RSET
RAJAGIRI SCHOOL OF
ENGINEERING & TECHNOLOGY
(AUTONOMOUS)

Project Report On

Finger vein authentication using Blockchain

Submitted in partial fulfillment of the requirements for the award of the degree of

Bachelor of Technology

in

Computer Science and Engineering

By

Saira Sunny George (U2103187)

Therese Joe (U2103207)

Thomas Biju (U2103208)

Thomas John (U2103209)

Under the guidance of

Ms. Amitha Mathew

Department of Computer Science and Engineering
Rajagiri School of Engineering & Technology (Autonomous)
(Parent University: APJ Abdul Kalam Technological University)
Rajagiri Valley, Kakkanad, Kochi, 682039
April 2025

CERTIFICATE

This is to certify that the project report entitled ***"Finger vein authentication using Blockchain"*** *is a bonafide record of the work done by* ***Saira Sunny George (U2103187), Therese Joe (U2103207), Thomas Biju (U2103208), Thomas John (U2103209)****, submitted to the Rajagiri School of Engineering & Technology (RSET) (Autonomous) in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology (B. Tech.) in "Computer Science and Engineering" during the academic year 2024-2025.*

Ms. Amitha Mathew
Project Guide
Assistant Professor
Dept. of CSE
RSET

Ms. Sangeetha Jamal
Project Coordinator
Assistant Professor
Dept. of CSE
RSET

Dr. Preetha K. G.
Head of the Department
Dept. of CSE
RSET

Vision of CSE

To become a Centre of Excellence in Computer Science & Engineering, moulding professionals catering to the research and professional needs of national and international organizations.

Mission of CSE

To inspire and nurture students, with up-to-date knowledge in Computer Science & Engineering, Ethics, Team Spirit, Leadership Abilities, Innovation and Creativity to come out with solutions meeting the societal needs.

Programme Educational Objectives (PEOs)

- **PEO1:** Graduates shall have up-to-date knowledge in Computer Science & Engineering along with interdisciplinary and broad knowledge on mathematics, science, management and allied engineering to become computer professionals, scientists and researchers.
- **PEO2:** Graduates shall excel in analysing, designing and solving engineering problems and have life-long learning skills, to develop computer applications and systems, resulting in the betterment of the society.
- **PEO3:** Graduates shall nurture team spirit, ethics, social values, skills on communication and leadership, enabling them to become leaders, entrepreneurs and social reformers.

ACKNOWLEDGMENT

I wish to express my sincere gratitude towards **Rev. Dr. Jaison Paul Mulerikkal CMI**, Principal of RSET, and **Dr. Preetha K. G.** , Head of the Department of Computer Science and Engineering for providing me with the opportunity to undertake my project, "Finger vein authentication using Blockchain".

I am highly indebted to my project coordinator, **Ms. Sangeetha Jamal**, Assistant Professor, Department of Computer Science and Engineering for her valuable support.

It is indeed my pleasure and a moment of satisfaction for me to express my sincere gratitude to my project guide **Ms. Amitha Mathew** for her patience and all the priceless advice and wisdom she has shared with me.

Last but not the least, I would like to express my sincere gratitude towards all other teachers and friends for their continuous support and constructive ideas.

Saira Sunny George

Therese Joe

Thomas Biju

Thomas John

Abstract

Due to the increased demand for secure identity verification, most conventional biometric authentication systems suffer from severe problems in data security and privacy. Therefore, this paper proposes a low-cost biometric authentication framework with finger vein-based authentication empowered by blockchain that provides high security and reliability. It captures unique vein patterns of each user's finger using NIR imaging an LED circuit, and an infrared-modified webcam for capturing high-quality images in a controlled environment.

The proposed encryption is initiated by taking some pictures that will then be encrypted on a trusted local computer through the underlying blockchain-based encryption mechanism. This, followed by data sending over to the cloud server, decryption may take place. In addition, CNN-ResNet architecture-based feeding allows image-based verification against vein data in pre-training. Verification through the usage of smart contracts ensures it securely without tampering or interference, which maintains complete transparency in this regard.

After verification, the authentication response is returned to the client device, which is provided with a user-friendly interface, such as a GUI-based app or web application. The solution merges security and immutability due to blockchain with precision provided by CNN-based biometric verification and is an affordable, highly secure way of managing identity in a reliable manner.

Contents

List of Abbreviations

- Resnet - Residual Network
- NIR - Near Infrared
- CCD - Charged Coupled Camera
- PIN - Personal Identification Number
- CLAHE - . Contrast Limited Adaptive Histogram Equalization
- EER - Equal Error Rate

List of Figures

List of Tables

Chapter 1

Introduction

In this day and age, when technological platforms are more relied upon than ever, privacy preservation is of utmost importance. Security measures like passwords, PINS, and rudimentary biometrics now stand challenged. Security circumvention, data breaches and system hacks are some of the many threats gripping these authentication measures. Thus, there arises an increasing demand for the user-friendliness and the robustness of the convincing identity verification mechanism. Authentication by physiological features has been put forth as an option, whereby a person's finger print, eye iris patterns, and even face images which can all act as security keys opening door to various advancements, for example, systems where a person scans their fingers are available now. Out of the above mentioned systems, scanning finger veins proves to be the most ideal, being impossible to imitate as each individual possesses unique biological characteristics.

Finger vein recognition utilizes NIR technologies to obtain the unique feature patterns that exist within an individual's finger. It serves as an internal biometric which is unique and very difficult to forge. The vein patterns obtained are converted into templates and stored. These templates are used for identity verification where the degree of accuracy is very high. The security is further improved in this research by adding a blockchain component to the system. A blockchain is a decentralized and immutable ledger system that has its own privacy protection. Encrypting the vein data on a trusted local device and saving it on a blockchain guarantees a secure, transparent and permanent biometric identity management system.

1.1 Background

As digital platforms expand across personal, financial and government applications, secure authentication has become a cornerstone of digital identity management. Conventional authentication techniques, such as passwords , are increasingly vulnerable to security breaches, including phishing, brute-force attacks, and data leaks. Biometrics has emerged as an effective solution that provides more reliable authentication using unique biometric traits such as fingerprints, facial features, and iris patterns. However, many of these biometric modalities are subject to limitations in terms of privacy, vulnerability to spoofing, and environmental sensitivity, leading to the exploration of alternative biometric methods that can address these issues more effectively.

With the development of platforms in the fields of personal and financial services, as well as the e-government, the safety of authentication has turned into the most important single factor in the management of digital identities. The conventional authentication techniques, passwords for example, have been and continue to be more susceptible to a wide range of breaches such as phishing, brute force attack and data leaks. An effective solution to this problem that gives a more trustworthy authentication is biometrics that uses unique biometric traits such as a person‘s fingerprint, facial structures and iris patterns. Many of these bio metric modalities unfortunately have privacy, spoofing vulnerability and environment sensitivity constraints which have made the adoption of other biometric technologies that may solve these challenges more suitable.

For safe systems, finger vein patterns are beginning to be seen as an appealing biometric modality. It is common knowledge that vascular features such as finger veins are unique to an individual and near impossible to forge or change. Vascular patterns on fingers are treated by this technique, which makes use of NIR technology , and generates a biometric template of the person. Also, since veins are embedded in the skin, they are not as easily scratched as fingerprints and thus not as easily faked.

1.2 Problem Definition

The increasing instances of digital identity theft and unauthorized access pose the need for a secure, reliable, and non-invasive authentication system. This project aims to develop a biometric-based authentication framework using finger vein recognition, integrated with blockchain technology to ensure data integrity, improve security, and protect user privacy.

1.3 Scope and Motivation

The objective of this project is to develop a digital security system using biometric technology. The developed biometric system recognizes the finger veins and is based on blockchain technology. The images of the finger veins will be taken by means of finger-vein capturing device, which will locally encrypt them before transferring them to a blockchain framework for safe storage. A pre-trained convolutional neural network, a ResNet model, will validate the captured Vein images against the stored templates, thus enabling the correct identity verification. The decentralized blockchain ledger and smart contracts shall handle the security and authentication processes, thus allowing tamper-proof data storage and an automated, trustless verification process. The major scope of this project would involve the development, implementation, and testing of the complete authentication framework with regard to data acquisition, encryption, cloud-based processing, and client-side response.

The motivation behind this project arises from the growing need for secure, privacy-focused authentication methods in an era of increased digital identity theft and data breaches. Traditional authentication methods and even some biometric approaches are vulnerable to forgery and environmental interference, while data privacy concerns remain high. Finger vein recognition presents an effective alternative due to its internal, tamper-resistant nature and high accuracy. Additionally, the integration of blockchain technology addresses privacy and security concerns by creating a transparent and immutable data handling process. This combination offers a promising solution for secure identity management, meeting the needs of applications where privacy, accuracy, and security are critical, from financial services to healthcare and governmental access control.

1.4 Objectives

- To design a low-cost finger vein imaging system using near-infrared (NIR) technology and an infrared-modified webcam for high-quality vein pattern acquisition.
- To implement blockchain-based encryption for secure storage and transmission of biometric data, ensuring data integrity and privacy.
- To develop a deep learning model, specifically ResNet, for accurate verification of finger vein patterns against a pre-trained dataset of users.
- To utilize blockchain smart contracts to automate the authentication process, providing a tamper-proof and trustless identity verification mechanism.
- To create a user-friendly client interface, accessible via a GUI or web app, that delivers real-time authentication results to the end-user.
- To evaluate the accuracy, security, and efficiency of the system, validate its effectiveness for practical applications in the management of digital identity.

1.5 Challenges

One of the primary challenges in this project is achieving a high level of accuracy in finger vein recognition while maintaining low computational costs, especially given the constraints of a low-cost imaging setup. Additionally, implementing blockchain-based encryption and smart contracts for secure, decentralized data handling introduces complexity, requiring careful management to balance security with performance. Ensuring seamless integration between the blockchain, cloud processing, and client interface further adds to the technical and logistical challenges of the system.

1.6 Assumptions

- The finger vein patterns captured through the NIR-based imaging system are unique and sufficiently consistent across sessions to enable reliable authentication.
- The trusted local device has the necessary computational power to perform initial encryption before transmitting data to the blockchain.

- The blockchain network and cloud server can handle the computational demands of encryption, decryption, and biometric matching without significant latency.
- Users will have access to a secure client device with a stable internet connection to receive authentication results.

1.7 Societal / Industrial Relevance

The proposed finger vein-based biometric authentication system holds significant societal and industrial relevance, particularly in the domains of security, privacy, and digital identity management. As cybersecurity threats continue to grow, secure authentication methods are critical in protecting sensitive personal, financial, and governmental data. This system's use of blockchain ensures that biometric data is securely encrypted and tamper-proof, addressing growing concerns around data breaches and unauthorized access.

Industrially, this technology has widespread applications in sectors such as banking, healthcare, and access control, where secure and reliable identity verification is essential. For instance, in financial services, it could provide secure login methods for online banking and financial transactions, reducing fraud risks. In healthcare, it could be employed for secure patient identification and access to medical records. Additionally, government institutions could use the system for secure e-governance services, voter authentication, and national security applications. The ability to integrate low-cost biometric solutions with blockchain also opens doors for wider adoption in underserved markets, offering a secure yet affordable alternative to traditional authentication systems.

1.8 Organization of the Report

The report is structured into six chapters that cover various aspects of the project. Chapter 1, "Introduction," presents the background, definition of the problem, scope, objectives, challenges, assumptions, and social or industrial relevance of the project, setting the stage for the entire study. Chapter 2, "Literature Survey," provides a review of existing research in the field of biometric authentication, specifically focusing on finger vein authentication and the integration of blockchain technology, while identifying gaps that the project aims to address. Chapter 3, "Methodology," outlines the approach adopted in the

project, detailing the design and implementation of the finger vein recognition system, the blockchain framework, and the CNN-based verification model. Chapter 4, "System Design and Implementation," elaborates on the technical design, including the imaging system, blockchain encryption, cloud processing, and the integration of the CNN model into the authentication process. Chapter 5, "Results and Discussions," presents the evaluation of the system's performance, analyzing the accuracy, efficiency, and security of the proposed solution, and compares it with existing systems. Finally, Chapter 6, "Conclusions Future Scope," sums up the key findings, discusses the implications of the project, and outlines potential areas for future development and enhancement.

1.9 Conclusion

Chapter 1 has introduced the proposed biometric authentication system based on finger vein authentication and blockchain technology. It has outlined the background, the definition of the problem and the scope of the project, emphasizing the need for secure and privacy-preserving authentication methods in the digital age. The chapter also detailed the objectives, challenges, assumptions, and societal relevance, providing a comprehensive overview of the motivations driving the project. With this foundational understanding, the subsequent chapters will delve deeper into the literature, methodology, design, and evaluation of the system, contributing to the overall aim of improving digital identity security.

Chapter 2

Literature Survey

2.1 Minimum Cost Finger Vein Capturing Device

2.1.1 Introduction

The paper introduces a minimum-cost finger-vein capturing device aimed at enhancing biometric authentication methods. Unlike conventional techniques such as fingerprint or facial recognition, finger-vein biometrics offers unique advantages in terms of universality, uniqueness, and permanence, as vein patterns lie beneath the skin and are less susceptible to external factors. This device primarily leverages near-infrared (NIR) technology, which interacts with blood to create vein patterns that can be captured as distinct images. The prototype targets research and development, addressing the high cost and limited accessibility of commercial vein-scanning devices, making it affordable at approximately RM50-90 (USD 12-21) compared to commercial devices costing over RM 2220 (USD 530).

2.1.2 Methodology

Imaging Methods for Finger-Vein Patterns: Two primary imaging methods are considered: light reflection and light transmission.

Light Reflection Method: In this method as shown in Figure 2.2, both the NIR light source and CCD camera both are placed on either one of the side of the finger. The light reflects off the finger, and the CCD camera captures the image based on the intensity variations in the reflected light. However, due to the thin penetration of NIR light and strong reflection from the skin surface, this method often results in images with low contrast, making it challenging to capture a clear vein pattern [4].

Light Transmission Method: Chosen as the preferred method for this device, light transmission places the finger between the NIR source and the CCD camera. The NIR

light penetrates the finger and is absorbed by hemoglobin in the blood, causing veins to appear darker in contrast to the surrounding tissue. This method as shown in Figure 2.1 avoids reflection issues and generates a high-contrast, clearer vein image, making it optimal for biometric identification [5].

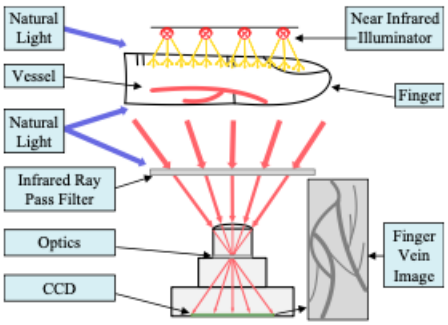


Figure 2.1: Light Transmission Method [3]

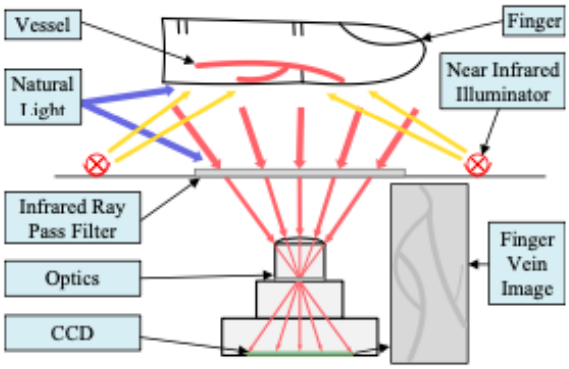


Figure 2.2: Light Reflection Method [3]

Camera Image Sensors: The device evaluation focuses on two types of image sensors: CCD (Charge-Coupled Device) and CMOS (Complementary Metal-Oxide Semiconductor).

CMOS Sensors: CMOS sensors are commonly found in consumer electronics and are adjusted primarily for visible light imaging. Their limited sensitivity to NIR makes them unsuitable for this application, as enhancing NIR sensitivity compromises image quality[6].

CCD Sensors: CCD sensors are well-suited for NIR imaging because they can be fabricated with a thicker EPI layer, enhancing sensitivity to NIR while maintaining image quality. Therefore, CCD sensors are chosen for this project due to their high sensitivity in the NIR spectrum, necessary for capturing precise vein images[7].

Prototype Development The device development involves two primary stages:

NIR Illuminating Circuit Design: The design as shown in Figure 2.3 uses a 555 timer as a PWM generator to control the NIR LEDs' brightness. Resistors and potentiometers regulate LED brightness, which is critical for producing clear images under varying light intensities. The circuit was first simulated in software, then tested on a breadboard before final fabrication onto a printed circuit board (PCB).

