National College of Ireland

Biometric based Fingerprint Verification System using Deep Learning for Secure Cloud Storage

MSc Research Project
MSc in Cybersecurity

Chenu Saiteja
Student ID: 23149132

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Chenu Saiteja
Student ID:	23149132
Programme:	Msc in Cybersecurity **Year:** 2024
Module:	Practicum
Supervisor:	Mark Monaghan
Submission Due Date:	12-08-2024
Project Title:	Biometric based Fingerprint Verification System using Deep Learning for Secure Cloud Storage
Word Count:	**Page Count**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Chenu Sai Teja

Date: 12-08-2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Biometric based Fingerprint Verification System using Deep Learning for Secure Cloud Storage

Chenu Sai Teja
23149132

Abstract

This project provides the fingerprint identification system which is accurate for this type of biometric as well by using SNN to increase rate of Biometric Recognition. This is the primary structure of proposed system SNNs for improved accuracy matching Fingerprint to provide strength security cloud distribution systems. This solution personalized an intuitive customer biometric approach interoperable with the cloud in order to follow best-in-class data privacy and security principals. Protecting not only biometric data in the cloud, as well as any other information uploaded to public servers anywhere it is the Holy Grail of cloud security. This might sound quite a bit over-specified, but the results were pretty good: it answers correctly with 99.67% on Robust. Classification report: accuracy and F1-score 100%. Therefore, this system is believed to be an innovative new technique in the secure data publication for guaranteeing protection of individual and organizational information released below cloud integration.

1 Introduction

The widespread adoption of cloud storage services in the 21st century further highlights why strong authentication measures are crucial when it comes to protecting confidential data. Although traditional access techniques are both vast and far-reaching, these often lack in precision, security or user experience resulting at times into being a victim of attack on unauthorised entry. This means, it is also implied that More advanced protection have to be developed as a way to keep the information stored inside the cloud relaxed regarding facts integrity and confidentiality.

There is a hopeful catch here as well that the system could be made secure by applying some Deep Learning based Biometric fingerprint verification solutions. It increases the accuracy and reliability of user authentication, also it brings a lot to enhance the users experience by making easy for them to get authenticate in seamless way with security at their base level. Deep learning algorithms, especially the state of the art Convolutional Neural Networks (CNNs) and Siamese Neural networks (SNNs), have shown strong promise in improving biometric verification systems.

The specific research question that this study seeks to address is as follows:

- Where Does Siamese Neural Network Fit in to Enhance Fingerprint Verification Accuracy and Biometric Security Fusion with Webbased Cloud Storage System?

This research, in nutshell will develop a deep learning based fingerprint verification system that can be implemented with the help of CNNs and SNNs; analyze how efficient our proposed solution is when evaluated on accuracy metric along some other evaluation metrics including precision recall F1score etc., check if integrating biometric authentication for cloud storage results into increased security level while maintaining user satisfaction.

The novelty of this work lies in providing a new secure biometric authentication methodology using deep learning technologies, the usability of CNNs and SNNs to practical fingerprint verification process, thus demonstrating that we can make our model applicable to wides display type research at all levels with ireopedent as well proof it empirically.

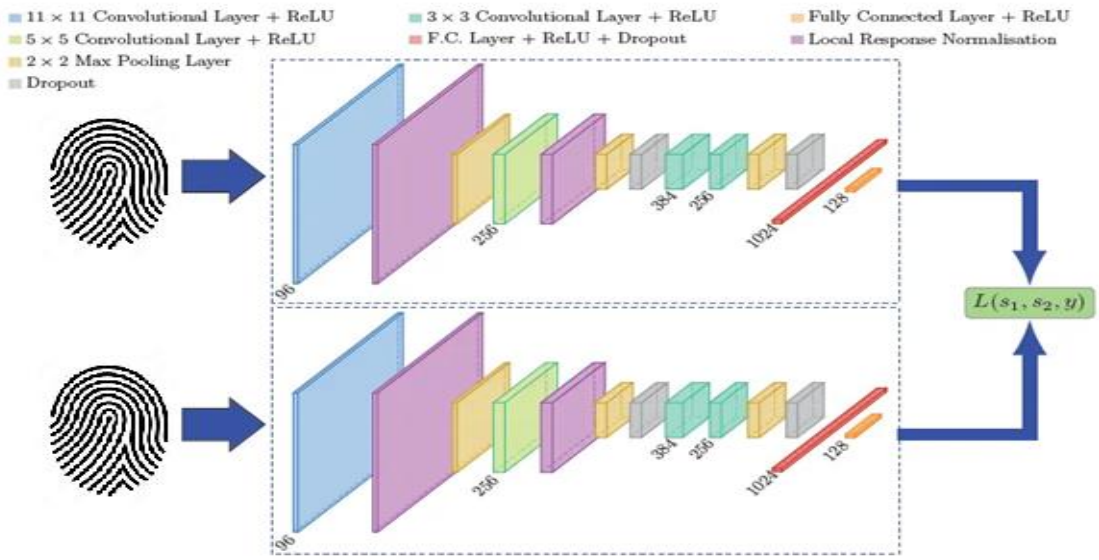

Figure 1: Siamese Neural Networks[1]

