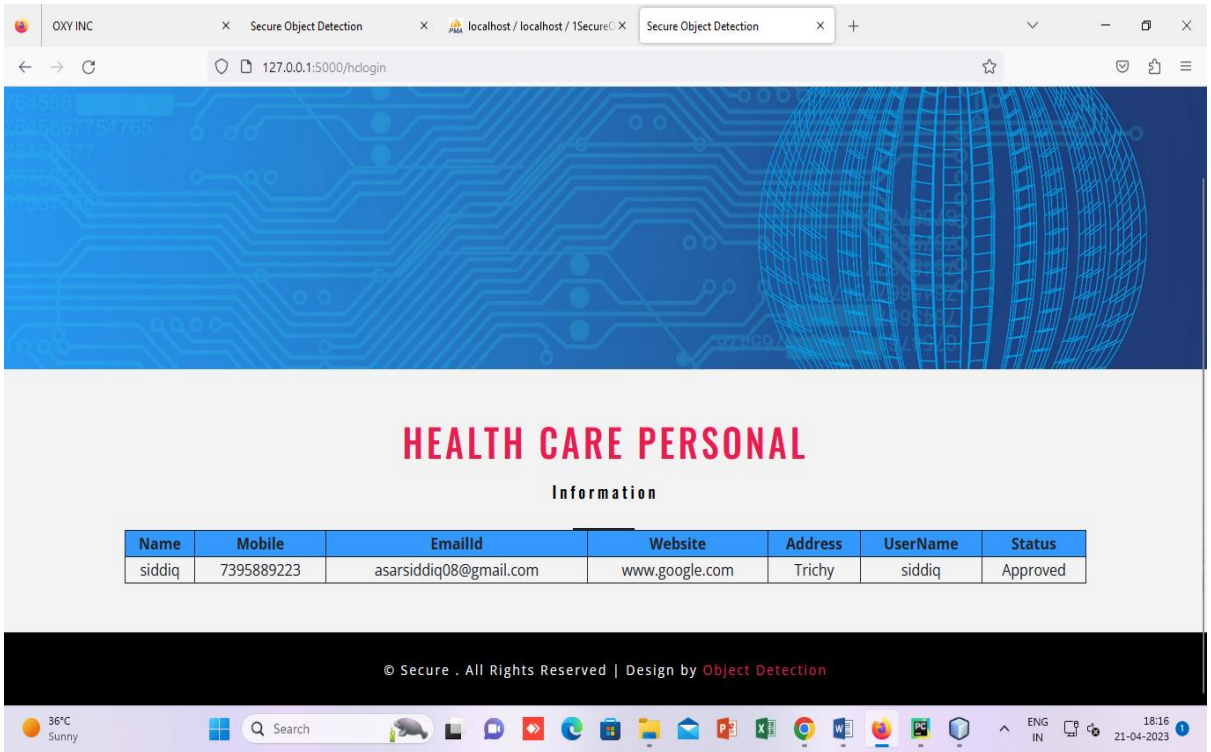


Fig B.12: View Approved Status

New Patient Register

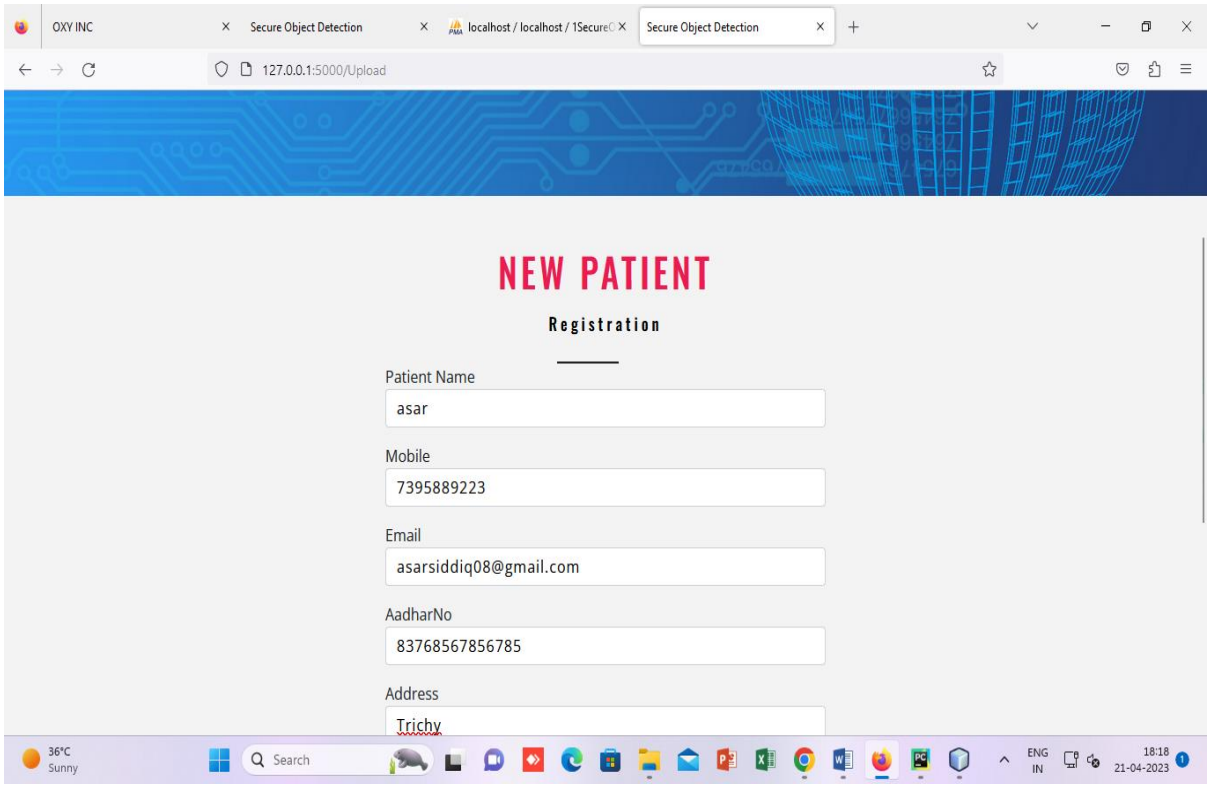


Fig B.13: New Patient Register

Upload Medical Image and Disease Prediction

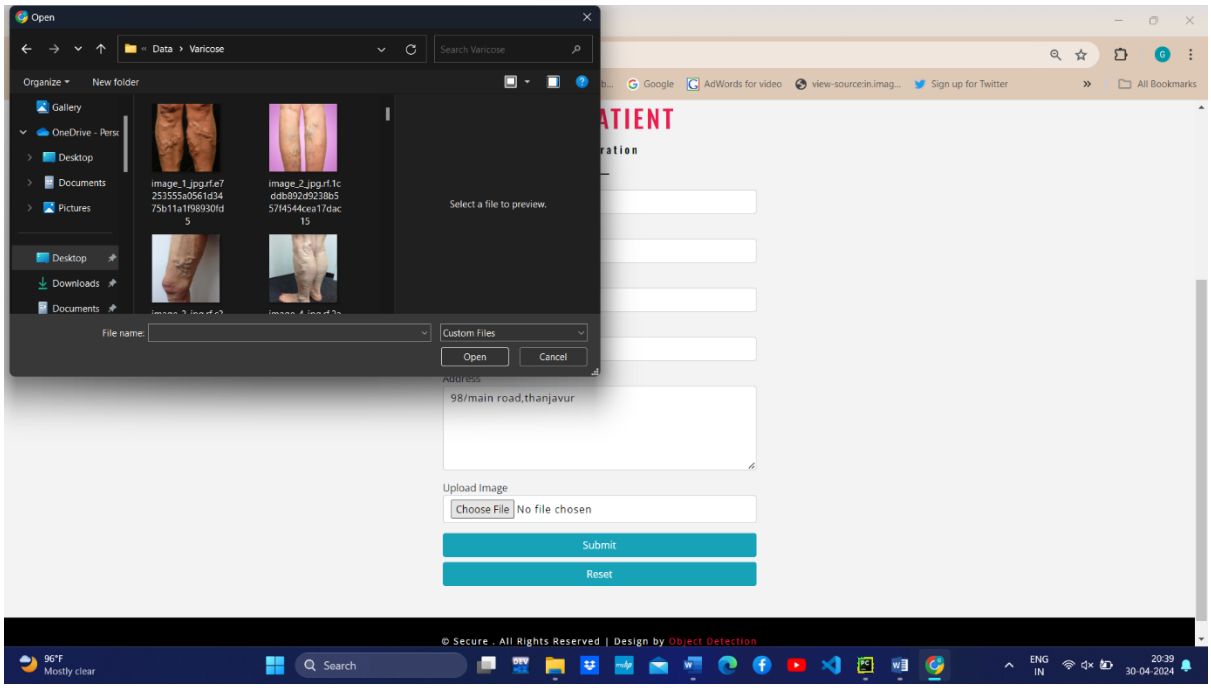


Fig B.14: Upload Medical Image and Disease Prediction