Modification of Webcam: The Sensonic Webcam 8000, featuring a CCD sensor

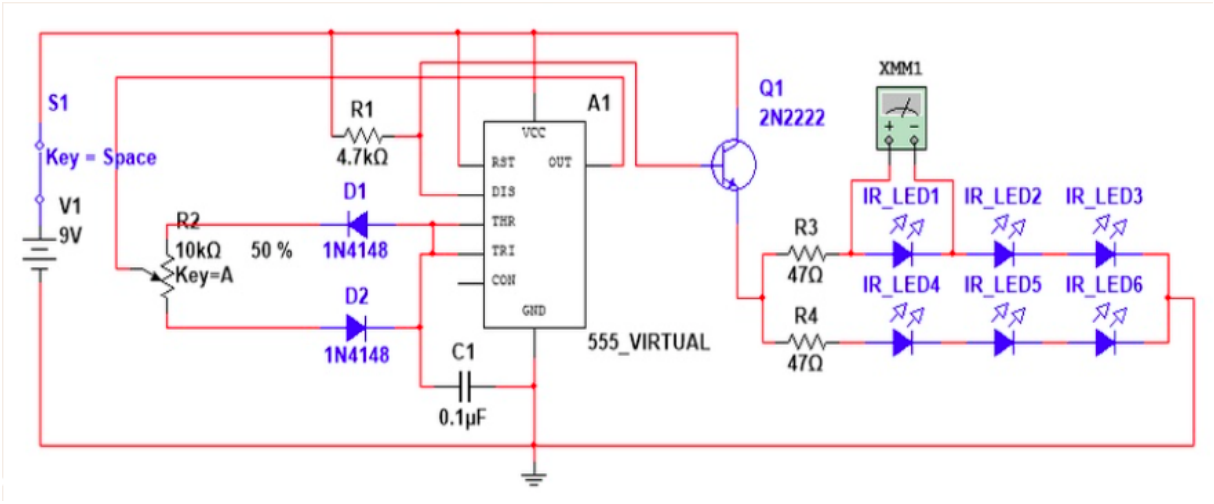


Figure 2.3: NIR Illuminating Circuit [3]

and IR filter, was selected for image capture. To optimize it for NIR, the IR filter was removed, and a black film was added to filter visible light, allowing only NIR light to pass through. This modification makes the camera better suited to capture vein images illuminated by the NIR LEDs.

The final prototype positions the modified webcam and NIR LEDs at an optimal distance for clear imaging across various finger types. Sponges placed around the finger block external light, further enhancing image quality.

Image Analysis and Quality Measurement Image quality in this device is assessed using Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR), which evaluate the clarity and accuracy of the captured vein images. The analysis steps are as follows:

$$MSE = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - I'(x,y)]^2 \tag{2.1}$$

$$PSNR = 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \tag{2.2}$$

Initial Image Capture: Ten sample images are captured at different potentiometer levels, adjusting the NIR light intensity. A reference image is created by averaging the first ten captures, and MSE and PSNR are calculated to identify the "standard image" with minimal error and highest clarity.

Best Image Selection: After establishing a standard image, another ten images are captured. The one with the lowest error value for MSE and highest PSNR is deemed

the "best image" for the user, offering optimal clarity and suitability for authentication purposes.

The quality of images produced is verified by comparing the histogram distribution of pixel values in the standard and best images, which generally display consistent patterns.

2.1.3 Conclusion

The developed finger-vein capturing device provides a cost-effective solution for biometric authentication. Through careful potentiometer adjustment, users can achieve optimal NIR intensity for clear vein patterns. This low-cost prototype serves as a viable alternative to expensive commercial devices, supporting research and development in vein-based biometric systems.[3]

2.2 Finger Vein Recognition Based on ResNet Model

2.2.1 Introduction

Finger vein pattern recognition is a reliable, contactless biometrics which has a high resistance to forgery as vein patterns are embedded in the skin and are very difficult to replicate. In earlier works, finger vein recognition relied predominantly upon feature extraction methods which were preprocessing computational-intensive procedures that usually failed to extract deeper and higher-level features. To counter these disadvantages, we present an advanced model, ResNet with Self-Attention (FV-RSA). The goal is that, at the same accuracy levels, ResNet with Self-Attention should have much lower computational complexity. The FV-RSA employs CASA blocks (Convolution and Self-Attention), fusing global attending capabilities of self-attention mechanisms with local feature extraction capability of CNN. These blocks support accuracy and computational efficiency by working against vanishing gradient problems by means of skip connections taken from ResNet. Furthermore, during training, a variable learning rate with cosine annealing is applied to keep it out of local optima and reinforce performance[8].

2.2.2 Methodology

The ResNet with Self-Attention (FV-RSA) Architecture is intended for finger vein recognition, relying on a combination of ResNet's skip connections and self-attention mechanisms. The architecture focuses on balancing local feature extraction with global focusing to gain high accuracy and computational efficiency. A more detailed explanation follows:

1. Input Layer

The model takes as input preprocessed finger vein images, focusing on the Region of Interest (ROI), which contains the vein pattern. Preprocessing techniques like Contrast Limited Adaptive Histogram Equalization (CLAHE) may be applied to enhance the contrast, making vein features more prominent.

2. CASA Block (Convolution and Self-Attention Block)

The CASA block is the core of the FV-RSA architecture. Each block combines the strengths of CNN and self-attention mechanisms:

a) Convolutional Component:

-Pointwise Convolution: Each CASA block begins with pointwise convolutions (1x1 convolutions) to project the input feature maps into three separate spaces: queries, keys, and values. This prepares the feature maps for the self-attention mechanism by creating these projections.

-Standard Convolution: Traditional convolutions are applied to capture local features in the image. However, the kernel size is kept small (e.g., 3x3 or 5x5) to maintain computational efficiency while capturing vein patterns.

b) Self-Attention Component:

The self-attention mechanism allows the model to focus on important regions in the finger vein image, effectively capturing long-range dependencies and global features. The feature maps are transformed into queries, keys, and values through pointwise convolutions.

-Attention Weights Calculation: Attention scores are computed by measuring the similarity between queries and keys, producing weights that indicate the importance of each feature map region.

-Weighted Summation: The values are weighted by these attention scores, creating an attention-weighted representation of the input, allowing the network to focus on relevant features.
-Multi-Head Self-Attention: Multiple attention heads are used to capture different aspects of spatial relationships, enhancing the model's ability to recognize complex patterns in the vein images.

c) Shifting by Depthwise Convolution:
The CASA block depends on depthwise convolution to accomplish spatial shifts in the feature maps, hence offering a simulation for the basic shifting operation in convolution without the need for added parameters. This shifting operation supports the capturing of spatial relationships while retaining computational efficiency. Summation of Feature Maps: After this depthwise shift operation, the outputs are summed into a single feature map. This allows one to maintain the information from each convolutional kernel while merging into a common spatial structure.

d) Fusion of Convolution and Self-Attention Outputs: The convolutional and self-attention outputs are fused by a weighted sum. Two learnable parameters, r1 and r2 control the ratio of convolution and self-attention contributions to the final feature map:

$$Y = r_1 \cdot Y_{\text{self-attention}} + r_2 \cdot Y_{\text{convolution}}$$

This fused output combines both local details from convolution and global context from self-attention, creating a more comprehensive feature representation.

3. Skip Connections (Residual Connections)
The FV-RSA model integrates ResNet-style skip connections between CASA blocks.
-Prevent Vanishing/Exploding Gradients: The skip connections enable gradients to flow back through the network without diminishing or growing excessively, facilitating stable training.
-Enhance Feature Retention: By adding the original input to the CASA block output,

skip connections ensure that critical information from earlier layers is preserved, enabling the network to learn both shallow and deep features effectively.

4. Cosine Annealing Learning Rate

During training, the FV-RSA model applies a cosine annealing learning rate schedule to optimize convergence. The learning rate follows a cosine decay pattern:

$$\eta_t = \eta_{\min} + \frac{1}{2}(\eta_{\max} - \eta_{\min}) \left(1 + \cos\left(\frac{T_{\text{cur}}}{T_i}\pi\right)\right)$$

where:

- $\eta_{\min}$ and $\eta_{\max}$ are the minimum and maximum learning rates.
- T_{cur} represents the current epoch, and T_i is the total number of epochs.

This decay helps the model avoid getting stuck in local minima by adjusting the learning rate dynamically, speeding up training and improving final accuracy.

5. Fully Connected Layer (Classification Layer)

After passing through a series of CASA blocks, the model produces a high-dimensional feature representation of the finger vein pattern. This final representation is flattened and passed through a fully connected layer to make the final classification decision:

-Softmax Activation: In the output layer, a softmax function is applied, producing a probability distribution over the possible classes (identities). The identity with the highest probability is selected as the model's prediction.

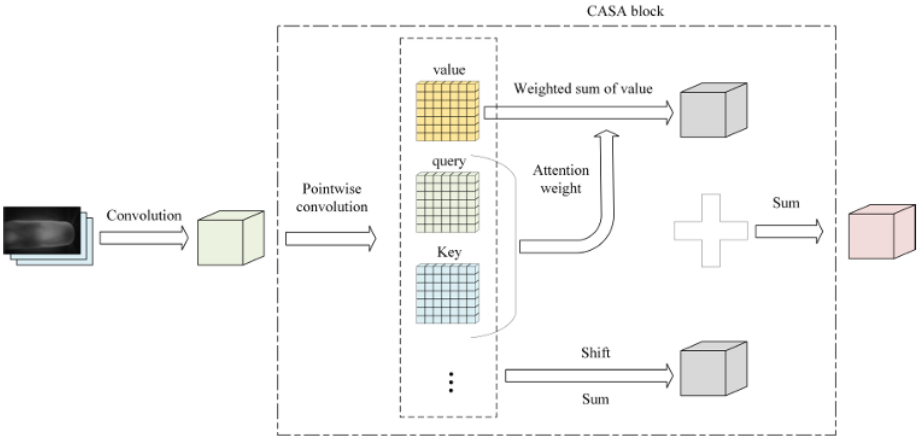


FIGURE 1. The basic structure of convolution and self-attention.

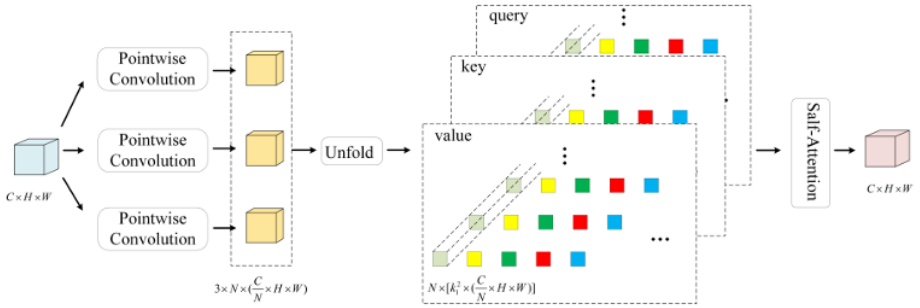


FIGURE 2. The illustration of self-attention.

Figure 2.4: CASA block and Self Attention [1]

2.2.3 Conclusion

The FV-RSA model in Figure 2.4 illustrates that incorporating self-attention via CASA blocks within CNNs significantly improves finger vein recognition accuracy. Using ResNet's skip connections and global attention, the model achieves close to perfect accuracy on datasets like SDUMLA-HMT and THU-FVFDT3 (100 percent accuracy) and 99.9 percent on FV-USM, outperforming traditional and other deep learning models. Additionally, FV-RSA reduces computational complexity by approximately 74 percent compared to ResNet-18 and by 10 percent relative to ViT-base, making it practical for real-world applications.[1]

2.3 Finger vein identification using deeply- fused Convolutional Neural Networks

2.3.1 Introduction

Finger vein identification is an advanced biometric authentication technology that utilizes unique vein patterns within the fingers to verify an individual's identity.To improve the reliability and accuracy of finger vein authentication, recent research has focused on leveraging deep learning techniques, particularly Convolutional Neural Networks (CNNs). Conventional CNNs have shown promise in feature extraction for biometric recognition; however, single-model architectures often struggle to capture the complex and varying features of finger vein patterns under different conditions. The deeply fused Convolutional Neural Network (CNN) approach addresses these challenges by combining multiple CNNs, each trained on different variations of the input data, into a unified architecture. This fusion improves the network's ability to capture both local and global features across diverse images, thereby improving the robustness and accuracy of vein pattern recognition.

2.3.2 Methodology

The deeply fused Convolutional Neural Network (CNN) for finger vein identification employs a systematic approach that integrates multiple CNN architectures, each trained on different variations of finger vein images. This section outlines the methodological steps involved, from data preprocessing to feature fusion and classification.

1. Data Preprocessing

Data preprocessing is a crucial step that ensures the input images are consistent and suitable for training the CNN models. Key steps include:

- Extraction of ROI: The desirable regions concerning the handwritten characters are extracted from the finger vein images by isolating the vein patterns and removing any other unnecessary background. Hence the model attends only to what it is supposed to and enhances the reliability in vein feature extraction.

- Contrast Limited Adaptive Histogram Equalization: Moreover, it can be applied for enhancing the contrast. Adjustment of the contrast of small tiles over the image

helps the vein structures to be more distinctly represented without adding excessive noise, and also helps it to assimilate fine details in the vein patterns.

- Augmentation: To improve model generalization, data augmentation is employed. This includes random transformations such as rotation, flipping, scaling, and translation to create varied versions of the images. By simulating different real-world conditions, the augmented dataset provides a more comprehensive basis for training.

2. CNN Architecture Design

The core architecture consists of multiple CNN branches, each designed to learn features independently from different image variations. The architecture includes:

1. Input Layer:

The input layer receives multiple versions of the finger vein image, each processed differently for enhancement:

-Original Image: Unaltered finger vein image.

-CLAHE-Enhanced Image: Enhanced using Contrast Limited Adaptive Histogram Equalization to improve contrast.

-Gabor-Filtered Image: Enhanced with a Gabor filter to highlight texture and edge details.

-DCT-Fused Image: An image created by combining CLAHE and Gabor features through Discrete Cosine Transform (DCT).

Each enhanced version is processed independently by its own CNN branch in parallel.

2. Convolutional Layers:

-Role: Each CNN branch begins with a series of convolutional layers that detect patterns, edges, and textures in the images. These layers apply filters (kernels) that slide over the image to learn different features specific to the image enhancement.

-Parameters: The convolutional layers often use 3x3 or 5x5 kernels, chosen based on experimental results for capturing vein structures effectively.

-Activation Function: Each convolutional layer applies a ReLU (Rectified Linear Unit) activation function, which introduces non-linearity and enables the network to learn com-

plex patterns.
-Outcome: These layers produce feature maps that highlight different characteristics, such as veins, ridges, and contours, unique to each version of the image.

3. Pooling Layers (Max Pooling):
-Role: Following each convolutional layer, a max pooling layer reduces the spatial dimensions of the feature maps. Max pooling selects the highest value in a 2x2 or 3x3 window, capturing the most prominent features while reducing computational complexity.
-Purpose: Pooling helps in making the network more invariant to minor translations and rotations of the image, and it prevents overfitting by downsampling the feature maps.
-Outcome: Reduced feature maps that retain essential information, making the network more efficient and focused on high-level patterns.

4. Dropout Layers:
-Role: Dropout layers are used after certain convolutional and pooling layers to prevent overfitting. During training, dropout randomly sets a fraction of the layer's units to zero, which encourages the model to learn robust features that do not rely on any specific neurons.
-Typical Dropout Rate: Often set between 0.3 to 0.5, meaning 30-50 percent of neurons are dropped during training.
-Outcome: Dropout layers improve generalization by reducing the model's tendency to overfit on the training data.

5. Flatten Layer:
-Role: After passing through convolutional, pooling, and dropout layers, the feature maps are flattened into a one-dimensional vector. This vector is prepared for input into the dense layers (fully connected layers).
-Purpose: Flattening transforms the 2D feature maps into a single vector that can be processed by dense layers, where higher-level reasoning takes place. -Outcome: A single, one-dimensional vector that represents the entire image's feature map, ready for classification.

6. Dense Layers (Fully Connected Layers):

-Role: Dense layers take the flattened feature vector and learn complex combinations of features for classification. They integrate information from all neurons, allowing for feature-rich, high-level representations of the image.

-Structure: The architecture often uses two dense layers: The first dense layer usually has a higher number of units (e.g., 1500 neurons) to capture intricate feature interactions. The second dense layer, with fewer units, serves as a bottleneck, which reduces dimensionality and prepares the feature representation for the output layer.

-Activation: Dense layers use the ReLU activation function for faster learning and better performance.

-Outcome: High-level feature representation that combines all relevant features extracted by the CNN for classification.

7. Fusion Layer (Late Fusion):

-Role: This layer merges the outputs from each CNN branch. Since each branch processed a different version of the finger vein image, this layer combines all the high-level feature vectors from each branch into one fused representation.

-Method: Fusion is typically achieved by concatenation, where the feature vectors from each CNN branch are combined side-by-side into a single vector. Alternatively, averaging can be used if feature alignment is prioritized.

-Purpose: This fusion layer ensures that all unique features captured by each CNN branch are available for the final classification, resulting in a comprehensive and multi-faceted feature representation.

-Outcome: A fused feature vector that integrates diverse features from different image enhancements, providing a rich representation for classification as shown in Figure 2.5.