The rest of this report was organized as follows: in Chapter 1 the introduction discussed anachronism during traditional fingerprint matching sets a timeline and motivation needs for cloud storage security with deep learning based biometric based fingerprint verification, research objectives presented their problem formulation including report structure. Chapter 2 provided an overview on Existing Classifications and Implementation of Deep Learning into Fingerprint Verifier System Chapter 3 : Dataset, Model Architecture and Evaluation Metrics In this chapter we explained the dataset used in ours experiments here, model architecture that is already listed above, evaluation metric. Chapter 4 described the experimental results, showed these using classification reports and confusion matrices. Results were then interpreted in chapter 5, benchmarked against the state of art and importance for future research was discussed. The findings, contributions to the field, and potential future work were all summarized in Chapter 6.

---

[1] https://towardsdatascience.com/afriendlyintroductiontosiamesenetworks85ab17522942

2 Related Works

The related work on latent and mobile authenticated cloud biometric matching methods provided detailed enhancements in these areas. Due to this, several studies have shown that deep learning by itself and with new protocols is able to increases the accuracy and security of biometric identification embedding systems in different applications.

Latent Fingerprint Matching

Deep learning has made enormous leaps in latent fingerprint matching. Ezeobiejesi and Bhanu (2018) proposed a new way to match latent fingerprints with corresponding rolled latents using deep learning network for patch representation optimization and convolutional neural network (CNN) for similarity score computation. Their system achieves an impressive rank I identification rate of 81.35% on the large NIST SD27 and introduces new SD4 datasets by combining patch based with minutia based similarity scores, outperforming previous best results of 74%. This improved the accuracy and robustness of this matching, showing how these paradigms might be exploited in forensic applications. The study also identified directions for future research as the development of deep learning based minutiae extraction methods and testing the approach on bigger, diverse databases to reinforce its efficacy (Ezeobiejesi &

Bhanu 2018). Finally, this work proves how powerful deep learning in biometric identification tasks is enough to operate on difficult circumstances (such as with latent fingerprints).

Biometric Based Cloud Authentication

Biometric-based authentication protocols are promising to improve security and usability in the domain of cloud security. Panchal et al. (2022) proposed a complex mechanism, in which biometric features were leveraged as the means of generating secret credentials to construct private and session keys without having to load or share any key. In this way, the coherence and intrinsic security provided by biometric traits are used to secure access control for cloud servers. The protocol was formally analyzed for security and shown to be secure against a variety of attacks like replay or maninthemiddle. Experiments showed that the key generation method based on fingerprint data has a precision rate of 95.12%, thus proving it to be practical and highly effective as well. The authors proposed future research towards studying other biometric modes of identity such as multimodal biometrics which can offer extra security for high impact applications (Panchal et al. 2022). The importance of biometrics in new authentication systems for cloud scenarios is a critical element emphasized in this study.

Privacy Preserving and Cancelable Biometrics

Cloud computing premises are also heavily reliant on privacy-preserving and cancelable biometric systems to protect the user data. Sudhakar and Gavrilova (2020) proposed a cancelable biometric system using pretrained deep learning models for feature extraction, yielding excellent accuracy of 99.55%. With this method, even after biometric data is leaked they can still be revoked and do not affect the security of the system. Similarly, Prabhu et al. (2022) proposed a steganography and encryption-based biometric authentication system that securely sends fingerprint data, improving the security of storing in cloud environment. Liu et al. (2019) A second contribution aimed to mitigate security threats in biometric identification protocols, by introducing a method proven secure against known-plaintext attacks and improved computational efficiency compared to the state-of-art counterparts. This highlights the necessity to design biometric system which not only provide high identification accuracy but also protect user privacy and are robust against diverse attacks (Sudhakar et al., 2020; Prabhu et al., 2022; Liu, Liu et al., 2019). The innovations in privacy-preserving biometrics are also a key enabler to trust and the uptake of biometric technologies within cloud computing.