Patient Login

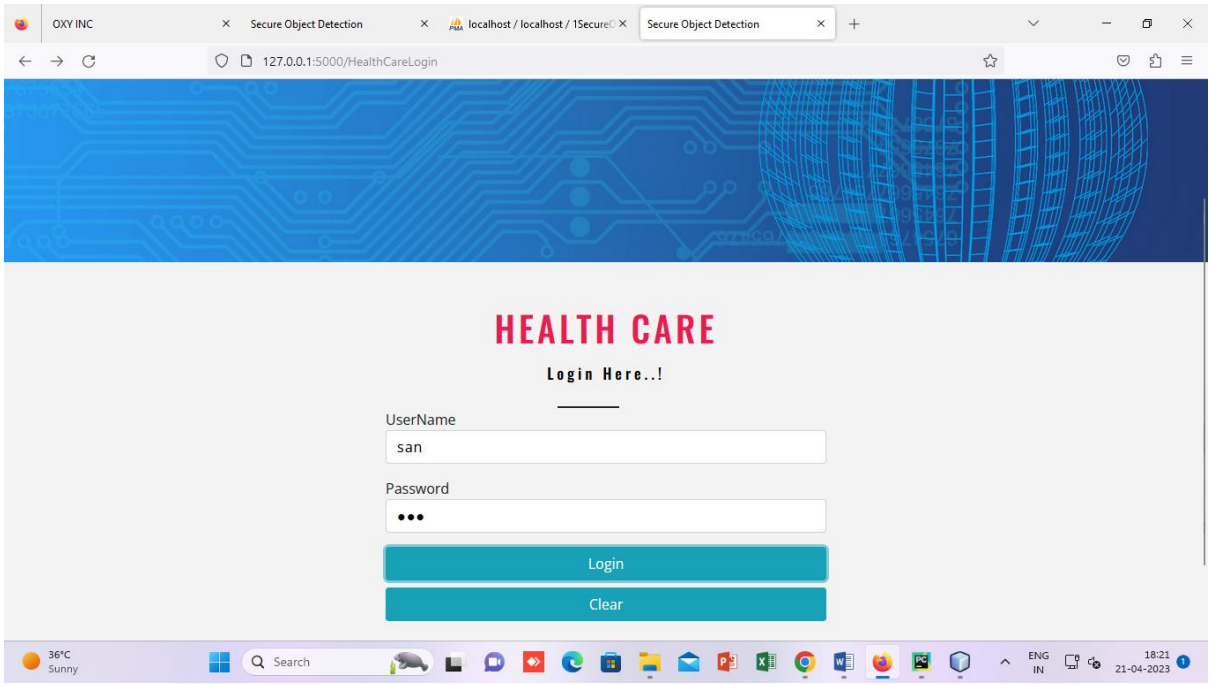
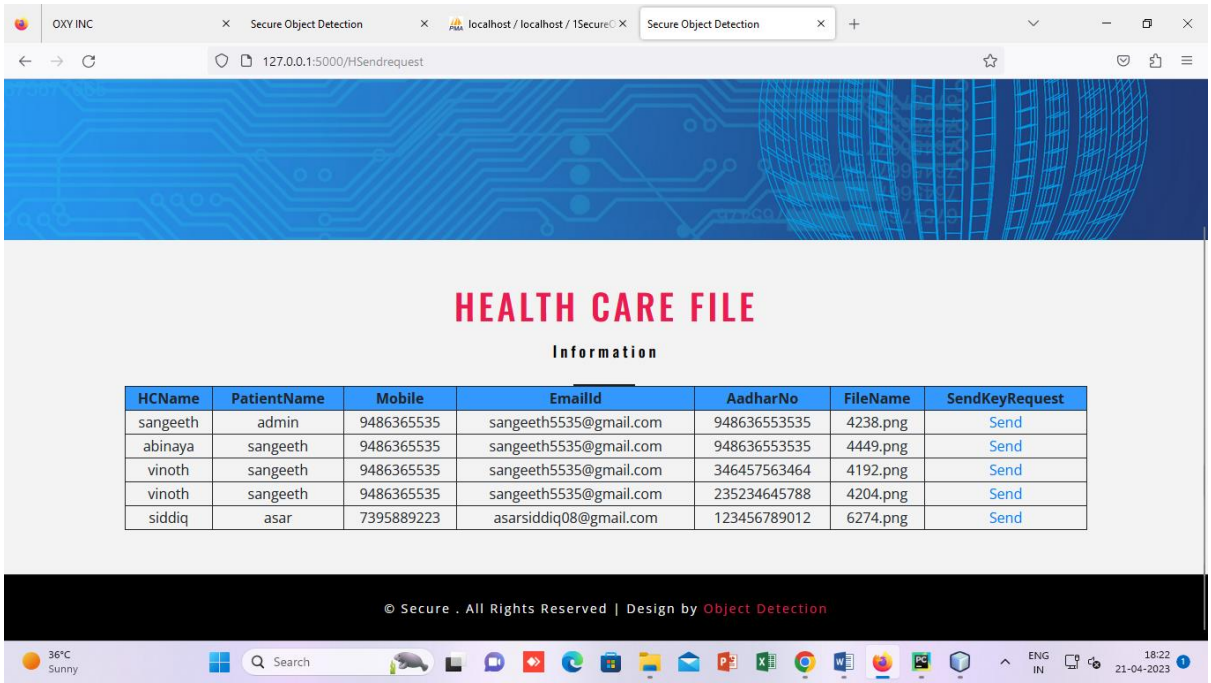


Fig B.15: Patient Login

Send Key Request



HCName	PatientName	Mobile	EmailId	AadharNo	FileName	SendKeyRequest
sangeeth	admin	9486365535	sangeeth5535@gmail.com	948636553535	4238.png	Send
abinaya	sangeeth	9486365535	sangeeth5535@gmail.com	948636553535	4449.png	Send
vinoth	sangeeth	9486365535	sangeeth5535@gmail.com	346457563464	4192.png	Send
vinoth	sangeeth	9486365535	sangeeth5535@gmail.com	235234645788	4204.png	Send
siddiq	asar	7395889223	asarsiddiq08@gmail.com	123456789012	6274.png	Send