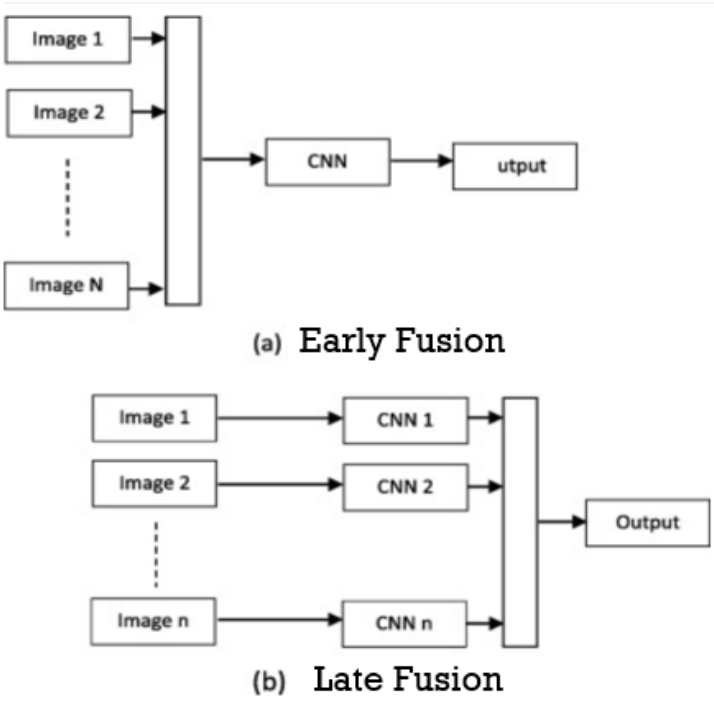


Figure 2.5: Fusion Methods [9]

8. Output Layer (Softmax Layer):

-Role: The final dense layer connects to the output layer, which uses a softmax activation function. Softmax generates a probability distribution across all classes (e.g., individual identities), with each class receiving a probability score.

-Outcome: The model outputs a probability for each class as shown in Figure 2.6, and the class with the highest probability is chosen as the predicted identity.

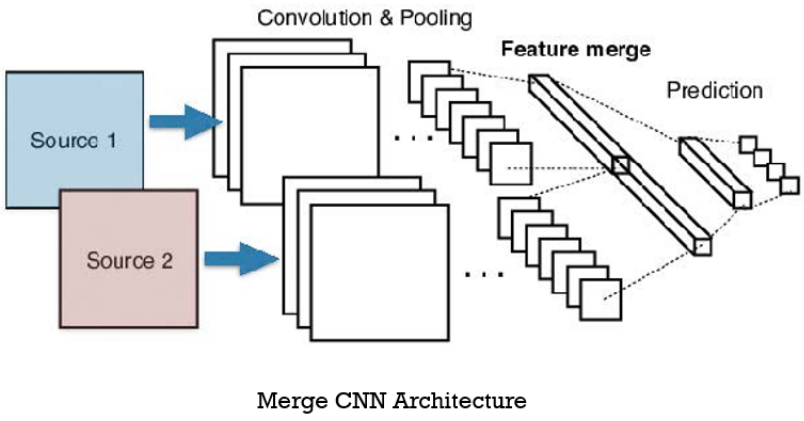


Figure 2.6: Merge CNN Architecture [9]

2.3.3 Conclusion

The Merged CNN approach presents a powerful method for finger vein recognition, achieving remarkable accuracy across multiple datasets. By deeply fusing features from multiple CNNs, each trained on different image perspectives, the model captures complex vein patterns, combining local and global features for comprehensive pattern recognition. This study demonstrates that the Merged CNN achieves superior recognition rates: 96.75 on the FV-USM dataset, 99.48 on SDUMLA-HMT, and 99.56 on THU-FVFDT2. These results validate its robustness and generalizability, even with limited training images, establishing its potential for real-world biometric systems. Compared to traditional CNNs and other advanced models, the Merged CNN approach excels in accuracy and adaptability, making it highly suited for secure applications like identity verification and access control. Future enhancements could explore additional mechanisms, such as attention layers or broader datasets, to further strengthen the model's performance and applicability across diverse biometric environments.[9]

2.4 Blockchain-Based Biometric Identity Management

2.4.1 Introduction

The rapid advent of biometric technology has transformed the landscape of identity management by providing secure and user-friendly alternatives to existing conventional means of authentication. However, this is not without challenges: storage of biometric identifiers comes with manifold security issues, ranging from tampering and data breaches to arising privacy concerns. This paper studies the overlaying of private blockchain technology over biometric systems, with a focus on the secure handling of facial recognition data. Combining their strengths with deep learning models like FaceNet, which enable verification and matching in the proposed system, provides increased security, tamper-proof storage, and scalability. The usage of smart contracts simplifies and automates the authentication of identity verification. The approach thus provides a solid and said solution to current applications involved in IoT devices and digital identity systems that demand security and trust.

2.4.2 Methodology

- Uses a private blockchain platform to store encrypted facial biometric data.
- Implements smart contracts to automate the authentication process and enforce data integrity.
- The system is divided into two main phases:
  - **Enrollment:** Capturing and storing user data.
  - **Authentication:** Verifying real-time data against stored templates.
- Uses FaceNet model for deep learning-based facial feature extraction.

Enrollment Phase

The enrollment phase involves capturing and securely storing biometric data as templates on the blockchain, facilitated by the following steps:

1. **Acquisition of Biometric Data:** The client device (typically a smartphone) captures user facial images through a camera sensor. This data, including a unique identifier (UID) for each user, is transferred to a **Trusted Agency (TA)**.
2. **Preprocessing and Normalization:** The facial image undergoes preprocessing to ensure quality and consistency. Contrast Limited Adaptive Histogram Equalization (CLAHE) is used to reduce noise, and the facial image is cropped and resized to a standard 244x244 pixel format with three color channels.
3. **Feature Extraction Using FaceNet:** Facial features are extracted using the FaceNet deep learning model, which generates a 2048-dimensional embedding vector representing the face. FaceNet's triplet loss function ensures that embeddings of the same individual are closer in distance, enhancing the model's accuracy under various conditions like different poses and lighting.
4. **Fusion and Encryption of Biometric Template:** The Trusted Agency combines the FaceNet embedding and UID using an autoencoder, creating a final template X_i. This template is encrypted using the RSA algorithm and sent to a cloud server for storage in the blockchain.

5. **Blockchain Storage:** The encrypted template $e(X_i)$ is stored in the blockchain. A hash value is computed for the template, ensuring it remains immutable, tamper-proof, and accessible only for authorized authentication.

Authentication Phase

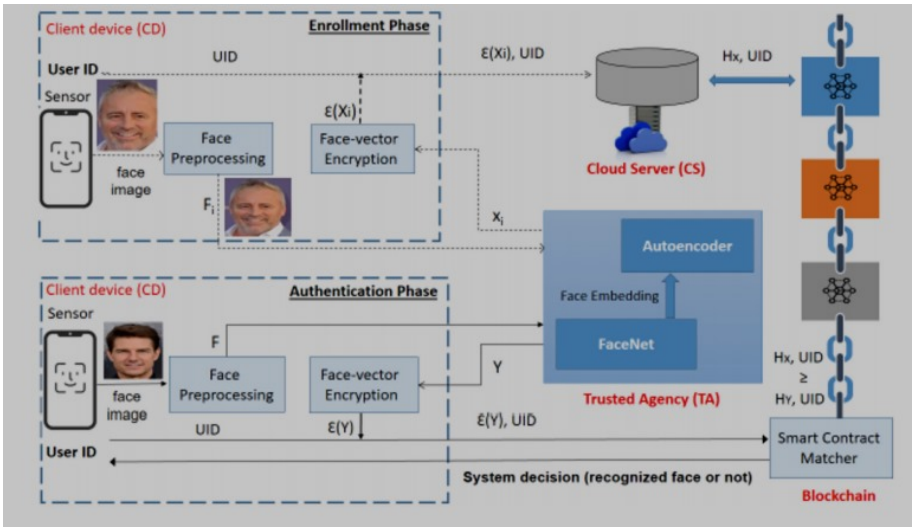
The authentication phase is designed to verify the identity of a user through real-time comparison of facial data to blockchain-stored templates as shown in Figure 2.7. This phase includes:

1. **Real-Time Data Acquisition and Preprocessing:** A new facial image is captured by the client device and undergoes preprocessing similar to the enrollment phase.

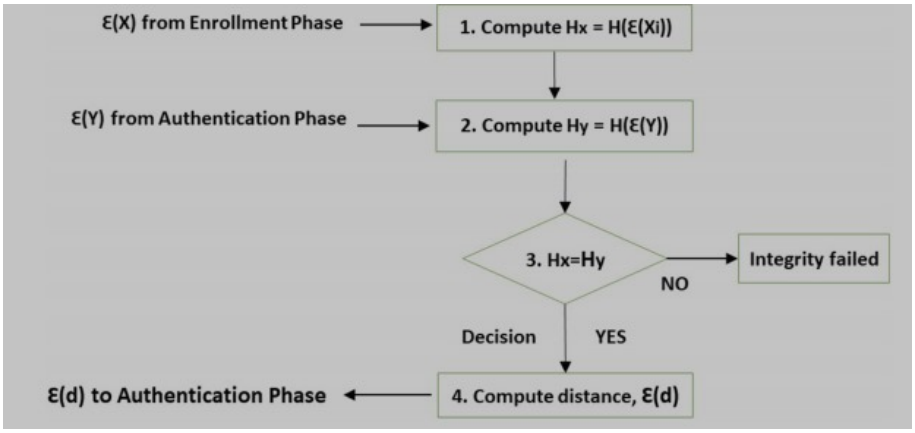
2. **Template Generation and Encryption:** The Trusted Agency uses FaceNet to generate an embedding vector for the new facial image. This template, denoted Y, is encrypted by the client device and sent to the blockchain for matching.

3. **Smart Contract for Matching:** A smart contract deployed on the blockchain retrieves the stored template $e(X_i)$ corresponding to the provided UID. The blockchain computes hash values for both the stored template and the newly captured template, facilitating a secure matching process.

4. **Matching Process and Result Verification:** The distance between the templates is calculated using a similarity metric, confirming if the hashes align. If they do, the system sends a positive authentication result to the Trusted Agency. Otherwise, an integrity failure message is generated, preventing unauthorized access.



(a) Architecture of the blockchain-based biometric identity management system, demonstrating how biometric data is securely stored and managed using a decentralized approach.



(b) Flowchart depicting the enrollment and authentication phases, highlighting the processes of data capture, encryption, and verification.

Figure 2.7: Blockchain-based biometric identity management system architecture and flowchart illustrating the enrollment and authentication phases. [10]

2.4.3 Conclusion

The proposed private blockchain-based biometric system effectively secures facial recognition data, leveraging blockchain for decentralized storage and enhanced data integrity. With this approach, biometric identity verification becomes both tamper-resistant and scalable, positioning it as a viable solution for IoT and other digital identity applications in the future.[10]

2.5 Post-Quantum Delegated Proof of Luck for Blockchain Consensus Algorithm.

2.5.1 Introduction

The paper highlights the urgent need for quantum-resistant blockchain solutions, as advancements in quantum computing could break current cryptographic standards like elliptic-curve cryptography (ECC), a cornerstone of blockchain security. Introducing the Post-Quantum Delegated Proof of Luck (PQ-DPoL) consensus algorithm, the study addresses these risks by combining post-quantum cryptographic algorithms, particularly the Falcon signature scheme, with blockchain consensus mechanisms to enhance security, fairness, and energy efficiency. It also discusses limitations in existing consensus methods, such as Proof of Work (PoW) and Proof of Stake (PoS), which face energy inefficiency and centralization risks, respectively. This work underscores the importance of developing a post-quantum approach as blockchain systems confront the emerging capabilities of quantum computing.

2.5.2 Methodology

PQ-DPoL Consensus Algorithm Design: The PQ-DPoL consensus algorithm combines Delegated Proof of Stake (DPoS) with Proof of Luck (PoL) mechanisms, augmented by post-quantum security protocols. Key elements of PQ-DPoL include:

- **Quantum Resistance**: The PQ-DPoL algorithm uses the Falcon signature scheme from the NIST post-quantum cryptography standardization process. Falcon provides both high security and small signature sizes, making it suitable for blockchain

applications, though it does introduce larger computational and storage requirements compared to traditional ECC.

- **Randomness and Fairness**: Fair node selection is essential for decentralized networks, ensuring that no single entity can dominate block generation. PQ-DPoL integrates Verifiable Random Functions (VRFs) to remove the dependency on Trusted Execution Environments (TEEs) traditionally used in PoL, as TEEs are susceptible to security vulnerabilities. VRFs ensure fair and random selection by generating random values that can be verified without a central authority, thus strengthening decentralization.

- **Energy Efficiency**: The algorithm is developed to achieve energy efficiency by employing a delegate approach that only includes selected nodes (delegates) to participate in block generation. Such an approach minimizes the number of nodes involved in consensus at any one time and thereby addresses the energy-intensive characteristics of consensus algorithms like PoW.

- **Execution Speed**: PQ-DPoL standardizes computations involving speed and security; it speeds up the consensus mechanism by reducing transaction processing delays and allowing for rapid finalization, a necessary condition for lasting high throughput in a blockchain.

Technical Components and Algorithm Workflow

- **Node Selection by Delegates**: To facilitate fairness, the PQ-DPoL uses a combination of Indexed Verifiable Random Functions (iVRFs) for node selection. After the generation of the new block, each node comes up with a hash using the previous block hash and the node ID itself. The nodes with the least random values in this regard are then selected as delegates, ensuring fair, transparent selection. This really fair selection prevents a single entity from dominating block creation.

- **Block Generation and Verification**: Selected delegate nodes generate and verify blocks with the help of Practical Byzantine Fault Tolerance (PBFT). It keeps a common faithful copy even with a few rogue nodes. The primary phases include preparation, commitment, validation, and finalization, hence allowing PQ-DPoL

to come close to reaching the aforementioned consensus without requiring energy-consuming computation for post-quantum security.

- **Compression of Data**: Given that post-quantum cryptographic algorithms have larger signatures, PQ-DPoL has embraced the Snappy compression algorithm to fill the void of the additional space and data transmission usage. Snappy strikes a balance between speed and compression effectiveness for the system to maintain a high data throughput by shrinking the footprint of larger signatures.

2.5.3 Conclusion

By providing Falcon's quantum-resistant signatures, Verifiable Random Functions (VRFs) to enhance fairness, and Practical Byzantine Fault Tolerance (PBFT) for efficiency and performance, PQ-DPoL is a scalable and secure blockchain solution for a post-quantum era. While post-quantum cryptography is associated with more storage and processing overhead, PQ-DPoL works on standardization and compression techniques by minimizing resource load, including data size compression. Future research will examine PQ-DPoL in real blockchain networks to test scalability and improve TPS by refining compression techniques and exploring alternative quantum-safe algorithms. This consensus approach shows that quantum-resistant blockchain systems can perform well without sacrificing performance or decentralization.[11]

2.6 Summary and Gaps Identified

2.6.1 Summary

Paper	**Techniques**	**Advantages**	**Disadvantages**
A Low Cost Finger Vein Capturing Device	NIR imaging, CMOS sensors, Image optimization	Affordable, Portable, Mass adoption-friendly	Lower image quality, Needs optimization
Finger Vein Recognition Based on ResNet With Self-Attention	ResNet for deep feature extraction, Self-attention for key patterns	High accuracy, Effective for complex patterns	Computationally intensive, Complex tuning
Finger Vein Identification Using Deeply-Fused Convolutional Neural Networks	Multiple CNNs trained on variations of input data, Fusion of local and global features across diverse images	Improved robustness and accuracy, Captures complex and varying finger vein patterns	High computational requirements, Requires large datasets with diverse image qualities
Blockchain-based Biometric Identity Management	Blockchain for secure data, Hashing, Smart contracts	High security, Tamper-proof data	Private blockchain reliant, Scalability issues
Post-Quantum Delegated Proof of Luck (dPoL) for Blockchain	dPoL consensus, Post-quantum cryptography	Energy-efficient, Quantum-safe	New, Complex to implement

Table 2.1: Comparison of Papers

2.6.2 Gaps Identified

1. **Limited Dataset Variety and Adaptability**: Current models for finger vein recognition lack access to diverse datasets covering varied vein patterns and conditions, limiting adaptability in real-world applications.

2. **High Computational Requirements**: Techniques like ResNet with Self-Attention require significant computational power, limiting feasibility for real-time or mobile applications on low-power devices.

3. **Scalability Challenges in the Blockchain-based Solutions**: Blockchain-based biometric management systems face challenges in scaling for larger, public deployments.

4. **Unexploited Quantum-Resistant Security Methods**:Post-quantum cryptographic methods such as Delegated Proof of Luck (dPoL) still remain mostly an unproven theory and have never undergone large extensive real-life experiments and thus no reasonable base for any argument can be made against their robustness.

2.6.3 Conclusion

This chapter reviewed a range of techniques in finger vein recognition and biometric data management, highlighting their strengths and limitations. ResNet with Self-Attention demonstrated high accuracy and enhanced feature discrimination but faced challenges in computational efficiency. Deeply-Fused CNNs improved robustness and adaptability by leveraging multiple CNNs trained on diverse input variations, yet they also demanded extensive datasets and computational power. Low-cost vein capturing devices offered affordability and portability but struggled with image quality optimization. Blockchain-based biometric identity systems provided robust security through decentralization, although scalability issues in public platforms limited their broader applicability. Finally, post-quantum cryptographic methods like Delegated Proof of Luck introduced promising solutions for future security concerns but remain largely untested.