Continuous Authentication and Anti Spoofing

Inclusion of continuous authentication and antispoofing within the biometric systems is a vital feature to uplift its security as well credibility. Uslu et al. (2003) In the same year also evaluated deep learning models on continuous authentication from behavioral biometrics, making it possible to verify users using a non-intrusive and plausible way with high accuracy rates. It uses the idea of behavioural authentication technology to extend specialized enterprise software that access desktop / web resources and further retrieves user activities against those data streams related which application domain. Gumaei et al. (2019) proposed a cloud based fingerprint identification anti-spoofing system which used an optimized combination of the state-of-the-art methods for identity verification with secure encryption against spoof attacks. Their method was able to successfully detect live fingerprints, while efficiently detecting any spoofed biometric input that were used for unauthorized access. Additionally, Yang et al. (2022) presented protocols for outsourcing biometric identification that are eficient, secure and privacypreserving which could be an absolute need of the industry when a cloud solution becomes popularized. Thirdparty cloud services used for biometric data processing must adhere to the abovementioned protocols, assuring insoluble authentication and privacy mechanisms (Uslu et al., 2023; Gumaei et al., 2019; Yang et al., 2022). Given the growing complexity and threat landscape, continuous authentication and antispoofing technologies are necessary to ensure that biometric systems remain secure.

Gap Analysis

The gap analysis demonstrated that although a significant improvement was made in areas like latent fingerprint matching, biometric-based cloud authentication and privacy preserving techniques, there still were some deficiencies. Although some studies have been done, most of these literature are focus on the traditional machine learning algorithm and this approach limited our studying object into Siamese neural networks to technically achieve more accurate fingerprint matching. There also remained difficulty in associating degraded fingerprint images, with matching performance dropping substantially under challenging conditions to date. This study provided enlightenment to the research community for further investigations in fusion of Siamese Neural model and proposed a stronger methodology, which can accommodate abnormal test based fingerprint images.

3 Research Methodology

In this chapter we provide the research methodology used to perform an analysis and improvement of secure storage based on a deep learning method for fingerprint verification. This includes the research process, its tools or techniques used as well as various types of scenarios being set up along with method discussed to conduct the data and use suitable analyzation.

3.1 Research Procedure

The following research procedure was followed to build fingerprint verification system that can withstand various types of deceptions:

Literature Review: A comprehensive literature review was conducted on available works in the areas of latent fingerprint matching, biometric based cloud authentication, privacy preserving and cancelable biometrics, continuous authentication techniques to identify research gap and develop an approach.

Data Collection: A large dataset of fingerprint images was collected. The dataset consists of a variety of sizes and resolutions for better noise resistance. Before training deep learning models, images were preprocessed to standardize dimensions and hence dimensions of the feature space, which eased model development efforts, as mentioned earlier; and also improved performance.

Model Selection and Architecture Design: Reviewing the literatures, a Siamese Neural network (SNN) architecture was selected on account of its efficiency in back grounding one shot learning levels, thereby improving accuracy of fingerprint matching. The SNN was built using a few convolutional feature extraction layers and contrastive loss function to train similarity scores.

Implementation and Training: SNN dense model was implemented using TensorFlow with Keras. Training, validation and test splits. The model was trained in successive iterations while keeping an eye on the learning curve to avoid overfitting.

Evaluation: Accuracy, precision, recall and F1scores were the evaluation metrics used to evaluate our model performances. I was evaluating this model by creating classification reports and confusion matrices for it to understand how well our model would work in reality.

Deployment: The model was evaluated and deployed to a Cloud Storage authentication system as part of our stable real-world benchmarks configurations.

3.2 Equipment and Tools

Software Requirements: Windows 10 (64-bit), Python 3, Anaconda, Flask, Keras, TensorFlow, OpenCV, Matplotlib, Scikit-learn, Numpy & Pandas, Jupyter Notebook with Notepad++ Editor, Anaconda Navigator, and tools for data visualization and machine learning.

Hardware Specifications: 1TB+ hard disk, Intel core i5 / i7 and at least 8/12GB of ram (useful for all deep learning model training) high spec compute resources such as GPUs or cloud based options.
Data Sets : The next Dataset[2] is the Sokoto Coventry Fingerprint Images Dataset (SCOFing) which is a fingerprint database containing images of 600 African people in total with 6,000 images where the images are further labeled with hand, finger's name, as well as the subject's gender. Dataset link-