Fig B.16: Send Key Request

Waiting for Key Permission

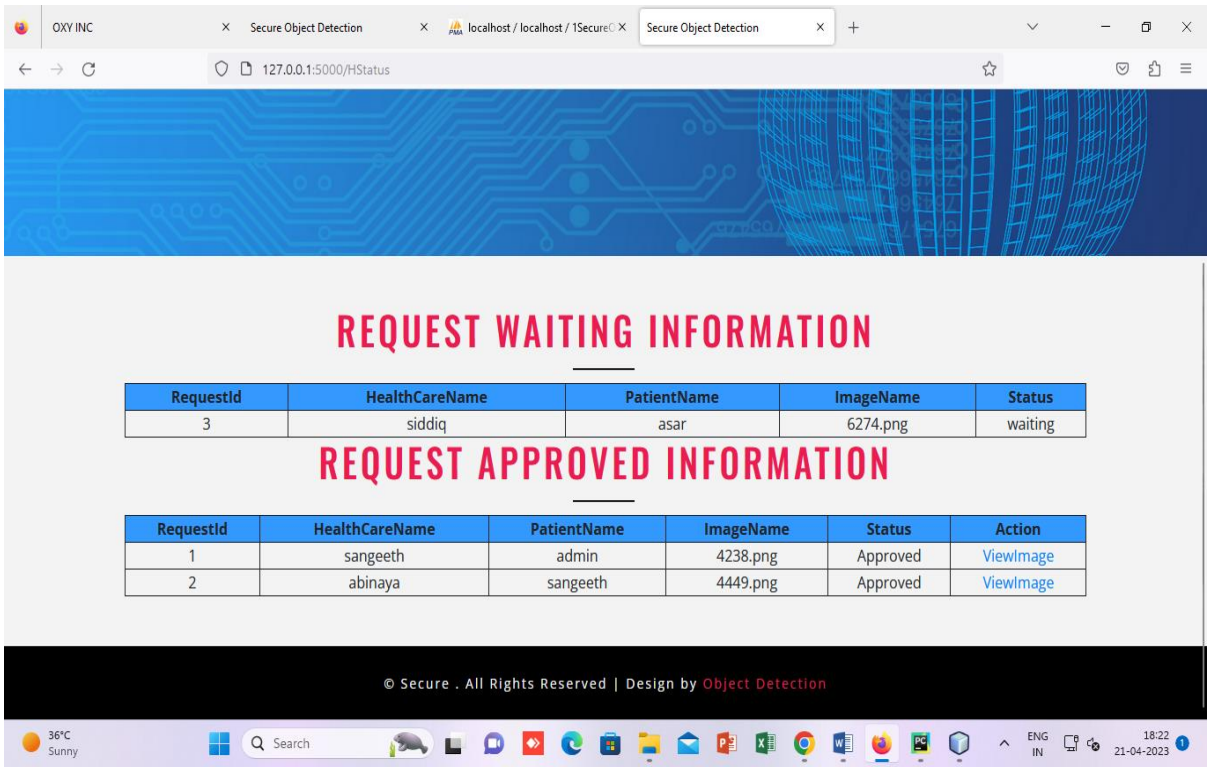


Fig B.17: Waiting for Key Permission

Healthcare Login

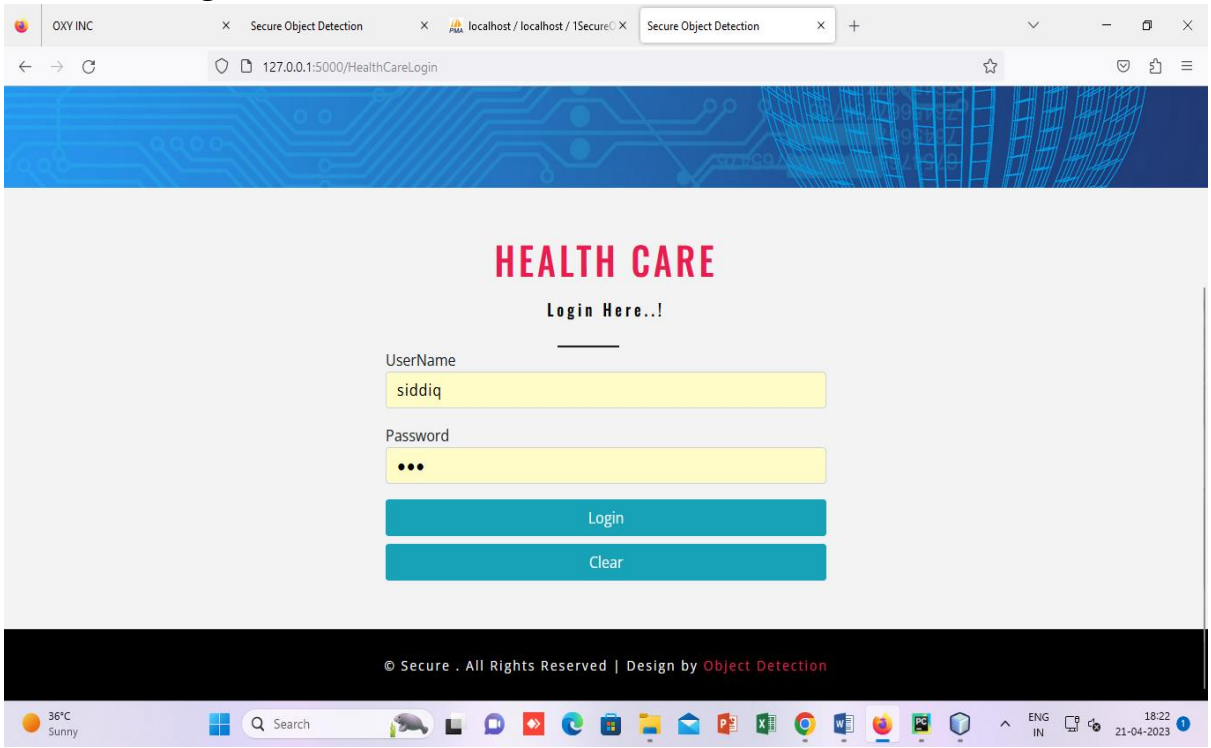


Fig B.18: Healthcare Login

Approval for Key Request

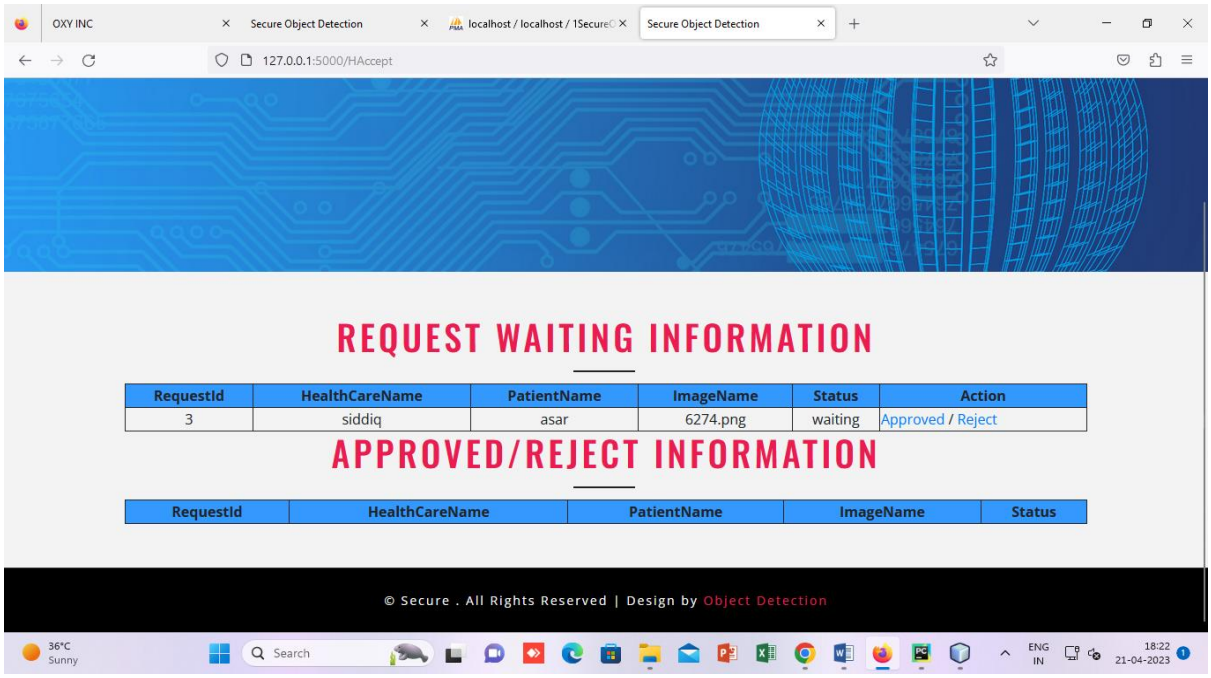