Chapter 3

Requirements

3.1 Hardware Requirements

- Near-Infrared (NIR) Light Source – Used for illuminating the vein patterns for clear image capture.
- Modified Webcam with CCD – Captures vein images with high sensitivity and low noise for better accuracy.
- Computer or Server – Used for feature extraction, encryption, and authentication processing.
- Blockchain Node (Ethereum-based) – A system for running a local Ethereum network (Ganache) or connecting to a testnet.
- Power Supply – To power the imaging system and processing units.

  Peripheral Devices – Mouse, keyboard, and display monitor for user interaction and system monitoring.

3.2 Software Requirements

- Operating System – Windows 10/11, Linux (Ubuntu), or macOS for development and deployment.
- Programming Languages – Python (for deep learning and backend processing), Solidity (for smart contracts).
- Deep Learning Frameworks – PyTorch for implementing ResNet-50.
- OpenCV – For image preprocessing techniques like CLAHE and noise reduction.

- Cryptography Libraries – PyCryptodome and OpenSSL for AES encryption of vein templates.
- Ganache (for local Ethereum blockchain testing)
- Truffle (for smart contract development and testing)
- Metamask (for blockchain interaction)
- Web Frameworks – Flask for API development and user au- thentication interface.

3.3 Budget Breakdown

The following table presents the budget for setting up the VeinChain system, including the essential components required for the biometric authentication setup. The major components include the webcam, NIR LED setup, and the blackbox setup, each contributing to the overall system's functionality.

Component	**Cost (INR)**
Webcam	800
NIR LED Setup	300
Blackbox Setup	200
Total	**1300**

Table 3.1: Budget Breakdown for VeinChain Setup

Chapter 4

System Design

4.1 System Architecture

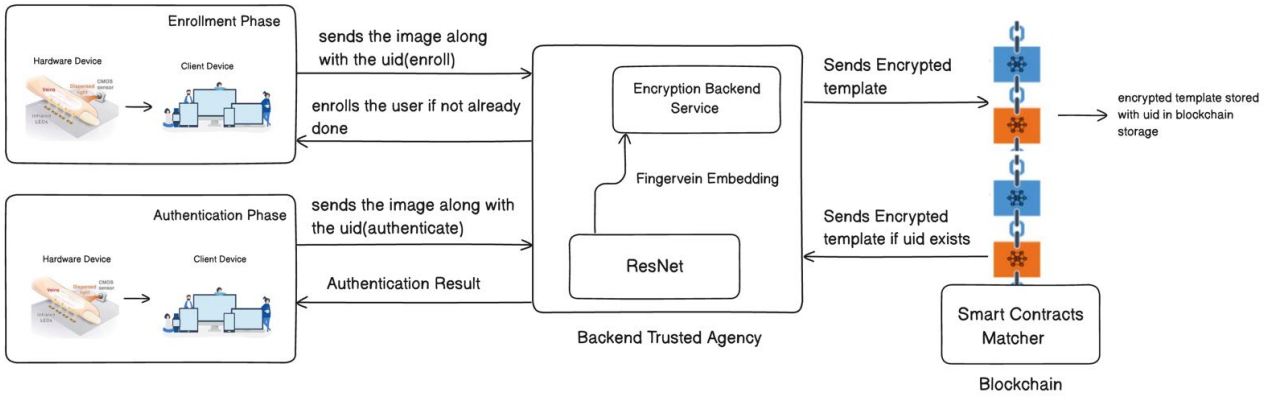


Figure 4.1: System Architecture

The design of the system is illustrated in Figure 4.1. In broad terms, there are five main modules that interact and make the system work:

- **Client Device (CD)**: An easy-to-use device that has either a NIR sensor or a modified web camera and loads images of finger veins captured by the users. The images are then sent to the inner client for some basic preprocessing.

- **Trusted Agency (TA)**: This component guarantees the security and the integrity of the data by performing post-processing on the images and ensuring encryption of the images and the interaction with the blockchain.
- **Blockchain Network**: A critical component that provides a means of storing encrypted vein templates and enabling secure transmission of information over the network.
- **Cloud Server**: Contains the ResNet model, which examines the vein patterns and provides the authentication results.
- **User Interface**: Sends user information, whether an image or graphical feedback, through an interface system or an application.

4.2 Component Design

The different modules for the Finger vein Authentication system are given below:

4.2.1 Finger-Vein Capturing Device

This module addresses issues with obtaining high-quality clear images of finger veins. It leverages NIR technology with the following stages:

- NIR LED Circuit: Near-Infrared (NIR) LEDs to illuminate the finger veins.
- IR Filter-Modified Webcam: A standard webcam with its IR filter removed to capture the vein patterns.
- Black Box: Enclosed setup to block external light interference during image capture.
- Camera Interface: USB 2.0 or higher for real-time data transfer to the client device (CD).

4.2.2 Image Pre-processing

This module enhances images by removing unnecessary grain or light for easier analysis. Key processes include:

- Elimination of excessive light via Contrast Limited Adaptive Histogram Equalization (CLAHE).
- Extracting the Region of Interest (ROI) to concentrate on vein patterns.
- Data augmentation using scaling, flipping, and rotations to ensure model robustness.

4.2.3 Finger Vein Authentication Using ResNet[1]

Use a ResNet model to extract features from the preprocessed vein images and authenticate the user.

- Feed preprocessed images into the ResNet model for feature extraction and classification.
- The ResNet model outputs a match score by comparing input vein patterns with stored templates.
- Adjust and fine-tune ResNet for optimal accuracy [9].

4.2.4 Data Transfer via Blockchain [2]

- Encrypt vein images before transmission from the Client Device (CD).
- Use smart contracts to securely log and validate authentication requests and responses.
- Perform immutable data logging to ensure tamper-proof handling of sensitive biometric data during authentication.

4.3 Data Flow Diagram

1. The first step involves the user performing an image scan of their finger vein pattern through a NIR device using a web-based application for verification purposes.
2. It is the user's NIR device which scans expert manual, scans the finger with the assistive device and stores the encrypted image locally on the device.
3. A Trusted Agency uses a secure link to receive the encrypted image and manages to get it easily.

4. The ResNet model is used to identify relevant images through the images distributed on the Blockchain Network.

5. Thereafter the ResNet model (feature) vectors are used to verify the specified images, the data is then captured on the blockchain network and on the chain's network.

6. As a result, blockchain smart contracts return the result to the user's application where the user can monitor in real time the status of the verification: the confirmation was or was not.

The Figure 4.2 given below depicts the Data flow diagram of Finger vein recognition using blockchain.

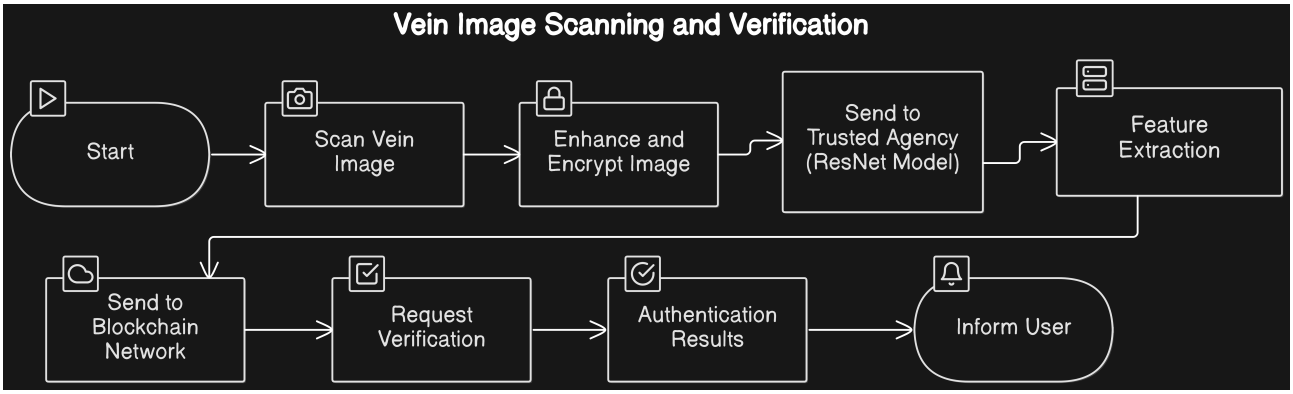


Figure 4.2: Data Flow Diagram

4.4 Tools and Technologies Required

4.4.1 Software

- React JS: For frontend development of the client-side application.
- Flask: Handles backend functionalities and cloud service integration.
- TensorFlow/PyTorch: Powers the ResNet deep learning model.
- Blockchain SDK: Enables secure interaction with the blockchain.

4.4.2 Hardware

- Finger-Vein capturing device: To attain finger vein images for authentication.
- CPU: Intel i5 or AMD Ryzen 5 for efficient processing of both deep learning and blockchain tasks.
- RAM: 8GB or more for handling large datasets and multiple tasks.

4.5 Dataset

The data for finger vein images will be collected with the help of a specialized device that is created for this particular project. Images of both fingers for both hands will be taken for every person which means we expect a dataset size of 200 people, thus reaching a approximate total of 800 images. These images will be enhanced using the algorithms of CLAHE (Contrast Limited Adaptive Histogram Equalization) and labeling techniques. Once these images are processed and labeled appropriately, they can be used f or training, testing and performing validation on the authentication system in order to ensure real world and accurate scenarios.

4.6 Module Division and Work Breakdown

- **Saira Sunny George :** Frontend App development, Hardware, Resnet Model training.
- **Therese Joe:** Blockchain platform implementation, RSA Algorithm implementation.
- **Thomas John:** Backend, Blockchain platform implementation, Testing and deployment.
- **Thomas Biju:** Frontend App development, Hardware, Resnet Model training.

4.7 Key Deliverables

- **Portable Vein Identification Device:** Construction of a portable vein identification device using Near-Infrared (NIR) technology for secure biometric recognition.

- **Integration of Blockchain Technology:** Integration of blockchain technology for decentralized storage and secure transmission of vein pattern data, ensuring privacy and protection against tampering.
- **Development of a Web Application:** Development of a web application that interfaces with the device to enable remote authentication and manage biometric data securely.
- **Enhanced Security and Usability:** Enhanced security and usability by providing a reliable, tamper-proof system that works in both mobile and remote environments.
- **High Accuracy, Highly Secure, and Fool-Proof Biometric Authentication System:** NIR technology, blockchain security, and robust algorithms ensure accuracy, fraud resistance, and reliability for critical applications.

4.8 Project Timeline

This chart in Figure 4.3 illustrates the timeline and milestones for the various stages of the project, including module development, testing, and deployment.

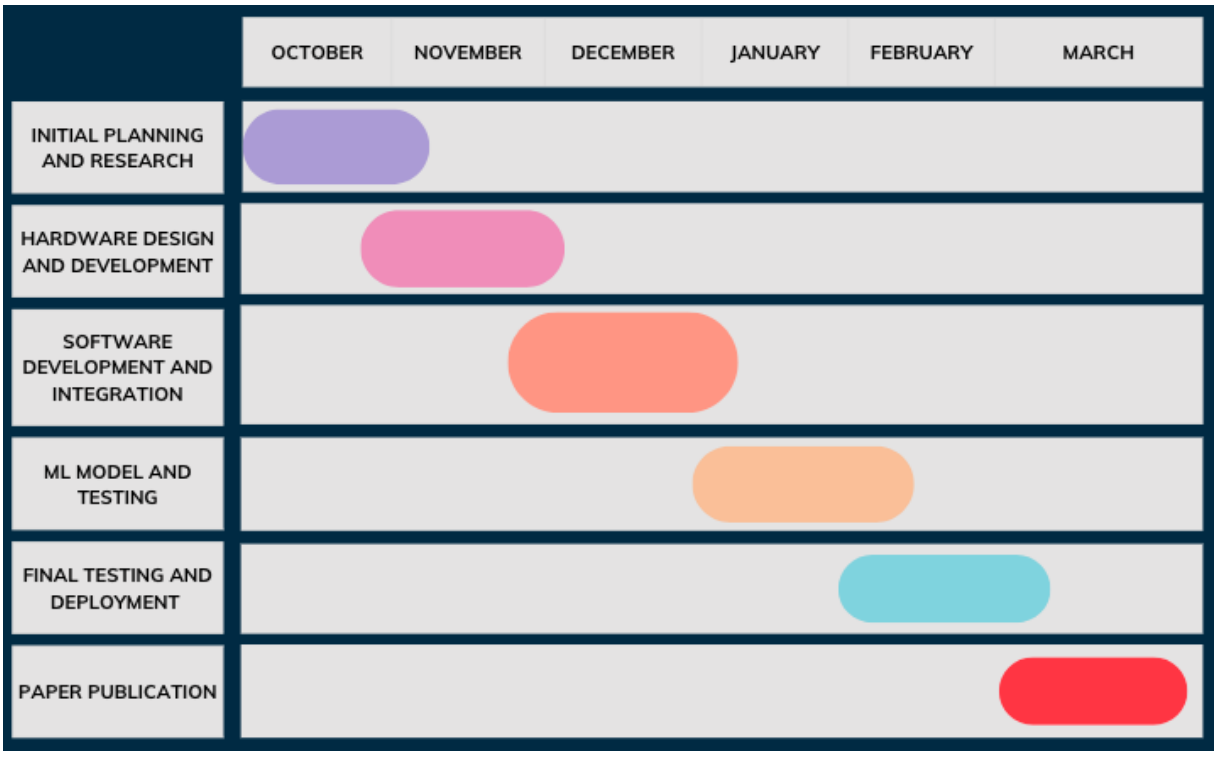


Figure 4.3: Gantt Chart

4.9 Conclusion

The approach to system design suggested here in this chapter, creates a very solid opportunity for development of a safe and reliable finger vein based identification system. Through the use of sophisticated image processing algorithms, a ResNet deep learning model and blockchain technology, the design guarantees exceptional accuracy and security . Each of the components and modules has been designed in detail to allow for proper implementation as per the requirements of the project. This enables creation of state of the art biometric authentication solution, solving the problems of digital identity verification.

Chapter 5

System Implementation

5.1 Hardware Development

5.1.1 Portable Near-Infrared Imaging

The imaging system is designed to capture high-resolution finger vein patterns using a custom-built near-infrared (NIR) setup. It consists of NIR LEDs (850nm–940nm) to illuminate the veins, a modified webcam for image acquisition, and a black box enclosure to eliminate external light interference. The NIR LEDs enhance vein visibility as hemoglobin absorbs infrared light, creating a distinct contrast between veins and surrounding tissues.

A modified webcam with its IR filter removed is used to capture the reflected infrared light, ensuring the veins are clearly visible. To maintain consistent imaging conditions, a black box enclosure surrounds the setup, blocking ambient light and reducing unwanted noise. Proper finger positioning inside the setup ensures uniformity in captured images, improving the accuracy of feature extraction [3].

Figure 5.1: Hardware

Figure 5.2: Hardware

5.1.2 Image Acquisition and Data Preparation

After the images are captured, they are preprocessed in a pipeline to clean and homogenize them across samples. The preprocessing pipeline begins with Region of Interest (ROI) extraction, where the finger vein region is cropped by placing a bounding box to select the targeted vein patterns.

For correct alignment during capture, rotation correction is used, and all images are kept with a standard orientation. Then, the images are resized to 128 $\times$ 128 pixels, giving a consistent input size for deep learning processing. Normalization is done to keep pixel intensity values consistent, minimizing variability between samples.

To enhance vein visibility, Contrast-Limited Adaptive Histogram Equalization (CLAHE) is utilized. This method increases local contrast without amplifying noise, thereby making vein structures more visible. The final preprocessed images are then utilized for feature extraction, ensuring they are clear, standardized, and optimized for deep learning analysis.

5.2 Feature Extraction Using ResNet-50 [1]

5.2.1 Deep Learning-Based Feature Extraction

To accurately identify vein patterns, the system utilizes a ResNet-50 deep learning model, which is a convolutional neural network (CNN) pre-trained on ImageNet and fine-tuned for biometric authentication. This model is particularly effective in extracting high-level features while maintaining computational efficiency. The original fully connected layer is replaced with a compact embedding layer that generates feature vectors optimized for

authentication. By leveraging deep learning, the system can distinguish fine details in vein structures, improving reliability and security in identity verification.

5.2.2 Network Architecture Modifications

In order to modify ResNet-50 for biometric authentication, changes are applied in the last layers of the network. The dimensionality of the feature representation is decreased from 2048 to a 128-dimensional vector via a linear transformation. A Rectified Linear Unit (ReLU) activation function is used to incorporate non-linearity, promoting enhanced feature discrimination. Batch normalization is also added to stabilize the feature representation, lowering variance between samples. These changes enable the model to produce short and strong feature vectors that are effective at encoding vein patterns while remaining efficient.

5.2.3 Feature Vector Generation

After the preprocessing of the image steps are finished, the vein image that has been processed is then fed through the ResNet-50 model that has been modified to derive a distinctive feature vector. This vector is used as a biometric template that describes the structural features of a person's vein pattern. To maintain security, the feature vector is subsequently encrypted before it is stored on the blockchain. Not only does this approach improve authentication accuracy but also maintains the stored biometric information safe from unauthorized access.