3.3 Techniques Applied

Siamese Neural Network (SNN): This is the main technique applied as it gives one-shot learning power to use. Two neural networks with shared weights. The first layer operates on one of the input images, and performs convolutional layers to extract features at subnetwork processing unit level. We measure the distance between these feature vectors using a contrastive loss, which helps teach our network to distinguish similar versus dissimilar fingerprint pairs.
Convolutional Neural Network (CNN): In the SNN, CNN is utilized to extract significant features from finger-print images. Its architecture consists of number of convolutional layers with pooling to capture spatial hierarchies and reduce dimensionality. Using the CNNs we generate feature vectors and these final feature vectors are compared in similarity.
Contrastive Loss Function: It trains the SNN with Contrastive Loss Function. It does so by reducing distance of feature vectors/codelines in same fingerprint pairs, but maximizes the distance between unrelated coders and features. Or in other words, The Contrastive Loss is formally:

$$L = (1 - Y) \cdot \frac{1}{2}(D_W^2) + (Y) \cdot \frac{1}{2}\{\max(0, m - D_W)\}^2$$

Y is the binary label of if pairs are similar or distinct, m is margin between different categories, $\mathbf{D_W}$ can be trained by network .

---

[2]https://www.kaggle.com/datasets/ruizgara/socofing

3.4 Data Collection and Pre-processing

Data Standardization: Here all the fingerprint images are resized to a uniform size and made them standard for both transferring less noisy image while training, testing.

Real **Easy** **Medium** **Hard**

Figure 2: Types of Fingerprint Images

Types of Fingerprint Images

1. Real: Controlled Conditions allowed for in high-quality, clear images. These will be our benchmarks that the SNN is compared to on ideal conditions.

2. Easy: Less quality images with visible ridge and valley structures. These are meant to mimic small amounts of wear or natural environmental changes that the SNN will need to be able handle just through working day-to-day.
3. Medium: Images with some degradation such as smudging or partial occlusion. They provide a challenging for SNN robustness in less than ideal conditions.
4. Hard: Images are extremely distorted, some perhaps to the point of damage making them almost entirely unrecognizable from a starting image. This class evaluates the trustworthiness in highly corrupted settings of an SNN.
Data paring: A total volume set was shaved down to 6000 images for fingerprint data training and testing purpose on Siamese Neural Network (SNN) based biometric/smart card finger print verification domain. The dataset contains four different types of fingerprint images, comprising real and faded ones (real; easy; medium or hard).
Positive Pairs: These are two images of fingerprint that belong to the same finger and hence, the same person. For example, two images from the left index finger of that person (even if captured in different conditions say real-easy-medium-hard)
Negative Pairs: A pair of fingerprint images from different fingers or different individuals. This could mean verifying an image of a 1st finger VS thumb (same person) or an unmatched comparison between images.
Pairing Process

To train the SNN well, fingerprint images appear in pairs:

Positive Pair Generation: Created by two images that come from the same finger of a single individual Balancing the four categories of images will allow a balanced training experience for our model.
Negative Pair Generation: Pairs from various finger images; pairs of two individuals Include different negative pairs to make the dataset balanced that will avoid a bias during training.
It would guarantee that SNN learns the matching as in one fingerprint image corresponding to another or not as real-life fingerprints could be damaged or partially occluded, improving overall accuracy of network performance.

Normalization: Normalization takes place only in the images that rescale pixel values to have a range of [0, 1] for making model training easier and faster.

3.5 Statistical Analysis

Performance Metrics: Calculated performance metrics (accuracy, precision, recall and F1score) for a range of hyper-parameters. All these metrics ensure a very good analysis of the performance in classifying the fingerprint pairs correctly by each model.

Classification Report: This report describes the precision, recall and F1score of a matching as well as non-matching fingerprint pairs per class (matching/non-matching). This report enables one to gauge how well the model does in terms of predictive accuracy across classes and helps identify any training biases.

Confusion Matrix: This is used to view the performance of how your model did. It tells you how many true positives, false negatives, positions of negative and positive are there which in turn provides an understanding about the accuracy level of classification.

3.6 Steps from Data Collection to Final Results

Dataset Preparation: Selection of fingerprint images and Preprocessing.
Model Design and Training: Implementation of SNNCNN model, Training in iterations.
Model Evaluation: Assessment using classification reports and confusion matrices.
Deployment: Integration as a cloud storage authentication.

Results Analysis: Validation of the model against performance metrics.

The proposed methodology provides a detailed systematic approach to developing and validating a species of the Deep learning-based fingerprint verification system. The method will play a significant role in addressing the security concern of cloud storage.

4 Design Specification

Here is a specification of the fingerprint authentication system using Siamese Neural Network (SNN). It learns to differentiate between legitimate and impostor users using a dataset of matching fingerprint pairs. Packed with an access control page, helps secure cloud storage and only allows the right persons to download files via fingerprint. Access control is established as admins and data owners need to sign up. It is a scalable system that also satisfies the security features needed for secure data access and SNN-based model training.