Fig B.19: Approval for Key Request

Secret Key Verification

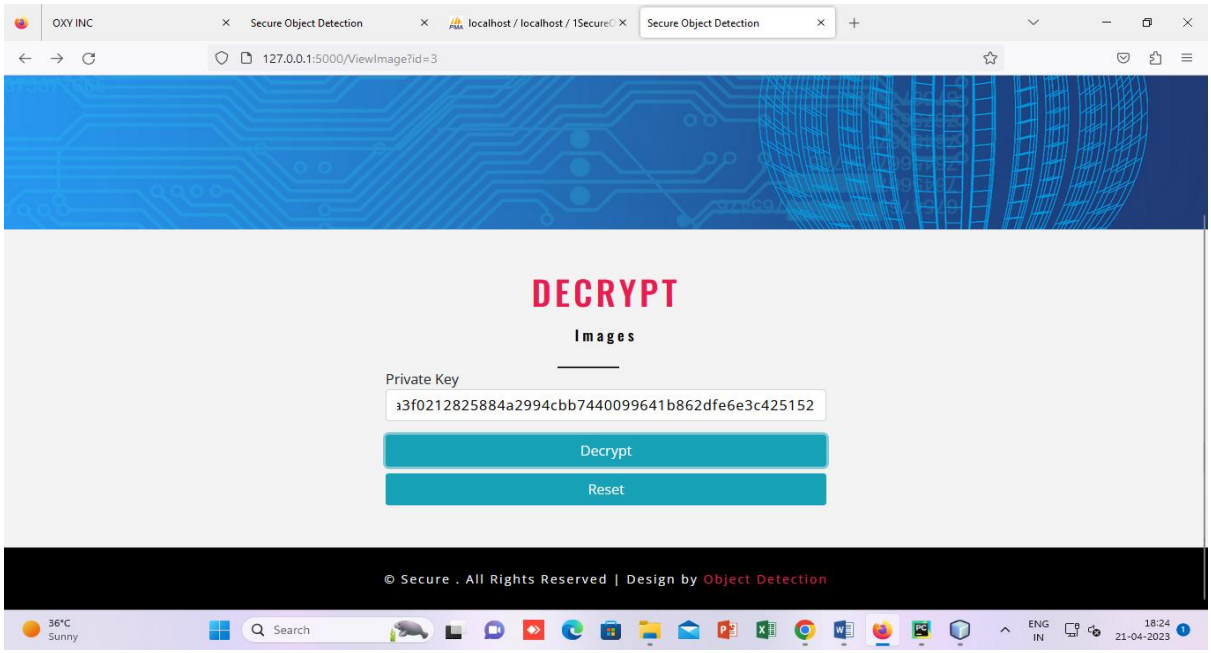


Fig B.20: Secret Key Verification

Image Shares Decryption

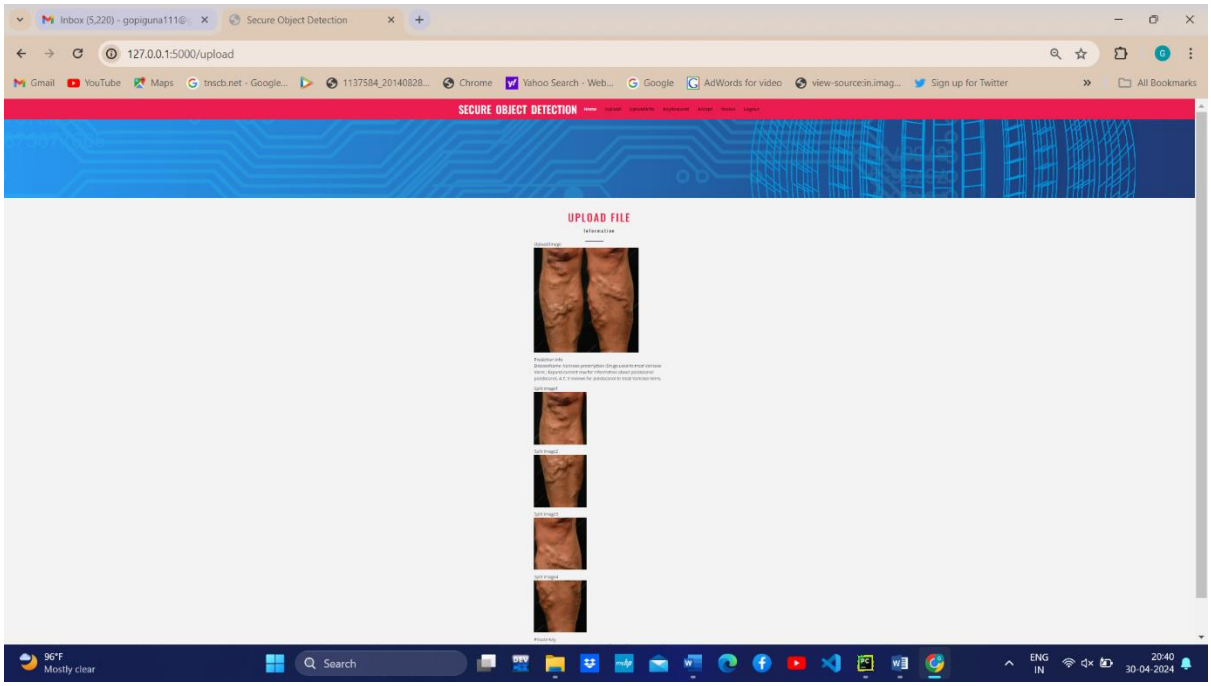


Fig B.21: Image Shares Decryption

Share Reconstruction and Medical Data Extraction

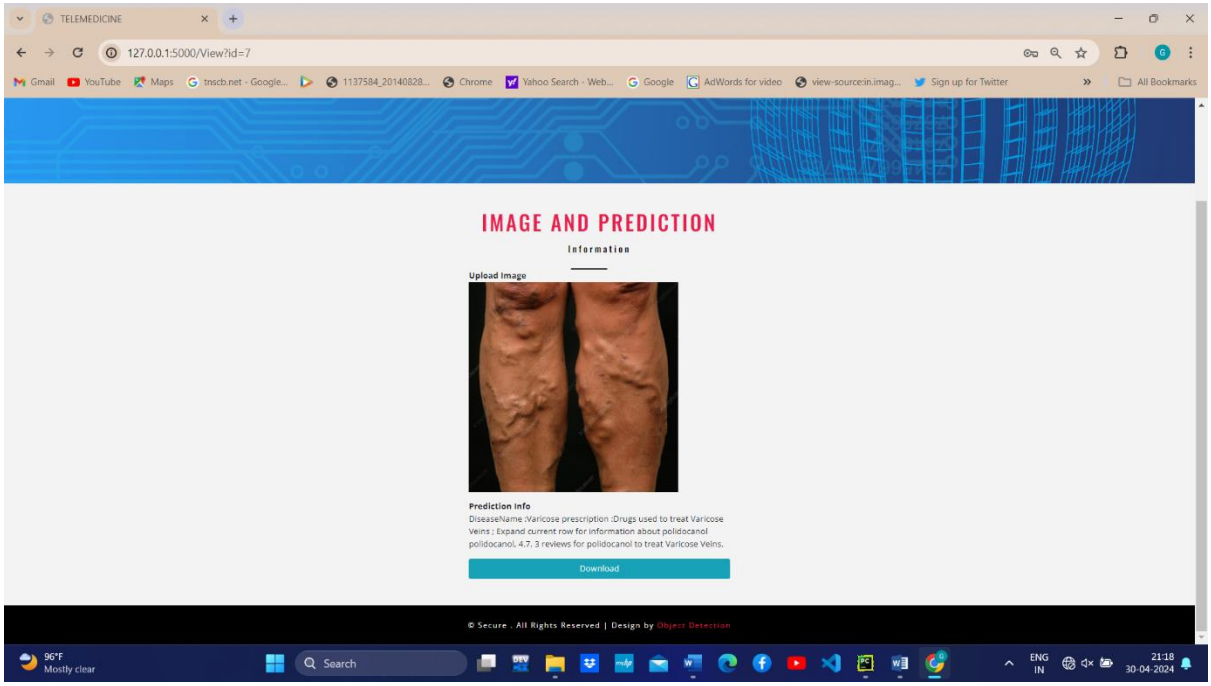


Fig B.22: Share Reconstruction and Medical Data Extraction

REFERENCES

[1] Machine Learning-Based Diagnosis of Chronic Venous Disorders Using Duplex Ultrasound Images" by Jiaqian Chen, Mengdi Gao, and Zhonghua Sun (Published in the IEEE Journal of Biomedical and Health Informatics, 2023)