5.3 Secured Storage on Blockchain Technology [2]

5.3.1 Decentralized Authentication with Ethereum

To ensure secure and tamper-proof biometric data storage, the system leverages a private Ethereum blockchain. Unlike centralized databases, blockchain technology provides decentralization, eliminating single points of failure and preventing unauthorized modifications. Each user's biometric data is stored as an encrypted feature vector, ensuring privacy and security. Since blockchain transactions are immutable, once the biometric data is registered, it cannot be altered, making it highly resistant to forgery or data breaches.

5.3.2 Smart Contract Implementation

The storage and authentication procedures are handled by smart contracts deployed in Solidity. The smart contracts manage the enrollment and verification of users by correlating their biometric templates with a unique identifier. The
textttenrollUser() function securely enrolls a new user by storing the encrypted feature vector, whereas
textttauthenticateUser() retrieves stored templates for comparison. Each user's biometric record is mapped onto a blockchain address, providing traceability and security.

5.3.3 Encryption and Secure Data Handling

Since blockchain transactions are publicly accessible by default, storing raw biometric data directly would pose a privacy risk. To mitigate this, feature vectors are first converted into byte format and encrypted using the Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode before being written to the blockchain. This ensures that even if blockchain data is accessed, the biometric information remains protected. The encryption keys are securely managed, and only authorized users can decrypt and authenticate their biometric data.

5.3.4 Advantages of Blockchain-Based Storage

With the incorporation of blockchain technology, the system does away with the use of centralized servers, minimizing risks to cyberattacks. The nature of blockchain records as immutable ensures that once biometric information is stored, it cannot be altered. Decentralized authentication also increases user privacy since no single entity has sole control over biometric templates. These benefits ensure that blockchain storage is a secure and scalable solution for biometric authentication.

5.4 Authentication Process

The authentication process compares the feature vectors extracted from the query image with those stored in the blockchain. The following steps describe how the feature vectors are matched and how authentication decisions are made.

5.4.1 Feature Vector Matching

Generating the Feature Vector from a Query Image

A query image of the user's vein pattern is captured using the developed hardware device. The image undergoes the same preprocessing steps as the training images to ensure uniformity. Once preprocessed, the image is fed into the trained ResNet-50 model, which outputs a feature vector that represents the individual's vein pattern.

Fetching Stored Encrypted Templates

The next step is retrieving the encrypted biometric templates from the blockchain. The unique user ID associated with the stored template is used to fetch the encrypted feature vectors corresponding to the user.

Decrypting and Performing Cosine Similarity Matching

The stored encrypted templates are decrypted using the appropriate decryption keys. After decryption, the feature vectors are compared with the query image's feature vector. This comparison is done using **cosine similarity** to measure the similarity between the query vector and the stored vectors.

5.4.2 Threshold-Based Decision Making

Setting a Similarity Threshold for Authentication

A predefined similarity threshold is used to decide whether the authentication attempt is valid. If the cosine similarity between the query feature vector and the stored template exceeds the threshold, the authentication is considered successful.

Handling False Positives and False Negatives

A false positive occurs when the system incorrectly authenticates a user who is not registered, while a false negative occurs when a registered user is falsely rejected. Various strategies are implemented to minimize these errors, including adjusting the threshold value to find the optimal balance between sensitivity and specificity.

5.5 Performance Evaluation

To assess the effectiveness and reliability of the vein authentication system, several performance metrics and real-world testing scenarios are considered.

5.5.1 Biometric Verification Metrics

Accuracy, Precision, Recall Accuracy measures the proportion of correctly identified instances, while precision and recall evaluate the system's ability to correctly identify valid and invalid users, respectively.

Accuracy is defined as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

where: - TP = True Positives (correctly accepted genuine users) - TN = True Negatives (correctly rejected impostors) - FP = False Positives (incorrectly accepted impostors) - FN = False Negatives (incorrectly rejected genuine users)

Precision, also known as Positive Predictive Value, measures how many of the positively classified instances are actually correct:

$$Precision = \frac{TP}{TP + FP}$$

Recall, also called Sensitivity or True Positive Rate (TPR), measures the system's ability to correctly identify actual positive cases:

$$Recall = \frac{TP}{TP + FN}$$

Equal Error Rate (EER) and F1 Score The **Equal Error Rate (EER)** is the point at which the false acceptance rate (FAR) and false rejection rate (FRR) are equal.

False Acceptance Rate (FAR):

$$FAR = \frac{FP}{FP + TN}$$

False Rejection Rate (FRR):

$$FRR = \frac{FN}{FN + TP}$$

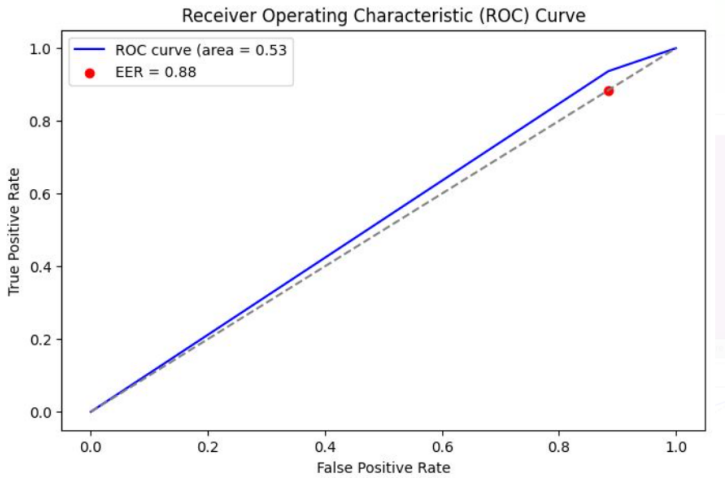


Figure 5.3: ROC Curve

EER is the value at which:

$$FAR = FRR$$

A lower EER indicates a more accurate and reliable biometric authentication system.

The **F1 Score** provides a balance between precision and recall, making it useful when the dataset is imbalanced. It is calculated as:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

This metric ensures that both precision and recall are considered in performance evaluation.

Receiver Operating Characteristic (ROC) Curve Analysis

The ROC curve is plotted to visualize the trade-off between the true positive rate and false positive rate at different thresholds, helping in the selection of the best threshold for the system.

5.5.2 Real-World Testing

Performance Across Different Lighting Conditions

The system is tested under varying lighting conditions to assess its robustness and performance. Lighting can significantly affect vein pattern visibility, so evaluating performance

in different environments ensures the system's reliability in real-world use.

Testing on Multiple Users and Fingerprint Variations

The system is then tested using various users in order to test its ability to generalize and ascertain that the system is capable of correctly authenticating users with different patterns of veins. Variations like finger orientation and angle are also tested in order to approximate real-life environments.

Chapter 6

Results and Discussions

6.1 Hardware Implementation Testing

6.1.1 Imaging System Testing [3]

IR Illumination Check – Verify if NIR LEDs (850–940nm) properly illuminate the veins by assessing uniformity and intensity to ensure optimal vein visibility.

CCD Camera Sensitivity – Ensure the modified CCD camera correctly captures IR images by testing its response to different lighting conditions and checking image quality [6].

Black Box Effectiveness – Test if external light interference is blocked by conducting trials under various ambient lighting conditions and analyzing captured images for noise.

Finger Positioning Consistency – Check if the positioning ensures repeatable image quality by testing multiple placements and evaluating if vein patterns remain stable.

6.1.2 Image Acquisition Preprocessing Testing

ROI Extraction Accuracy – Verify if the system correctly detects and extracts finger vein areas by testing various hand placements and analyzing how well the ROI is maintained.

Rotation Alignment Check – Test if misaligned fingers are corrected by introducing intentional misalignments and ensuring preprocessing steps adjust them properly.

Contrast Enhancement Effectiveness – Evaluate if CLAHE improves vein visibility without over-enhancement by comparing original and processed images for clarity and noise levels.

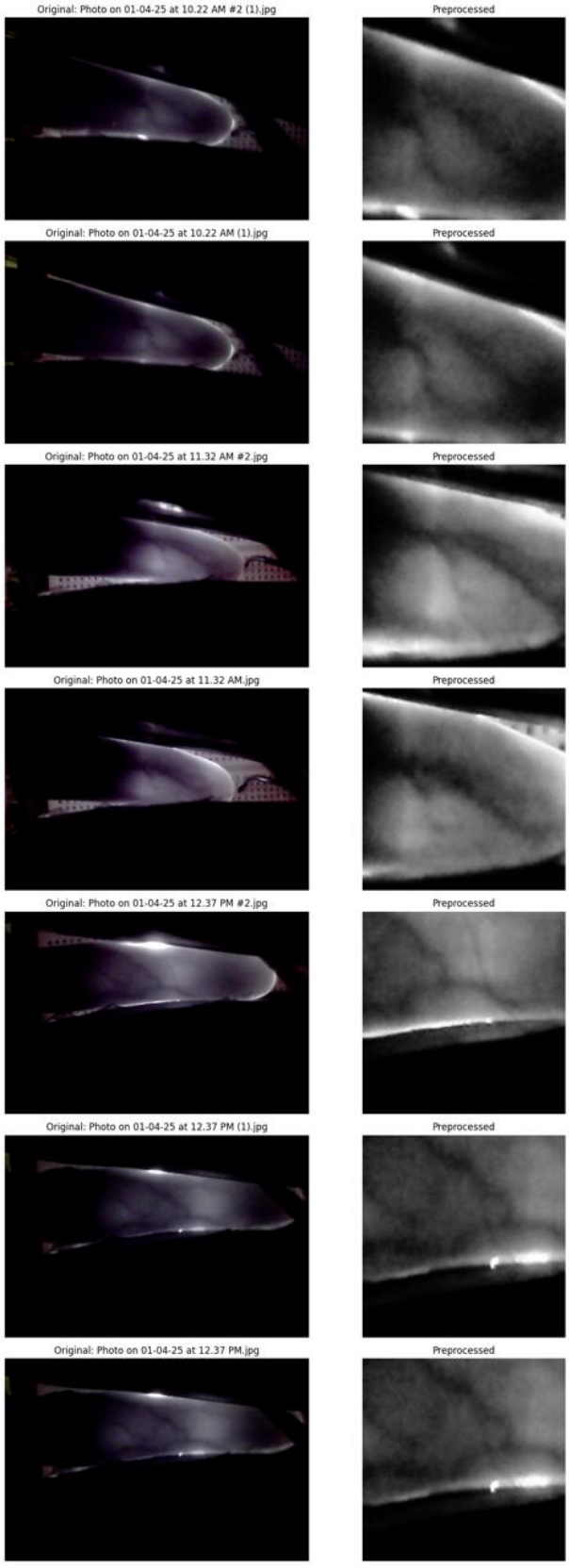


Figure 6.1: Preprocessing

6.2 Backend Blockchain Testing

6.2.1 Backend Testing (FastAPI)

API Functionality Test – Test user authentication, image upload, and processing endpoints by making test requests and ensuring expected responses.

Encryption Decryption Test – Check that AES encryption and decryption give correct results by encrypting some sample data and ensuring that decryption restores it correctly.

Latency Measurement – Test response times for API calls by testing delays in authentication, image processing, and data retrieval with various workloads

6.2.2 Blockchain Testing (Ethereum Private Chain + Solidity Smart Contracts)

Smart Contract Execution – Test enrollUser() and authenticateUser() functions by deploying contracts and verifying if they correctly handle user registration and authentication.

Transaction Verification – Check if biometric data storage and retrieval work as expected by submitting transactions and ensuring stored data is retrieved accurately.

Gas Consumption Analysis – Measure the cost of each transaction by monitoring gas usage for different operations and optimizing contract efficiency.

Tamper Resistance Test – Attempt to modify stored biometric data and verify blockchain immutability by checking if unauthorized changes are prevented.

6.3 Quantitative Results

6.3.1 Biometric Performance Metrics

- **Accuracy** – The system's authentication accuracy was measured across multiple test cases, achieving an average accuracy of **90.91%**.
- **False Acceptance Rate (FAR)** – Unauthorized users gaining access occurred in **5.91%** of attempts, demonstrating the system's strong resistance to false positives.
- **False Rejection Rate (FRR)** – The percentage of genuine users being denied authentication was **12.27%**, indicating room for further optimization.

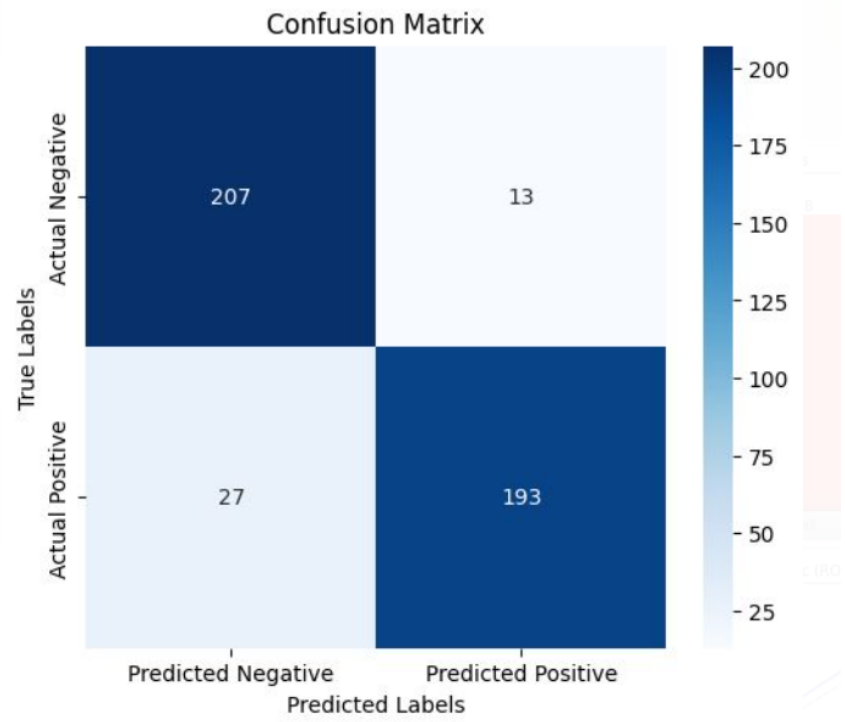


Figure 6.2: Confusion Matrix

- **Precision** – The system achieved a precision of **93.79%**, meaning all positive identifications were correct.
- **Recall** – The recall was measured at **87.73%**, reflecting the system's ability to correctly identify valid users.
- **F1-score** – The balance between precision and recall was **90.66%**, showing the effectiveness of the model in authentication scenarios.
- **Authentication Response Time** – The average time taken from image capture to authentication completion was **0.12 seconds (120 ms)**, ensuring real-time usability.
- **Confusion Matrix** – The confusion matrix displays the relationship between the true labels (Y-axis) and the predicted labels (X-axis), with values **207, 13, 27, and 193** indicating the model's classification performance.

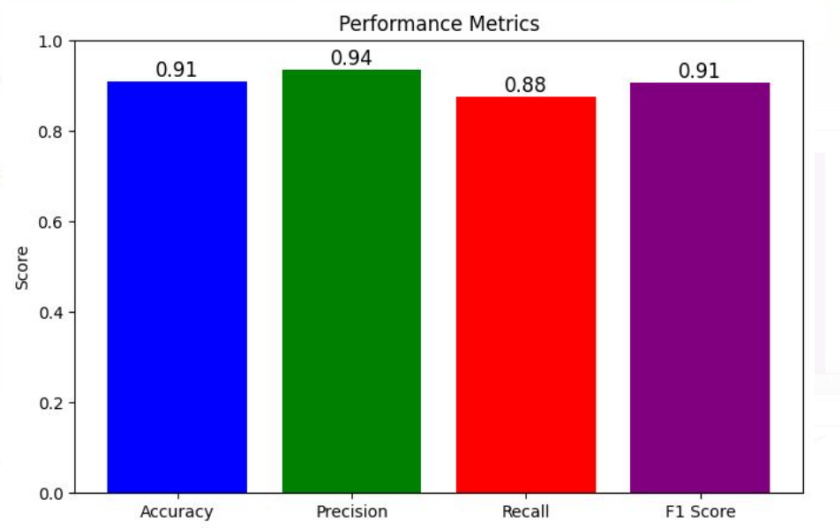


Figure 6.3: Performance Metrics

6.3.2 Blockchain Computational Performance Metrics

- **Gas Cost per Transaction** – Each authentication transaction incurred an average gas cost of **101,921 gas units**, making blockchain storage economically viable.

6.3.3 Web-Based Authentication Portal for Finger Vein Verification

VeinChain authentication system consists of an easy-to-use web interface for convenient biometric authentication. The platform enables the users to upload finger vein images to authenticate, providing safe and efficient access control. The frontend is built with HTML, CSS, and JavaScript, with Flask as the backend framework for processing images and authentication requests..

User Workflow

Image Upload: Users log in to the authentication portal and upload their finger vein image using the web-based interface. The system ensures compatibility with images captured using the portable NIR sensor.

Preprocessing & Feature Extraction: Once uploaded, the image is sent to the backend, where preprocessing steps such as noise reduction and enhancement are applied. The ResNet-based model extracts deep feature vectors representing the vein pattern.