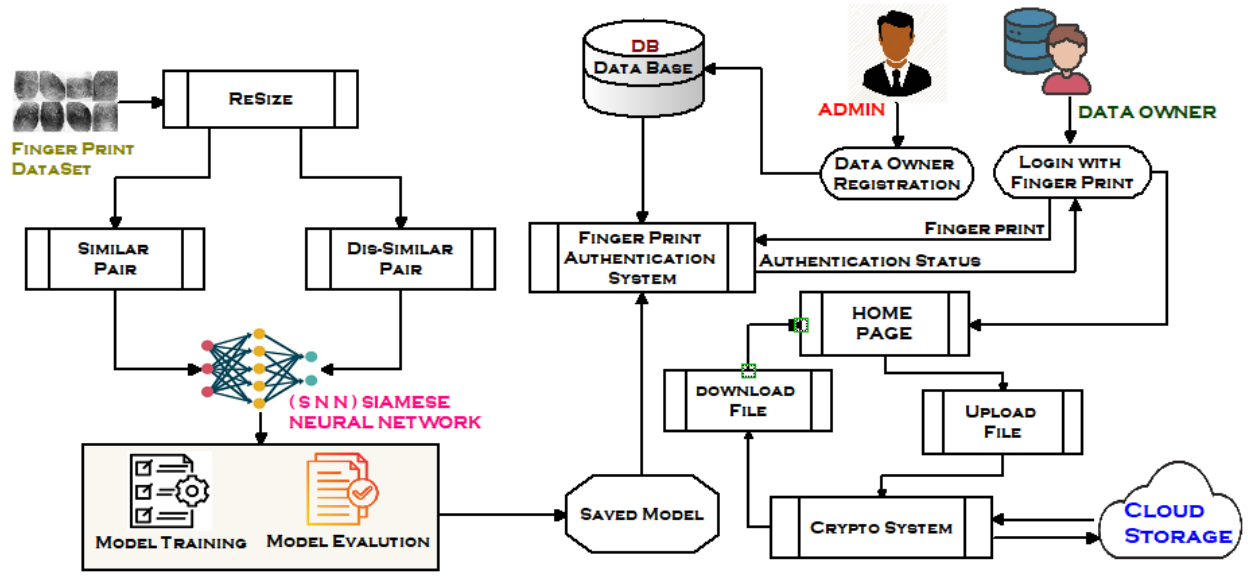

Figure 3: System Architecture

In Figure 3 Secure and Efficient Data Holder Authentication with Fingerprint Based Access in a Cloud Figure is made for the security aware authentication technique used to authenticate data owners based on their fingerprints & cloud storage management. It first starts by gather fingerprint dataset$_2$ then use the same to train Siamese Neural Network in order to evaluate similarity b/n pairs of fingerprints. After training and evaluation, the model is saved to be used in authentication in future. It has a fingerprint authentication system; fingerprints data are stored in our database and the owner information.

Whenever a data owner tries to enter in system they should log using their finger print., the same will be checked against its stored database. You can access the home page only if your fingerprint matches. Being administered by a system admin, the user can enroll new data owners and run database. Admin Home, request downloads on files. Data producers can push their files to the cloud and they are securely placed in storage; authorized users download these according with permissions. There is also a request file download feature for users to ask files be placed from the cloud storage.

Architecture and Framework

In the authentication system the Siamese Neural Network (SNN) is a key part When two fingerprint images (pictures) are compared for likeness, SNN is at ease one-shot learning tasks. During the training process, the fingerprint dataset is prepared by resizing it and then splitting into similar and dissimilar pairs, which ensures that SNN can distinguish between matching and non-matching fingerprints. Two subnetworks with identical configuration are used to process input images produce feature vectors for the comparison function, and a distance metric such as Euclidean distance is then applied in order to yield the similarity rating between them. The authenticated SNN model is used for authentication purposes after being tested rigourously. Cloud uploads are protected using RSA encryption, meaning that it is encrypted before being uploaded to the cloud and decrypted when downloaded. The system is divided into two roles: where Admin help to manage the accounts and fingerprints of data owner in a secure way, so here Data Owners authenticate themselves with fingerprint + password to get access on the cloud upload their files & securely keep track of them. Features like access control settings and file management are easily found in the front-end interface which, using RSA encryption methods for confidential data transfer throughout.

5 Implementation

A secure, efficient & well-deserved cloud storage solution The end result a working biometric-based fingerprint verification system employs the five requested elements that together constitute an effective alternative to existing solutions already in use. This section also details the last phase of implementation, detailing outputs created and tools used.