[2] Endovenous Laser Ablation vs. Foam Sclerotherapy for Varicose Veins: A Systematic Review and Meta-analysis" by Elias T. Mobarak et al. (Published in the Journal of Vascular Surgery: Venous and Lymphatic Disorders, 2022)

[3] Masood, Fawad, Maha Driss, Wadii Boulila, Jawad Ahmad, Sadaqat Ur Rehman, Sana Ullah Jan, Abdullah Qayyum, and William J. Buchanan. "A lightweight chaosbased medical image encryption scheme using random shuffling and XOR operations." Wireless Personal Communications (2021): 1-28.

[4] Hasan, Mohammad Kamrul, Shayla Islam, Rossilawati Sulaiman, Sheroz Khan, Aisha-Hassan Abdalla Hashim, Shabana Habib, Mohammad Islam et al. "Lightweight encryption technique to enhance medical image security on internet of medical things applications." IEEE Access 9 (2021): 47731-47742.

[5] Aparna, Puvvadi, and Polurie Venkata Vijay Kishore. "Biometric_based efficient medical image watermarking in E_healthcare application." IET Image Processing 13, no. 3 (2019): 421-428.

[6] Kamal, Sara T., Khalid M. Hosny, Taha M. Elgindy, Mohamed M. Darwish, and Mostafa M. Fouda. "A new image encryption algorithm for grey and color medical images." IEEE Access 9 (2021): 37855-37865.

[7] Li, Xin, and Dongxiao Zhu. "Robust detection of adversarial attacks on medical images." In 2020 IEEE 17th International Symposium on Biomedical Imaging (ISBI), pp. 1154-1158. IEEE, 2020.

[8] Liu, Xiyao, Jieting Lou, Hui Fang, Yan Chen, Pingbo Ouyang, Yifan Wang, Beiji Zou, and Lei Wang. "A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images." Ieee Access 7 (2019): 76580-76598.

[9] Zhou, Yi, Xiaodong He, Lei Huang, Li Liu, Fan Zhu, Shanshan Cui, and Ling Shao. "Collaborative learning of semi-supervised segmentation and classification for medical

images." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 2079-2088. 2019.

[10] Li, Zhuoling, Minghui Dong, Shiping Wen, Xiang Hu, Pan Zhou, and Zhigang Zeng. "CLU-CNNs: Object detection for medical images." Neuro computing 350 (2019): 53-59.

[11] Deepika Princess D., Mohan Jagannath and Biju ShalvinY.J,"Ultrasound Therapy for Varicose Vein", International Research Journal of MedicalSciences, Vol.1(10), November(2013), no.1, 22-25.

[12] Gennady Victoro vich Savrasov, Nikita Vladimirovich Belikov, Alexander Vasilyevich Gavrilenko, Irina VitalyevnaKhaydukova, Anna SergeevnaBorde, Irina Alexandrovna Seliverstova, AnastasiyaDmitrievnaSolntseva "Comparison of Mechanical Parameters of the Great Saphenous Vein under Various Test Conditions", IEEE AACCESS(2019), no.2, 44-47.

[13] G.D.Parmar, NavdeepsinghV.Limbad "Vein Pattern Detection System Using Cost Effective Modified IR Sensitive Webcam", International Journal For Technolgical Research, Volume 1,issue 9, May2014, no.3.

[14] ManamMansoor, Sravani S.N, Sumbul Zahra Naqvi, Imran Badshah,"Real Time Low Cost Infrared Vein Imaging System" International conference on signal processing and pattern, IEEE 2013, no,4.

[15] Naomi Christianne Pereira, Jessica D'souza, Parth Rana, SupriyaSolaskar "OBESITY RELATED DISEASE PREDICTION FROM HEALTHCARE COMMUNITIES USING MACHINE LEARNING", IEEE – 45670, July 6-8, 2019, no.5.

[16] Ruizong Zhu , HuipingNiu , Ningning Yin , Tianjiao Wu, Yapei Zhao"Analysis of Varicose Veins of Lower Extremities Based on Vascular Endothelial Cell Inflammation Images and MultiScale Deep Learning", IEE ACCESS. 2019.2954708, Vol. 7, December 16, 2019, no.6.

[17] S. Prasantamrongsiri "3D finite element analysis of varicose vein therapy by using microwave ablation" Biomedical Engineering international conference ,2012, no.7.

[18] Thor Bechsgaard, Kristoffer Lindskov Hansen, Andreas Hjelm Brandt, Simon Holbek "Blood Flow Velocity in the Popliteal Vein using Transverse Oscillation Ultrasound ", Proc of SPIE Vol.9790 979003-1, no.8.

[19] M-C Nogaro, D J Pournaras, C Prasannan, A Chaudhuri. Varicose vein. BMJ 2012;344:e667 .

[20] Franz A, Wann Hansson C. Patients' experiences of living with varicose veins and management of the disease in daily life. J clinNurs 2016;25(5-6):733-41

[21] Cardia G, Catalano G, Rosafio I, Granatiero M, De Fazio M. Recurrent varicose veins of the legs. Analysis of a social problem; GChir 2012;33(11-12): 450-4.