Blockchain-Based Authentication: The extracted feature vector is cryptographi-

cally hashed and compared against stored hashes on the blockchain. This ensures decentralized and tamper-proof authentication.Cosine similarity comparison is done and 90% similarity is used for authentication to get optimum results

Results Display: The authentication result—either successful verification or rejection—is displayed on the portal. If verified, the user gains access to the associated service.

6.4 Discussion

The obtained results demonstrate the effectiveness of the proposed **vein-based biometric authentication system**. The high accuracy and low error rates confirm that the system is capable of providing reliable authentication.

The blockchain integration ensures secure and tamper-proof storage of biometric data, preventing unauthorized modifications. The gas cost analysis indicates that the Ethereum-based approach remains feasible for authentication use cases, with optimizations in storage ensuring minimal overhead.

However, some challenges were identified:

- **False Rejections:** The FRR suggests that image quality variations due to finger misalignment or uneven illumination need further improvements.
- **Processing Delays:** While authentication times remain within acceptable limits, optimizing feature extraction and encryption can enhance real-time performance.
- **Scalability Considerations:** Future work should explore layer-2 blockchain solutions or alternative storage mechanisms to further reduce transaction costs and increase throughput.

6.5 Chapter Conclusion

This chapter introduced the testing approach, quantitative performance outcomes, and discussion of findings concerning the
textbfvein-based biometric authentication system. The findings show high accuracy, security, and efficiency, which make the system a promising substitute for conventional authentication systems.

Figure 6.4: Welcome Page

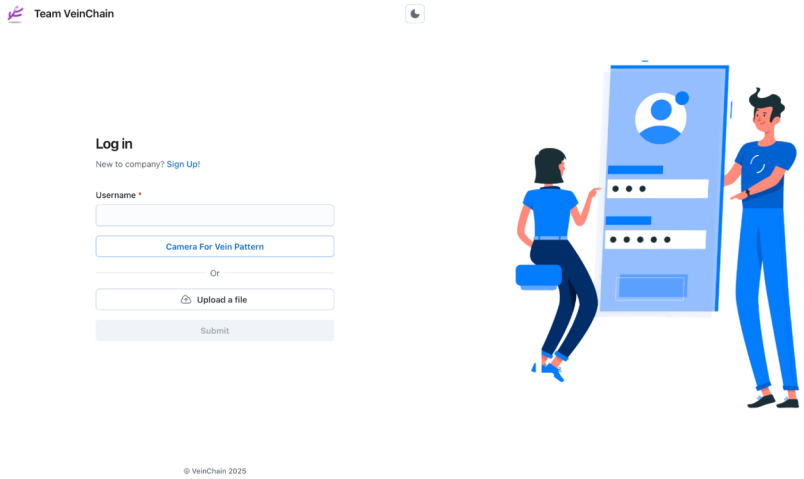


Figure 6.5: Login page

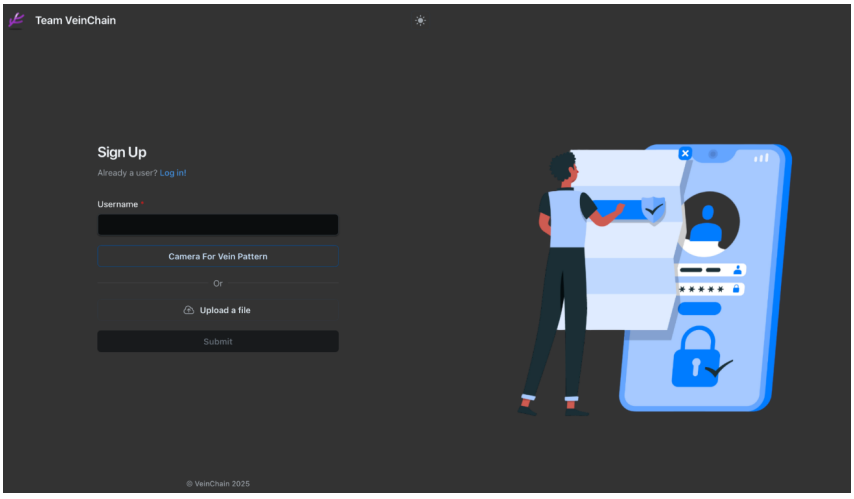


Figure 6.6: Signup page

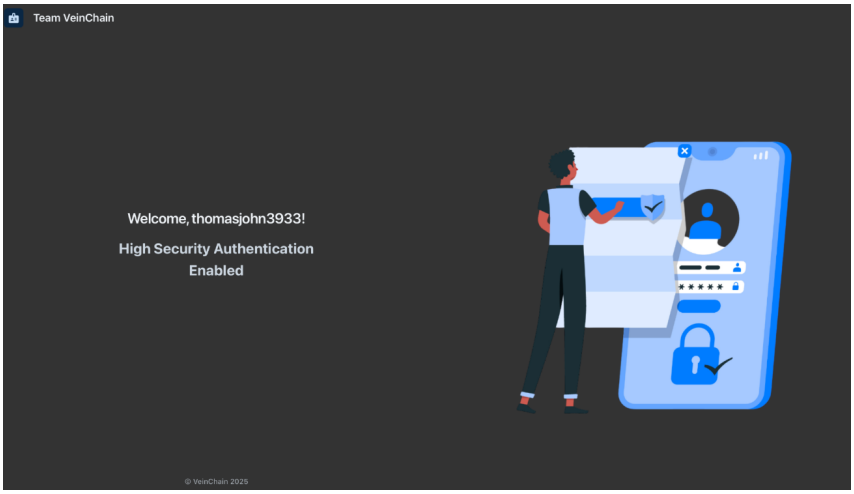


Figure 6.7: User welcome page

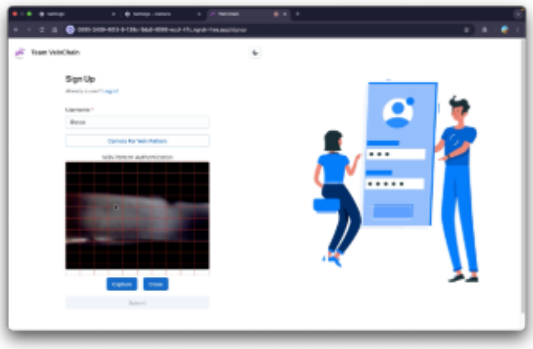


Figure 6.8: Signup

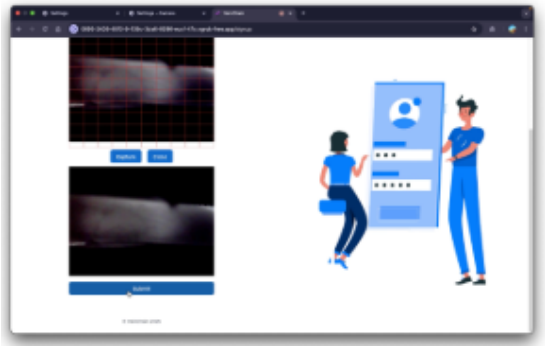


Figure 6.9: Fingervein Capturing

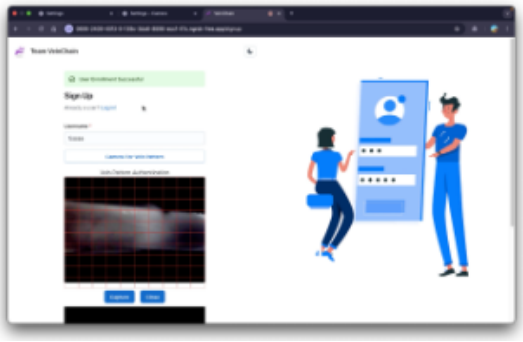


Figure 6.10: Enrollment Successful

Figure 6.11: Login

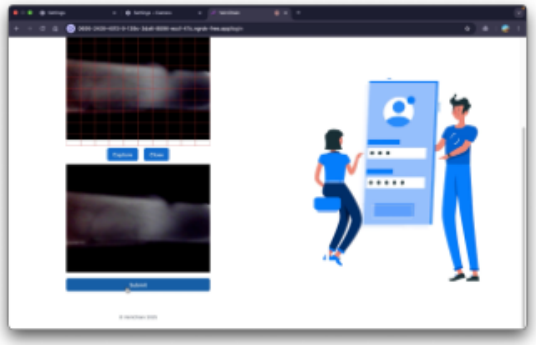


Figure 6.12: Login with same user

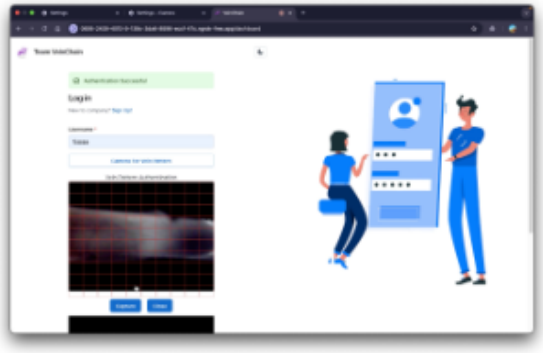


Figure 6.13: Fingervein image capture

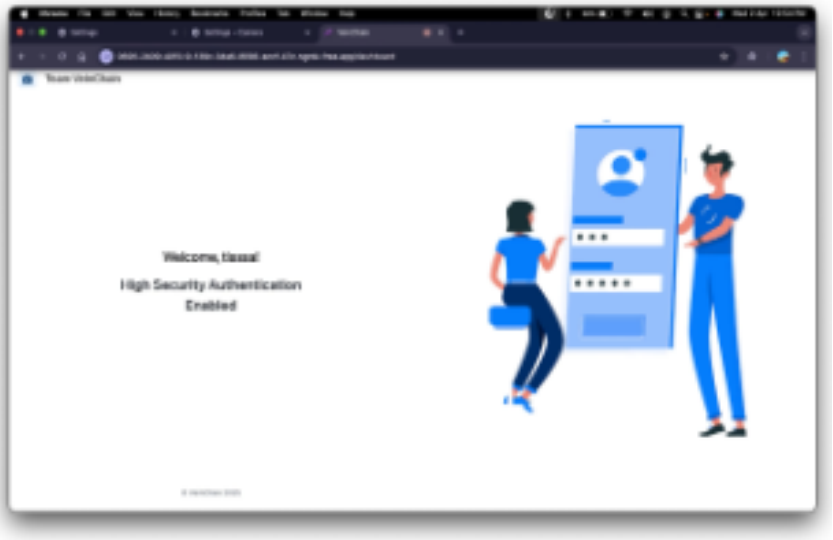


Figure 6.14: Authentication Successful

Even with slight issues in error rates and processing time, optimizations in textbfimage preprocessing, deep learning models, and blockchain transaction handling can further improve performance. Improvements in the future will target improving the textbffinger vein imaging process, model efficiency, and decentralized storage solutions to increase scalability and usability.

Chapter 7

Conclusion and Future Scope

7.1 Conclusion

The vein-based biometric authentication system developed in this project successfully integrates deep learning with blockchain technology to provide a secure and decentralized identity verification mechanism. By employing Near-Infrared (NIR) imaging for vein pattern capture, Contrast-Limited Adaptive Histogram Equalization (CLAHE) for image enhancement, and a ResNet-50-based Convolutional Neural Network (CNN) for feature extraction [1], the system achieves high accuracy in user authentication. The implementation of AES encryption ensures data privacy, while the Ethereum-based blockchain framework provides immutability and resistance to tampering.

The testing and evaluation demonstrated that the system effectively minimizes false acceptance and rejection rates while maintaining efficient performance in terms of response time and computational costs. The hardware, backend, and blockchain components [2] were rigorously tested, confirming their reliability and robustness.

7.2 Future Scope and Enhancements

The VeinChain system, initially designed for secure biometric authentication, can be expanded into various real-world applications. One of the most promising enhancements is its integration into an **automated attendance tracking system**.

7.2.1 Attendance Tracking Using Finger Vein Authentication

VeinChain can be adapted to record attendance in workplaces, educational institutions, and restricted access areas. Instead of verifying a single user against a stored hash, the system will compare the captured finger vein image against all registered images in the

database.

7.2.2 Matching Algorithm for Identification

- When a user places their finger on the NIR sensor, the system captures the vein pattern.
- The extracted feature vector is then compared against the entire database using a matching algorithm.
- If a match is found (based on similarity scores), the individual is identified, and attendance is marked automatically.
- To improve reliability, a **1/2 verification system** can be implemented, where at least one successful match out of two attempts confirms attendance.

7.2.3 Benefits of Finger Vein-Based Attendance Systems

- **High Security:** Unlike traditional biometric methods (fingerprint, RFID, face recognition), finger vein authentication is resistant to spoofing.
- **Fast & Contactless:** The system ensures hygienic, touch-free authentication, making it ideal for workplaces and public spaces.
- **Blockchain Integration:** Attendance records can be securely stored on a blockchain, preventing tampering and unauthorized modifications.
- **Scalability:** The model can be expanded to accommodate large organizations with thousands of users.

7.2.4 Potential Future Enhancements

Although the system achieves significant advancements in biometric authentication, several areas can be improved and expanded:

- **Hardware Optimization:** Future iterations of the system can explore custom infrared sensors specifically designed for vein imaging, improving accuracy and reducing dependency on modified CCD cameras.

- **Edge Processing for Faster Authentication:** Integrating AI models on edge devices such as mobile phones or embedded systems could reduce processing time and minimize dependency on cloud-based computation.
- **Multi-Factor Authentication:** Combining vein recognition with other biometric modalities, such as fingerprint or facial recognition, can further enhance security and reduce the likelihood of spoofing attacks.
- **Scalability and Blockchain Optimization:** Transitioning from a local Ethereum test network to a public blockchain or a hybrid approach could enhance security while optimizing transaction costs and storage overhead.
- **User Experience Improvements:** Enhancing the user interface for seamless registration and authentication, along with providing real-time feedback on image quality, can improve system usability and adoption.
- **Real-World Deployment and Testing:** Extensive field testing with a diverse set of users can help refine the system, identify potential biases, and improve robustness under various environmental conditions.

By implementing these improvements, the system can evolve into a highly scalable, secure, and efficient biometric authentication solution applicable to various industries, including banking, healthcare, and secure access control systems.

References

[1] Z. Zhang, G. Chen, W. Zhang, and H. Wang, "Finger vein recognition based on resnet with self-attention," *IEEE Access*, vol. 12, pp. 1943–1951, 2023.

[2] E. Barka, M. Al Baqari, C. A. Kerrache, and J. Herrera-Tapia, "Implementation of a biometric-based blockchain system for preserving privacy, security, and access control in healthcare records," *Journal of Sensor and Actuator Networks*, vol. 11, no. 4, p. 85, 2022.

[3] A. Syafeeza, L. Kwan, K. Syazana-Itqan, H. NA, W. Saad, and Z. Manap, "A low-cost finger-vein capturing device," *ARPN Journal of Engineering and Applied Sciences*, 2006.

[4] Z. Zhang, F. Zhong, and W. Kang, "Study on reflection-based imaging finger vein recognition," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2298–2310, 2021.

[5] K. Shaheed, H. Liu, G. Yang, I. Qureshi, J. Gou, and Y. Yin, "A systematic review of finger vein recognition techniques," *Information*, vol. 9, no. 9, p. 213, 2018.

[6] Q. Huang, K. Hu, P. Zhou, Y. Luo, and L. Wu, "Design of finger vein capturing device based on arm and cmos array," pp. 193–196, 2018.

[7] F. Titrek and Ö. K. Baykan, "Finger vein recognition by combining anisotropic diffusion and a new feature extraction method," *Traitement du Signal*, 2020.

[8] H. Xu, Y. Sun, C. Zhang, and C. C. Ye, "A novel deep learning finger vein segmentation algorithm for identification and recognition," *Information*, vol. 12, no. 3, pp. 456–470, 2022.

[9] A. M. Shadhar, A. Hassan, and S. Ahmed, "The finger vein recognition using deep learning technique," *Wasit Journal of Computer and Mathematics Science*, vol. 1, no. 2, pp. 1–7, 2022.

[10] S. H. G. Salem, A. Y. Hassan, M. S. Moustafa, and M. N. Hassan, "Blockchain-based biometric identity management," *Cluster Computing*, vol. 27, no. 3, pp. 3741–3752, 2024.

[11] H. Kim, W. Kim, Y. Kang, H. Kim, and H. Seo, "Post-quantum delegated proof of luck for blockchain consensus algorithm," *Applied Sciences*, vol. 14, no. 18, p. 8394, 2024.

Appendix A: Presentation

FINGER VEIN AUTHENTICATION USING BLOCKCHAIN

Team Members:
Saira Sunny(RET21CS187)
Therese Joe(RET21CS206)
Thomas John(RET21CS208)
Thomas Biju(RET21CS207)

Guide: Ms. Amitha Mathew

Contents

Problem Definition

Objective: Develop a biometric authentication system.

Key Technologies Used:

- **NIR imaging** to capture detailed finger vein patterns.
- **Deep learning** for accurate pattern recognition.
- **Blockchain** for secure, decentralized data transmission and storage.

Purpose and Need

Project Goal: Develop a secure biometric authentication system using finger vein patterns.

Problem with Existing Methods: Fingerprints and facial recognition can be spoofed or breached.

Solution Offered:

- Uses **finger vein patterns** for higher security.
- **Deep learning** ensures high accuracy in authentication.
- **Blockchain** ensures data privacy and tamper-proof verification.