5.1 System Overview

The system offers a secure file upload and download services for data owners via biometric authentication (along with plain password) as an identity. Creation of data owners can be done by admin Using the cloud you generate and manage keys for encryption of file uploads with RSA algorithm.

5.2 Front-End Development

The front-end interface for data owners and admin is straightforward to use. Assembled using standard web technologies (HTML, CSS and JavaScript), data owners can access the interface by fingerprint biometric in combination with password as credentials. It allows for secure file upload and downloading. An admin interface is made to create and manage data owners, including setting permissions for accessing the files, transactions of these files. The interface makes sure that the relationship with a cloud storage system is secure and easy to navigate. Few of the Important Key System Functions is:

Admin Functions: The admin has the responsibility to create and maintain accounts of data owner can be seen in Figure 3 by providing secure and effective management over users. This entails the addition of new users, dealing with user lists and access rights to ensure that only those who should be allowed in can get through it.

Log In: Data owners in Figure 4 can access the system in a more secure way for their fingerprints and passwords with which they have always been authenticated by using. This two-level, user verification model makes the system more secure as only valid users would be able to read/write-any-data.

Manage Files: There are places for people to put their files with safe uploading and downloading, whereby encryption will provide a layer that preserves the integrity of suspect data. An example of this capability is shown in Figures 5 and 6 Files are encrypted with the RSA encryption algorithm before uploading to provide users an extra layer of security, protecting their files from both upload and download. It allows users to easily and securely handle their files.

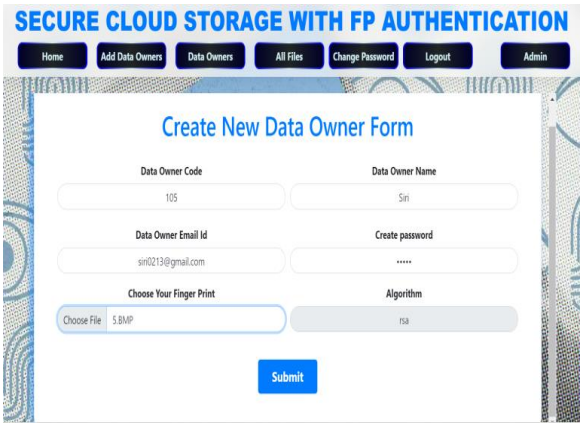

Figure 3: Admin Functions

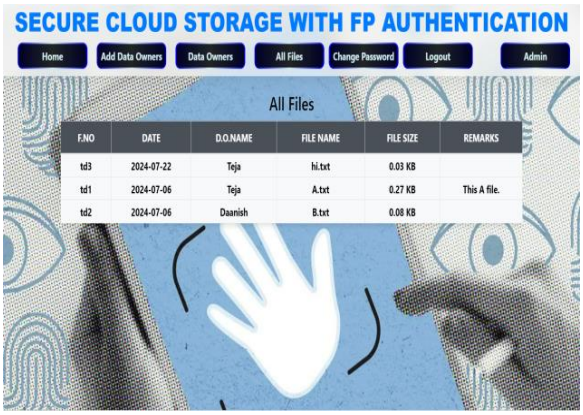

Figure 5: Data uploaded

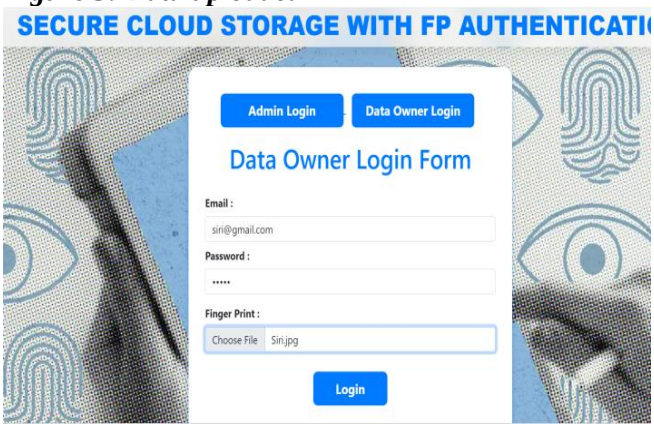

Figure 4: Data owner Authentication

Figure 6: Data Downloaded

5.3 Encryption and Cloud Storage

After authenticating, the clients are allowed to upload files and it is as well encrypted with RSA. It auto-generates the keys and securely stores them on your cloud account. With cloud storage the encrypted files are stored securely and only authorized users can access them.

5.4 Biometric Authentication:

The biometric authentication part takes a Siamese Neural Network (SNN) trained with an extensive database of fingerprint images. A set of different types of fingerprints such as realistic, easy, medium and hard images are used to assess the performance of SNN. This leads to reliable authentication even when the system faces conditions like scratched, wet or oily fingers.