[22] National Clinical guidelines centre. Varicose veins in legs: The diagnosis and management of varicose veins; Commissioned by the National Institute for Health and Care Excellence. July 2013.

[23] Kohno K et al. Standing posture at work and overweight exacerbate varicose veins: Shimane CoHRE Study. J Dermatol 2014;41(11):964-8.

[24] LesiakMR,Brêborowicz GH KasperczakJ.Risk factors for the development of venous insufficiency of the lower limbs during pregnancy. Ginekol Pol 2012;83(12).

[25] Ahti TM, Makivaara LA, Luukkaala T, Hakama M, LaurikkaJo.Lifestyle factors and varicose veins: does cross-sectional design result in underestimate of the risk. Phlebology 2010;25(4):201-6.

CONFERENCE CERTIFICATES

DHANALAKSHMI SRINIVASAN
COLLEGE OF ENGINEERING
COIMBATORE – 641 105
www.dsce.ac.in

INTERNATIONAL CONFERENCE ON
EMERGING TRENDS IN FUTURE ENGINEERING' 24
(ICETFE' 24)

CERTIFICATE

This is to certify that ~~Prof.~~ / ~~Dr.~~ / ~~Mr.~~ / Ms. GOPIKA G

Department of COMPUTER SCIENCE AND ENGINEERING from K.RAMAKRISHNAN COLLEGE OF TECHNOLOGY, TRICHY has presented a paper titled HARNESSING VARICOSE VEINS USING IMAGE VIA PROCESSING VIA CRYPTOGRAPHY in the International Conference on Emerging Trends in Future Engineering' 24 (ICETFE' 24) held on 25.04.2024

DEAN ACADEMIC
(Dr. K. Baghirathi)

PRINCIPAL
(Dr. C. Jegadheesan)

Organized by
Departments of AI & DS, AGRI, BME, Civil, CSE, ECE, EEE, FT & MECH

In association with
IEEE, ISTE, IETE, ISME, ICI & CSI

DHANALAKSHMI SRINIVASAN COLLEGE OF ENGINEERING

COIMBATORE – 641 105

www.dsce.ac.in

INTERNATIONAL CONFERENCE ON EMERGING TRENDS IN FUTURE ENGINEERING' 24 (ICETFE' 24)

CERTIFICATE

This is to certify that ~~Prof.~~ / ~~Dr.~~ / ~~Mr.~~ / Ms. KAMYARASI S

Department of COMPUTER SCIENCE AND ENGINEERING from K.RAMAKRISHNAN COLLEGE OF TECHNOLOGY, TRICHY has presented a paper titled HARNESSING VARICOSE VIENS USING IMAGE PROCESSING VIA CRYPTOGRAPHY in the International Conference on Emerging Trends in Future Engineering' 24 (ICETFE' 24) held on 25.04.2024

DEAN ACADEMIC
(Dr. K. Baghirathi)

PRINCIPAL
(Dr. C. Jegadheesan)

Organized by
Departments of AI & DS, AGRI, BME, Civil, CSE, ECE, EEE, FT & MECH

In association with
IEEE, ISTE, IETE, ISME, ICI & CSI

DHANALAKSHMI SRINIVASAN COLLEGE OF ENGINEERING

COIMBATORE – 641 105

www.dsce.ac.in

INTERNATIONAL CONFERENCE ON EMERGING TRENDS IN FUTURE ENGINEERING' 24 (ICETFE' 24)

CERTIFICATE

This is to certify that ~~Prof.~~ / ~~Dr.~~ / ~~Mr.~~ / Ms. KEERTHIGA B

Department of COMPUTER SCIENCE AND ENGINEERING from K. RAMAKRISHNAN COLLEGE OF TECHNOLOGY, TRICHY has presented a paper titled HARNESSING VARICOSE VEINS USING IMAGE PROCESSING VIA CRYPTOGRAPHY in the International Conference on Emerging Trends in Future Engineering' 24 (ICETFE' 24) held on 25.04.2024

DEAN ACADEMIC
(Dr. K. Baghirathi)

PRINCIPAL
(Dr. C. Jegadheesan)

Organized by
Departments of AI & DS, AGRI, BME, Civil, CSE, ECE, EEE, FT & MECH

In association with
IEEE, ISTE, IETE, ISME, ICI & CSI

DHANALAKSHMI SRINIVASAN COLLEGE OF ENGINEERING

COIMBATORE – 641 105

www.dsce.ac.in

INTERNATIONAL CONFERENCE ON EMERGING TRENDS IN FUTURE ENGINEERING' 24 (ICETFE' 24)

CERTIFICATE

This is to certify that ~~Prof.~~ / ~~Dr.~~ / ~~Mr.~~ / Ms. LATCHAYA G from Department of COMPUTER SCIENCE AND ENGINEERING, K. RANGARAJAN COLLEGE OF TECHNOLOGY, TRICHY has presented a paper titled HARNESSING VARICOSE VEINS USING IMAGE PROCESSING VIA CRYPTOGRAPHY in the International Conference on Emerging Trends in Future Engineering' 24 (ICETFE' 24) held on 25.04.2024

DEAN ACADEMIC
(Dr. K. Baghirathi)

PRINCIPAL
(Dr. C. Jegadheesan)

Organized by
Departments of AI & DS, AGRI, BME, Civil, CSE, ECE, EEE, FT & MECH

In association with
IEEE, ISTE, IETE, ISME, ICI & CSI