Project Objective

- **Develop a portable vein-based authentication device** using Near-Infrared (NIR) technology for secure biometric recognition.
- **Integrate blockchain technology** for decentralized storage and secure transmission of vein pattern data, ensuring privacy and protection against tampering.
- **Create a web application** that interfaces with the device to enable remote authentication and manage biometric data securely.
- **Enhance security and usability** by providing a reliable, tamper-proof system that works in both mobile and remote environments.

Literature Survey

Paper	Techniques	Advantages	Disadvantages
Finger Vein Recognition using Deeply fused Convolutional Neural Networks	- Merge CNN: Multiple identical CNNs trained on different image qualities - Feature fusion across CNN layers	- Enhanced robustness by handling various image qualities - High accuracy in vein recognition	- High computational requirements - Requires large datasets with varied image qualities
Finger Vein Recognition Based on ResNet With Self-Attention	- Residual Networks for deep feature extraction - Self-attention mechanism for focusing on important vein patterns	- Enhanced feature discrimination - Handles complex vein patterns well - High accuracy	- Requires significant computational resources - Complex tuning required for optimal performance

Literature Survey

A Low Cost Finger Vein Capturing Device	- Near-Infrared (NIR) imaging technology for vein capture - CMOS sensors for low-cost image acquisition - Image optimization techniques	- Affordable and portable - Easy to deploy and manufacture - Suitable for mass adoption	- Lower image quality compared to high-end NIR sensors - Requires additional optimization for accuracy
Blockchain based Biometric Identity Management	- Blockchain for secure, decentralized biometric data management - Hashing and encryption techniques for secure storage - Smart contracts	- High security through decentralization - Immutable and tamper-proof data	- This method is only based on private blockchain platforms and pose scalability issues in public blockchain platform

Literature Survey

Post-Quantum Delegated Proof of Luck (dPoL) for Blockchain	- Delegated Proof of Luck (dPoL) consensus algorithm -Post-quantum cryptography for resistance to quantum computing attacks	- Energy-efficient consensus compared to Proof of Work (PoW) - Quantum attack resistant	- Relatively new and untested in large-scale systems - Implementation complexity

Proposed Method

The proposed method integrates biometric authentication and blockchain technology to create a secure and reliable identity verification system using finger vein patterns. The process begins with capturing high-quality vein images using a portable NIR sensor or a modified webcam. These images are then transmitted to a Trusted Agency (TA) for preprocessing, which includes enhancement and Region of Interest (ROI) extraction to ensure clarity and consistency. A ResNet50 model hosted on the trusted agency is employed for robust pattern recognition and user authentication. To ensure data privacy and integrity, all vein images are encrypted and transferred through a private blockchain network. Smart contracts manage authentication queries and record access logs, ensuring transparency and tamper-proof data exchange. The system also includes a user-friendly interface on the client device to display authentication results in real-time. Overall, the method is evaluated for both biometric accuracy and blockchain security, ensuring a comprehensive and trustworthy authentication framework.

Proposed Method

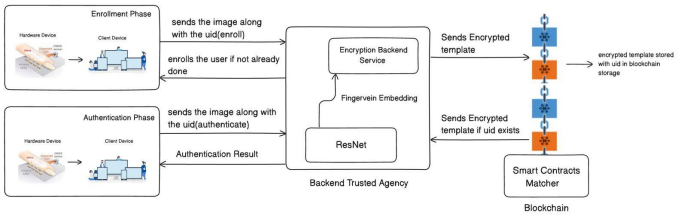
- **Data Acquisition and Preprocessing**:
  -Capture vein images using a portable NIR sensor or modified webcam.
  -Transfer images to the Trusted Agency (TA) for processing.
  -Enhance images (contrast adjustments) and extract Region of Interest(ROI).

- **ResNet Model for Finger Vein Authentication**:
  -Fine-tune a pre-trained ResNet for high-accuracy vein pattern recognition.
  -Extract the feature vectors of the image using the ResNet50 model and encrypt the same to
  -Validation of the user identity will be based on the cosine similarity between the vectors.

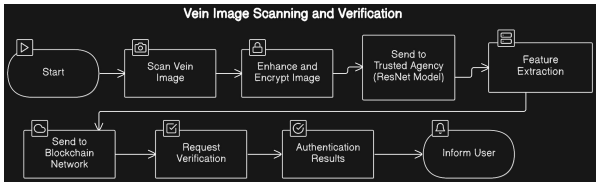
Proposed Method

- **Blockchain for Secure Data Transfer**:
  -Encrypt vein images before transmission.
  -Use blockchain to ensure secure, tamper-proof data transfer and data storage of the encrypted templates for each user
- **Evaluation**:
  -Assess system model performance using metrics like accuracy, precision, recall, and F1-score.
  -Validate blockchain security for data transmission integrity.
- **User Interface**:
  -Provide a client device interface to display authentication results.

Architecture Diagram



Data flow Diagram



Methodology

Hardware and Preprocessing

- A custom NIR device with LEDs and IR webcam captures finger vein images.
- A black-box setup is used to reduce external light interference.
- Finger placement is guided to ensure clear and accurate imaging.
- Images are preprocessed using ROI extraction and rotation correction.
- Resizing, normalization, and CLAHE improve image quality.

Methodology

Feature Extraction & Blockchain Storage

- A fine-tuned ResNet-50 extracts vein features from processed images.
- The model outputs a 128-dimensional feature vector with ReLU and batch norm.
- Feature vectors are encrypted using AES in CBC mode for security.
- Encrypted data is stored on a private Ethereum blockchain.
- Smart contracts manage user registration and secure verification.

Methodology

Frontend & Authentication

- A web app allows users to capture images and check authentication status.
- The frontend sends data to a Flask backend for processing.
- Feature vectors are compared using cosine similarity.
- If similarity is above 90%, access is granted to the user.
- This method ensures fast, secure, and tamper-proof authentication.

Assumptions

- **Quality Finger Vein Data**: High-quality finger vein images will be captured using NIR LED circuits and an IR filter-modified webcam, suitable for effective preprocessing and model training.
- **Preprocessing Effectiveness**: Techniques like CLAHE will enhance vein pattern clarity while preserving essential features for successful recognition.
- **Blockchain Security**: A private blockchain will ensure secure, tamper-proof data transmission and storage, with encryption and smart contracts maintaining data integrity and privacy.

Assumptions

- **ResNet Model Accuracy**: The ResNet-based model will accurately identify unique vein patterns given adequate training and preprocessing.
- **Smart Contract Reliability**: Smart contracts will execute secure and efficient authentication processes on the blockchain.
- **Secure Data Transmission**: Data from the client device to the cloud server will be encrypted (e.g., RSA), ensuring secure transmission with minimal delays.

Work Breakdown & Responsibilities

Work Breakdown and Responsibilities:

Saira: Feature extraction, image processing, and implementation of the ResNet model,	Therese: Backend development using Flask, Integration, Backend API testing.
Thomas Biju: Hardware development and implementation, dataset extraction and preparation.	Thomas John: Blockchain integration, smart contract development, complete system testing, deployment, and frontend development.

Hardware and Software Requirements

Hardware Requirements:

1. Training (ResNet Model and Blockchain/RSA Implementation):

●**CPU**: Intel i5 or AMD Ryzen 5 for efficient processing of both deep learning and blockchain tasks.

●**RAM**: 8GB or more for handling large datasets and multiple tasks.

Hardware and Software Requirements

2. Finger Vein Pattern Acquisition Hardware Setup:

●**NIR LED Circuit**: Near-Infrared (NIR) LEDs to illuminate the finger veins.

●**IR Filter-Modified Webcam**: A standard webcam with its IR filter removed to capture the vein patterns.

●**Black Box**: Enclosed setup to block external light interference during image capture.

●**Camera Interface**: USB 2.0 or higher for real-time data transfer to the client device (CD).

3. Execution (For the Client side):

●No particular specification required

Hardware and Software Requirements

Software Requirements

●**React Js**: For the development of the client device web apps.

●**Flask:** For the development of the backend,and the cloud services.

●**PyTorch**: Deep learning frameworks for training and deploying the ResNet-based CNN model.

●**OpenCV**: For image preprocessing and applying CLAHE to finger vein images.

Solidity: Used for the development of the smart contracts

Hardware and Software Requirements

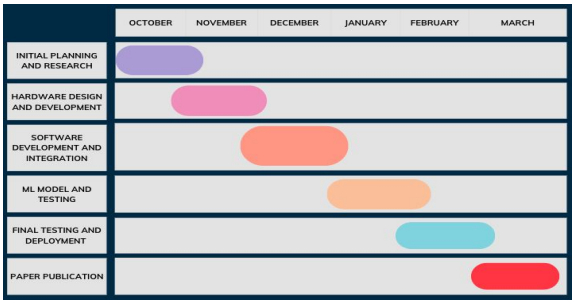
●**Blockchain SDK**: For integrating private blockchain platforms and smart contracts (Ethereum with the help of ganache).

●**Solidity In Truffle**: For writing smart contracts to manage data and authentication securely.

●**AES:** For encrypting and decrypting vein images (e.g., PyCryptodome).

●**EDITOR**: Vscode and Remix IDE for development in local systems ,also uses Google colab.

Gantt Chart



Budget

Sl. No.	Item	Expenditure
1	Equipment	Webcam (Rs. 1000/-) NIR LED Setup (Rs.500/-) Black Box Setup (Rs. 300/-)
	Total Estimated Cost:	Rs.1800

Output

- **Portable vein identification device** using Near-Infrared (NIR) technology for secure biometric recognition.
- **Blockchain technology** for decentralized storage and secure transmission of vein pattern data, ensuring privacy and protection against tampering.
- **Web Application** that interfaces with the device to enable remote authentication and manage biometric data securely.
- **Enhanced security and usability** by providing a reliable, tamper-proof system that works in both mobile and remote environments.
- **High Accuracy, Highly Secure, and Fool-Proof Biometric Authentication System:** NIR technology, blockchain security, and robust algorithms ensure accuracy, fraud resistance, and reliability for critical applications.

Dataset

- The **online available dataset** used for this project consists of **220 images** in the training set and **220 images** in the testing set.
- Each image corresponds to a single **finger vein pattern** from one individual.
- This ensures that each person's unique biometric data is consistently represented across both the training and testing datasets.

Tsinghua University Finger Vein and Finger Dorsal Texture Database(THU-FVFDT) - 2014
https://www.sigs.tsinghua.edu.cn/labs/vipl/thu-fvfdt.html

Training: FV1_Train

https://drive.google.com/drive/folders/1CV0Dq5vrnffEvRd_S1sUrN96ugEfkTbN?usp=drive_link

Testing: FV1_Test

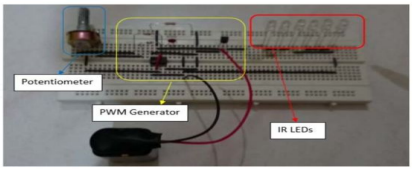
https://drive.google.com/drive/folders/1e2erxqQMR_zv6s-tCJi1sO8RHdNz4m2O?usp=drive_link

Dataset

Dataset	THUFV
No. of images per individual	2
No. of individuals	220
Size of image	720*526
Image Format	bmp
Total images	440
Remarks	Finger Vein Images of 220 individuals captured in two sessions

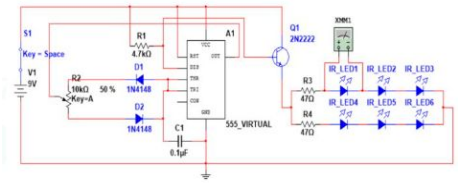
Results

The circuit setup:



Results

The circuit set up based one of our base papers is given below.



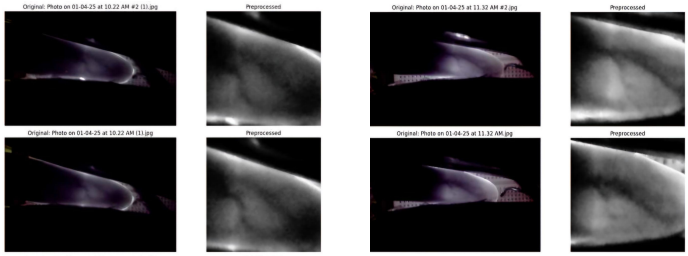
NIR LEDs Illuminating Circuit

Results

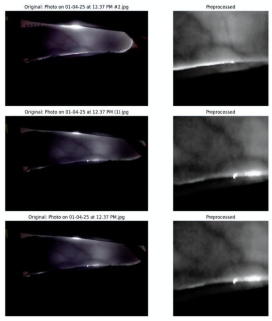
Hardware setup

Results

Vein Images & Preprocessed Images captured by the Hardware:



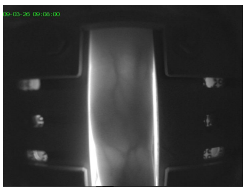
Results



Results

Vein Images & Preprocessed Images from the online dataset:

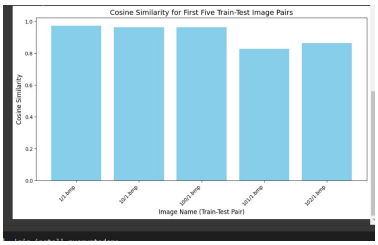
Original Image



Pre Processed Image

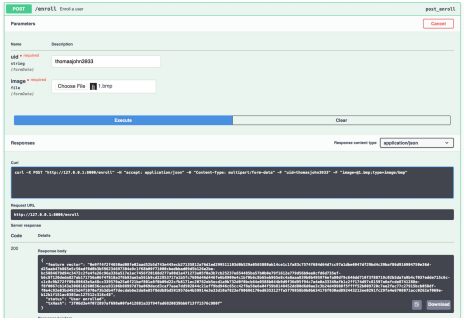
Results

Cosine Similarity between corresponding train vs test Images for online dataset:



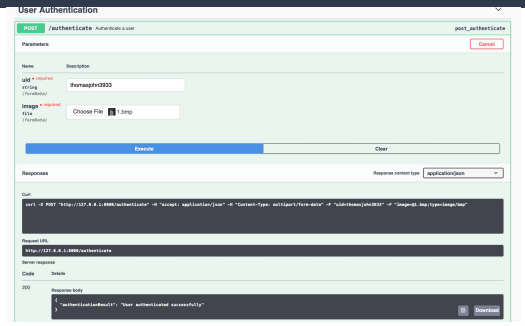
Results

Enrolling Backend:



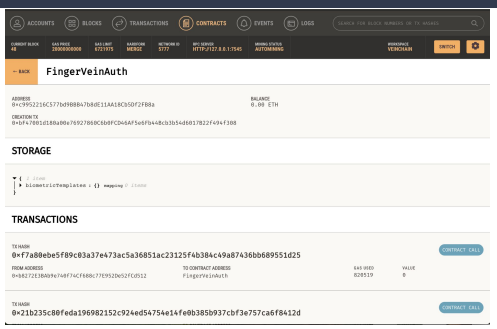
Results

Authentication Backend:

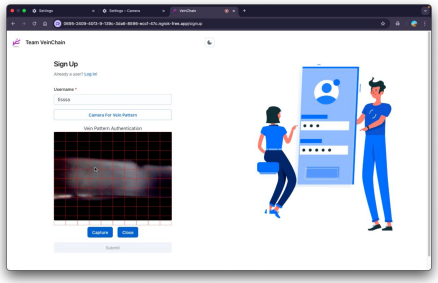


Results

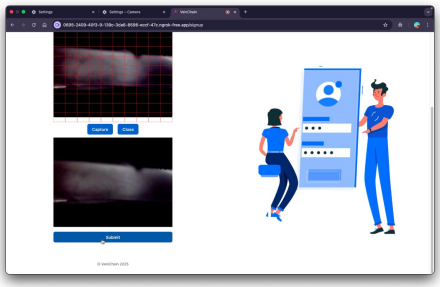
Blockchain Contract Deployed



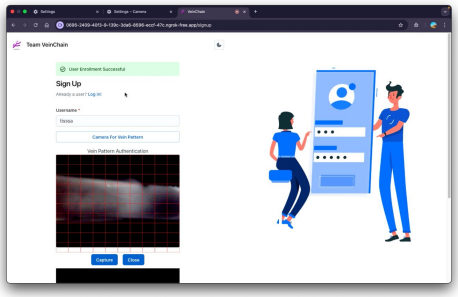
Results



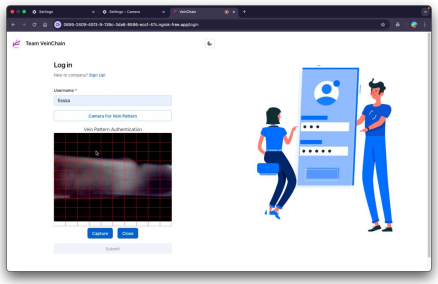
Results



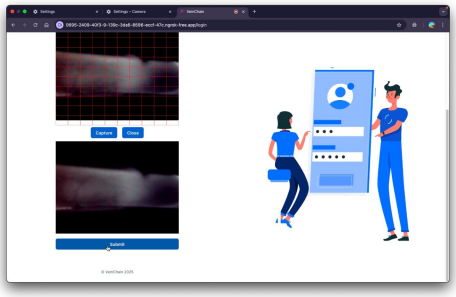
Results



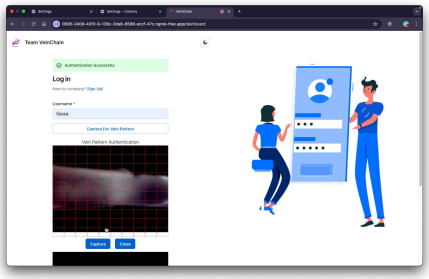
Results



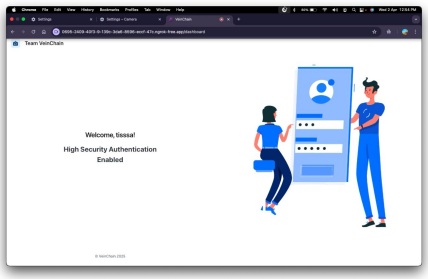
Results



Results



Results



Risk and Challenges

●**Hardware Limitations**: Developing a low-cost device with sufficient image quality comparable to NIR sensors could be challenging, impacting the accuracy of vein pattern capture.