5.5 Outputs Produced:

The function is used to describe the image formation process, which defines uniquely everything about a scene that carries visual information stored in clouds by encrypting these footprints using RSA public-private key pairs. The codebase includes an SNN model written in TensorFlow/Keras and a front-end interface based on web development frameworks. These trained models will be SNN which is able to generalise well over 6000 fingerprint images under various conditions. Encryption of files through, RSA encryption can provide security features Data owner interface a secure way to log in, manage the file and take / login activity. This all contributes to a better biometric verification and data storage in secure way.

6 Evaluation& Testing

The testing and evaluation of the Siamese Neural Network (SNN) as well as Convolutional Neural Network(CNN) implemented in fingerprint verification are discussed in this chapter. This report is made up of a comprehensive analysis on model performance, the implications of results and visual aids to accompany findings. This process is necessary to ensure that the system conform with the research goals and give consistent results in an real-world environment.

Key Performance Indicators measuring the capabilities of fingerprint authentication system for accuracy, precision, recall and F1score are evaluated. These metrics were computed on prediction over validation data.

6.1 Model Performance

The fingerprint verification system used the Convolutional Neural Network (CNN) model and delivered an accuracy rate. The high accuracy level It provides indicates it can differentiate true and false fingerprints.

Convolutional Neural Network (CNN) Classification Report

Using classification report and confusion matrix figure 7 shows the performance of fingerprint classification model based on CNN.

	precision	recall	f1-score	support
0	1.00	0.99	1.00	140
1	0.99	1.00	1.00	160
accuracy			1.00	300
macro avg	1.00	1.00	1.00	300
weighted avg	1.00	1.00	1.00	300

Figure7: Classification Report for CNN

Model accuracy was at a perfect 99.67 %, all samples were correctly classified as expected. Class 0 had a precision of 1.00, recall of 0.99 and F1-score is 1.00. For Class 1, Precision 0.99 Recall 1.00 and F1-Score. created a classification report and the result is displayed as output. Macro and weighted

averages for precision, recall, F1-score everything had flawless performance 1.00 across all the metrics.

Confusion Matrix: The model, classified 139 samples from the true Class0 and predicted value of DataSet in which 140 samples. The model was able to predict all 160 samples of Class1 without any mistake being made.

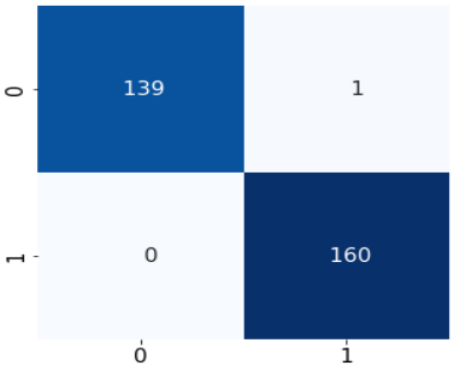

Figure8: Confusion matrix for CNN

6.3 Front-End Interface Testing

The Front-End Interface Testing in Biometric-based Fingerprint Verification System is used to test its usability, functionality & security of the user interface. Such testing ensures that the interface is capable of allowing data owners and administrators to perform essential tasks (ex: secure login, file management) efficient & effectively as well in a highly secured manner. This system has been tested by setting multiple test cases to evaluate the performance and security of a new file storage, including testing how this system performs login process for registered user, also observed testing whether it allows unauthorized accesses i.e. only registered users can access its functionalities either not so another one will try to use these capabilities or ability without having any permission too, the encryption & decryption functionality during uploading and downloading function.

Here are the test cases for those evaluations

- Test Case 1: LogIn process using the Registered user fingerprint.
- Test Case 2: Hacker trying to login with a different finger
- Test Case 3: File Upload with RSAencyption.
- Test Case 4: File Download Using RSA (Decryption)

6.5 Test Case 1: Registered User Fingerprint during Login Process

Table 1: Test Case 1: Registered User Fingerprint during Login Process

Objective	To verify that the system correctly authenticates a registered user using their fingerprint
Preconditions	The user must have already registered their fingerprint with the system. The fingerprint data is secure.
Expected Result	System should correctly match the captured fingerprint with the registered fingerprint. The user will be authenticated and can access system.
Actual Result	The system correctly matched the captured fingerprint with the registered fingerprint. The user was successfully authenticated and granted access to the system.
Status	PASS