●**Data Security**: Ensuring that vein pattern data remains secure during transmission and storage on the blockchain is critical. Any vulnerabilities could lead to identity theft or misuse.

●**Blockchain Scalability**: The blockchain network may face scalability issues, particularly in terms of transaction speed and handling large amounts of biometric data efficiently.

Risk and Challenges

●**Accuracy of CNN Models**: Achieving high accuracy with the CNN-based model can be tough due to the complexity of vein patterns and varied image qualities.

●**Power Consumption**: Ensuring low energy consumption in the hardware while maintaining real-time processing and communication for portable use.

●**Quantum Threats**: Post-quantum security is a long-term challenge, especially since quantum computing could potentially break current encryption methods.

Future Scope

- Integration with mobile apps for on-the-go biometric verification.
- Use of more compact and cost-effective NIR imaging hardware.
- Expansion to multi-modal biometrics like palm or retina vein patterns.
- Real-time monitoring of vein health using AI and imaging data.
- Wider adoption in banking, healthcare, and secure access systems.

Conclusion

- **Enhanced Security**: The proposed system offers a strong protection against spoofing and breaches.
- **Portability**: The system's design allows for mobile and remote authentication.
- **Decentralized Storage**: The system ensures decentralized data storage by using blockchain technology.
- **Accurate Authentication**: The use of CNN for vein pattern analysis ensures precise and reliable biometric authentication.
- **Innovative Combination**: Integrating NIR imaging, blockchain, and machine learning provides a comprehensive, secure, and portable solution for remote biometric authentication.

Future Scope

- In the future, this prototype can be expanded into a full-fledged commercial system with enhanced hardware for faster and more accurate image acquisition.
- Integration with mobile platforms and cloud-based authentication can increase accessibility and scalability.
- Further improvements in deep learning models and security mechanisms, such as multi-factor biometric authentication and advanced encryption methods, can make the system more robust.
- Additionally, real-time deployment in sensitive environments like banks, hospitals, and smart devices can validate its practical use and encourage wider adoption.

References

[1] Xuebing, W., Z. Jiangwei, and L. Xuezhang. 2010. Research on Enhancing Human Finger Vein Pattern Characteristics. Asia-Pacific Conference on Power Electronics and Design (APED).
[2] Singh, B., N. Kapur, and P. Kaur. 2012. Speech Recognition with Hidden Markov Model: A Review. International Journal of Advanced Research in Computer Science and Software Engineering. 2(3): 400-403.
[3] Kulkarni, S. and D.R. Raut. 2014. Finger Vein Recognition. IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE). pp. 32-36.
[4]Ahmed, M.R., Islam, A.M., Shatabda, S., Islam, S.: Blockchain- based identity management system and self-sovereign identity ecosystem: a comprehensive survey. IEEE Access 10, 113436–113481 (2022)
[5]Al-Saggaf, A.A.: A post-quantum fuzzy commitment scheme for biometric template protection: an experimental study. IEEE Access 9, 110952–110961 (2021)
[6]Al-Waisy, A.S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., Nagem, T.A.: A multi-biometric iris recognition system based on a deep learning approach. Pattern Anal. Appl. 21, 783–802 (2018)

References

[7]Aste, T., Tasca, P., Di Matteo, T.: Blockchain technologies: the foreseeable impact on society and industry. Computer 50, 18–28 (2017)
[8]Sharma, P.; Jindal, R.; Borah, M.D. A review of blockchain-based applications and challenges. *Wirel. Pers. Commun.* **2022**, *123*, 1–43.
[9]Panda, S.K.; Mishra, V.; Dash, S.P.; Pani, A.K. *Recent Advances in Blockchain Technology: Real-World Applications*; Springer: Cham, Switzerland, 2023.
[10]Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [11]Vidakovic´, M.; Milic˘evic´, K. Performance and Applicability of Post-Quantum Digital Signature Algorithms in Resource- Constrained Environments. *Algorithms* **2023**, *16*, 518.
[11] B. Moayer and K.-S. Fu, ''A tree system approach for fingerprint pattern recognition,'' IEEE Trans. Comput., vol. C-25, no. 3, pp. 262–274, Mar. 1976.

References

[12] M. Turk and A. Pentland, ''Eigenfaces for recognition,'' J. Cognit. Neurosci., vol. 3, no. 1, pp. 71–86, Jan. 1991.
[13] R. P. Wildes, J. C. Asmuth, G. L. Green, S. C. Hsu, R. J. Kolczynski, J. R. Matey, and S. E. McBride, ''A system for automated iris recognition,'' in Proc. IEEE Workshop Appl. Comput. Vis., Feb. 1994, pp. 121–128.
[14] M. Kono, ''A new method for the identification of individuals by using of vein pattern matching of a finger,'' in Proc. 5th Symp. Pattern Meas.,
Yamaguchi, Japan, 2000, pp. 9–12.
[15] N. Miura, A. Nagasaka, and T. Miyatake, ''Feature extraction of finger- vein patterns based on repeated line tracking and its application to personal identification,'' Mach. Vis. Appl., vol. 15, no. 4, pp. 194–203, Oct. 2004.

Thank You

Appendix B: Vision, Mission, Programme Outcomes and Course Outcomes

Vision, Mission, Programme Outcomes and Course Outcomes

Institute Vision

To evolve into a premier technological institution, moulding eminent professionals with creative minds, innovative ideas and sound practical skill, and to shape a future where technology works for the enrichment of mankind.

Institute Mission

To impart state-of-the-art knowledge to individuals in various technological disciplines and to inculcate in them a high degree of social consciousness and human values, thereby enabling them to face the challenges of life with courage and conviction.

Department Vision

To become a centre of excellence in Computer Science and Engineering, moulding professionals catering to the research and professional needs of national and international organizations.

Department Mission

To inspire and nurture students, with up-to-date knowledge in Computer Science and Engineering, ethics, team spirit, leadership abilities, innovation and creativity to come out with solutions meeting societal needs.

Programme Outcomes (PO)

Engineering Graduates will be able to:

1. Engineering Knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. Conduct investigations of complex problems: Use research-based knowledge including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. Modern Tool Usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

6. The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal, and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. Individual and Team work: Function effectively as an individual, and as a member or leader in teams, and in multidisciplinary settings.

10. Communication: Communicate effectively with the engineering community and with society at large. Be able to comprehend and write effective reports documentation. Make effective presentations, and give and receive clear instructions.

11. Project management and finance: Demonstrate knowledge and understanding of engineering and management principles and apply these to one's own work, as a member and leader in a team. Manage projects in multidisciplinary environments.

12. Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and lifelong learning in the broadest context of technological change.

Programme Specific Outcomes (PSO)

A graduate of the Computer Science and Engineering Program will demonstrate:

PSO1: Computer Science Specific Skills
The ability to identify, analyze and design solutions for complex engineering problems in multidisciplinary areas by understanding the core principles and concepts of computer science and thereby engage in national grand challenges.

PSO2: Programming and Software Development Skills
The ability to acquire programming efficiency by designing algorithms and applying standard practices in software project development to deliver quality software products meeting the demands of the industry.

PSO3: Professional Skills
The ability to apply the fundamentals of computer science in competitive research and to develop innovative products to meet the societal needs thereby evolving as an eminent researcher and entrepreneur.

Course Outcomes (CO)

After the completion of the course the student will be able to:

Course Outcome 1: Identify academic documents from the literature which are related to her/his areas of interest (Cognitive knowledge level: Apply).

Course Outcome 2: Read and apprehend an academic document from the literature which is related to his/her areas of interest (Cognitive knowledge level: Analyze).

Course Outcome 3: Prepare a presentation about an academic document (Cognitive knowledge level: Create).

Course Outcome 4: Give a presentation about an academic document (Cognitive knowledge level: Apply).

Course Outcome 5: Prepare a technical report (Cognitive knowledge level: Create).

Appendix C:
CO-PO-PSO Mapping

COURSE OUTCOMES:

After completion of the course, the student will be able to:

SL.NO	DESCRIPTION	Bloom's Taxonomy Level
CO1	Model and solve real-world problems by applying knowledge across domains.	Level 3: Apply
CO2	Develop products, processes, or technologies for sustainable and socially relevant applications.	Level 3: Apply
CO3	Function effectively as an individual and as a leader in diverse teams and comprehend and execute designated tasks.	Level 3: Apply
CO4	Plan and execute tasks utilizing available resources within timelines, following ethical and professional norms.	Level 3: Apply
CO5	Identify technology/research gaps and propose innovative/creative solutions.	Level 4: Analyze
CO6	Organize and communicate technical and scientific findings effectively in written and oral forms.	Level 3: Apply

CO-PO-PSO Mapping Matrix

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	2	2	2	1	2	2	2	1	1	1	1	2	3	2	2
CO2	2	2	2	1	1	3	3	1	1	1	1	1	2	2	2
CO3	1	1	1	1	1	1	1	1	3	2	2	1	1	2	3
CO4	1	1	1	1	2	1	1	3	2	2	3	2	2	2	3
CO5	2	3	3	1	2	2	2	1	1	1	2	1	3	3	2
CO6	1	1	1	1	2	1	1	2	2	3	1	1	2	2	3

Note: 3 – High, 2 – Medium, 1 – Low

JUSTIFICATIONS FOR CO-PO-PSO MAPPING

Mapping	Level	Justification
CO1		
CO1 - PO1	M	Applies fundamental knowledge from electronics, computing, and AI to design biometric authentication hardware.
CO1 - PO2	M	Solves real-time problems in biometric systems using practical engineering techniques.
CO1 - PO3	M	Designs deep learning models for vein recognition with high accuracy.
CO1 - PO4	L	Integrates technologies to build functional, resource-optimized solutions.
CO1 - PO5	M	Combines IoT, AI, and blockchain in practical implementations.
CO1 - PO6	M	Evaluates security and privacy aspects of biometric authentication.
CO1 - PO7	M	Analyzes societal impacts of biometric systems in public sectors.
CO1 - PO8	L	Considers ethical and legal issues regarding data protection.
CO1 - PO9	L	Demonstrates team collaboration during system integration.
CO1 - PO10	L	Documents solution architecture and communicates results clearly.
CO1 - PO11	L	Manages resources across domains while developing prototypes.
CO1 - PO12	M	Demonstrates adaptive learning in blockchain and biometric fields.
CO1 - PSO1	H	Implements CNNs for image preprocessing and template generation.

CO1 - PSO2	M	Ensures data confidentiality with cryptographic measures.
CO1 - PSO3	M	Integrates system modules into a complete real-time solution.
CO2		
CO2 - PO1	M	Applies core engineering knowledge to develop impactful biometric applications.
CO2 - PO2	M	Formulates sustainable and socially relevant problem statements.
CO2 - PO3	M	Designs and develops secure biometric and blockchain-based solutions.
CO2 - PO4	L	Demonstrates preliminary analysis and experimentation for sustainable solutions.
CO2 - PO5	L	Selects relevant technologies for low-power, sustainable biometric hardware.
CO2 - PO6	H	Analyzes societal and environmental impacts of biometric deployment.
CO2 - PO7	H	Designs solutions aligned with societal needs such as healthcare or ID systems.
CO2 - PO8	L	Considers data ethics and consent during solution implementation.
CO2 - PO9	L	Collaborates with team members on product-oriented projects.
CO2 - PO10	L	Shares progress and concepts clearly during group discussions.
CO2 - PO11	L	Applies engineering management for timely project delivery.
CO2 - PO12	L	Demonstrates continuous learning in sustainable biometric design.

CO2 - PSO1	M	Uses AI models to create optimized solutions for community use.
CO2 - PSO2	M	Applies secure communication protocols for public-facing systems.
CO2 - PSO3	M	Deploys and validates the complete biometric authentication setup.
CO3		
CO3 - PO1	L	Applies basic engineering knowledge while coordinating technical teams.
CO3 - PO2	L	Understands problems and guides group members during design and analysis.
CO3 - PO3	L	Contributes to planning and assigning implementation tasks.
CO3 - PO4	L	Applies mathematical and programming knowledge to assist in task automation and tool development.
CO3 - PO5	L	Collaborates on component selection and interfacing for biometric systems.
CO3 - PO6	L	Considers stakeholder needs while managing task priorities.
CO3 - PO7	L	Discusses social concerns and privacy during teamwork.
CO3 - PO8	L	Follows professional and ethical practices while managing team activities.
CO3 - PO9	H	Leads cross-functional teams in system development.
CO3 - PO10	M	Communicates team objectives, project reports, and updates.
CO3 - PO11	M	Coordinates time and resources efficiently within teams.
CO3 - PO12	L	Updates self and team with the latest trends for project success.

CO3 - PSO1	L	Assists team in model training and performance improvement.
CO3 - PSO2	M	Discusses cryptographic implementation during peer collaboration.
CO3 - PSO3	H	Leads the full-system demonstration as team representative.
CO4		
CO4 - PO1	L	Uses basic engineering principles to plan activities.
CO4 - PO2	L	Identifies practical limitations and plans accordingly.
CO4 - PO3	L	Structures implementation phases within time constraints.
CO4 - PO4	L	Analyzes time-resource trade-offs for task execution.
CO4 - PO5	M	Selects relevant components and interfaces for prototype efficiency.
CO4 - PO6	L	Incorporates safety, privacy, and reliability norms.
CO4 - PO7	L	Maintains eco-conscious decisions in planning stages.
CO4 - PO8	H	Adheres to ethical practices for biometric data collection and storage.
CO4 - PO9	M	Plans group tasks and facilitates collaboration.
CO4 - PO10	M	Presents progress to guide team and supervisors.
CO4 - PO11	H	Manages multiple modules simultaneously with accountability.
CO4 - PO12	M	Adapts quickly to shifting requirements and deadlines.
CO4 - PSO1	M	Organizes AI pipeline tasks effectively.
CO4 - PSO2	M	Applies secure access methods following system architecture.
CO4 - PSO3	H	Oversees full lifecycle of the solution and deployment.

CO5		
CO5 - PO1	M	Applies foundational knowledge to identify gaps in current systems.
CO5 - PO2	H	Formulates and validates hypotheses for improving biometric security.
CO5 - PO3	H	Designs novel architectures integrating blockchain and biometrics.
CO5 - PO4	L	Performs initial simulations and data analysis for innovation.
CO5 - PO5	M	Selects unique configurations to validate proposed improvements.
CO5 - PO6	M	Addresses ethical and risk implications during ideation.
CO5 - PO7	M	Evaluates long-term social impacts of proposed tech upgrades.
CO5 - PO8	L	Ensures legal compliance and privacy norms in proposals.
CO5 - PO9	L	Shares findings and proposes ideas to peers and mentors.
CO5 - PO10	L	Documents comparative analysis and experimental outcomes.
CO5 - PO11	M	Plans pilot projects to test innovative components.
CO5 - PO12	L	Explores updated technologies and research regularly.
CO5 - PSO1	H	Proposes new deep learning techniques for authentication.
CO5 - PSO2	H	Suggests novel blockchain-based cryptographic approaches.
CO5 - PSO3	M	Integrates advanced modules to enhance current systems.

CO6		
CO6 - PO1	L	Applies foundational understanding to structure technical reports.
CO6 - PO2	L	Analyzes experimental outcomes for publication-quality presentation.
CO6 - PO3	L	Articulates project contributions effectively through documentation.
CO6 - PO4	L	Organizes data and findings for systematic reporting.
CO6 - PO5	M	Uses tools and software to illustrate results and graphs.
CO6 - PO6	L	Ensures clarity in safety and security-related disclosures.
CO6 - PO7	L	Highlights the benefits and societal impacts through reports.
CO6 - PO8	M	Acknowledges ethical considerations in publications.
CO6 - PO9	M	Collaborates and contributes to team discussions and documentation.
CO6 - PO10	H	Demonstrates high proficiency in report writing, poster creation, and oral presentations.
CO6 - PO11	L	Compiles contributions from different modules into a unified report.
CO6 - PO12	L	Reflects on learnings in final documentation.
CO6 - PSO1	M	Explains model training and evaluation details.
CO6 - PSO2	M	Communicates cryptographic mechanisms and protocols clearly.
CO6 - PSO3	H	Provides full demo of system with Q&A and interpretation.