6.6 Test Case 2: Hacker Attempting to Login with Different Fingerprint

Table 2: Test Case 2: Hacker Attempting to Login with Different Fingerprint

Objective	For a positive outcome of the test, this is to prove that system can't access when an unknown fingerprint used.
Preconditions	This is because the registered user to which this fingerprint belongs has already set it up with the system. In addition to this, there is the fact that external attacks left no registered fingerprint on the system.
Expected Result	Representative approval is granted only if the system does not identify a match. The system should reject to login and display the alert message related to wrong authentication.
Actual Result	When fingerprints are not matched it is being rejected by the system and displays an error message.
Status	FAIL

6.7 Test Case 3: File Upload with RSA Encryption

Table 3: Test Case 3: File Upload with RSA Encryption

Objective	When fingerprints are not matched it is being rejected by the system and displays an error message.
Preconditions	The user needs to be authenticated and signed in.
Expected Result	The file should be encrypted through the RSA algorithm before uploading and an upload process is successful. Cloud where to keep the encrypted file
Actual Result	The file is encrypted on the end device using RSA before being uploaded and stored securely in-the-cloud.
Status	PASS

6.8 Test Case 4: File Download with RSA Decryption

Table 4: Test Case 4: File Download with RSA Decryption

Objective	To be sure that all downloaded cloud-side files are properly decrypted with RSA algorithm.
Preconditions	The user has to be signed in as well.
Expected Result	This is enough to download the file, and successfully decrypt it using an RSA algorithm. After this process, the user should get an unencrypted file.
Actual Result	URL becomes to decrypt file when user calls that URL: File gets downloaded successfully and decrypted with RSA then User will able to get back its decrypted handled files.
Status	PASS

6.9 Discussion

This research shows that the Siamese Neural Networks approach for a Biometric-Based Fingerprint Verification System in secure cloud storage improves data security and user authentication system. One of the key contributions, particularly from this SNN-based system, is its extensibility to new classes as you can continue learning on top without retraining entire model The dynamic property is especially useful for a real-time system since it can very easily adapt to any new user without degrading the performance or efficiency.

The SNN integration does great both in terms of the security and user experience: it is easy-to-use, has a good looking front-end that stores the unique info to cloud as well. It also uses RSA encryption to help ensure that data in the cloud remains private and unmodified.

The presented system tackles a number of critical issues in the current access control methods, where it can face low accuracy, security holes and bad user experience. Using deep learning methods, such as CNNs and SNNs to realize better accuracy in accurate detection of the fingerprints. This provides

an easy to use package and makes the authentication process much secure; which enhances user experience alongside enhancing cloud storage security. And its use of RSA encryption for files transferred to the cloud adds an extra level of security ensuring data is not only kept private. Such multi-layered security method makes the solution quite invincible against all kinds of cyber-threats and unauthorized access to it.

But their study has some weaknesses. The dataset that the SNN was trained on a perfect fit might not be a good representation of all users. In the future, research should leverage a wider and more comprehensive selection of datasets to ensure that the model is generalizable on other distributions. Moreover, the scalability of such a system to deal with billions records and millions of users needs further study. Advanced Layer Pervasive Biometric Based Fingerprint Verification System using SNN for secure cloud storage.

7 Conclusion and Future Work

Biometric Based Fingerprint Verification System is implementation of a secure cloud storage facility, and indeed; the Siamese Neural Networks (SNN) implementation has indeed provided a robust, very efficient solution to data security and user authentication. After integrating and conducting research into the application, it has been shown that the SNN model is indeed highly accurate and reliable in differentiation between the authorized and unauthorized users. This is evidenced by the impressive overall accuracy of 99.67%, out of 140 test fingerprint image it classified 139 images correctly in the report, with also perfect specificity, sensitivity, and F1-score measures of 100%. Cloud users can subscribe and have RSA encryption to protect data on the cloud. Clearly, the Siamese Neural Networks is a reliable solution.

Future work is to increase scalability need to handle large amounts of fingerprint data and the subsequent uptake of users. Develop interoperability standards to smooth the process of merging with existing cloud storage platforms; Then address legal and regulatory challenges associated with storing real fingerprint data on the human body and integrating these with the user interface. Optimize the SNN Model's performance through parallel processing, GPU acceleration, and transfer learning. Study an overarching security problem to pinpoint potential vulnerabilities and devise countermeasures. Add an access control system, complemented by firewalls and network-level security elements, to improve data security and user authentication.

Reference

Abied, O., Ibrahim, O. and Kamal, S.N.I.M., 2022. Adoption of Cloud Computing in EGovernment: A Systematic Literature Review. Pertanika Journal of Science & Technology, 30(1).

Ackerson, J.M., Dave, R. and Seliya, N., 2021. Applications of recurrent neural network for biometric authentication & anomaly detection. Information, 12(7), p.272.

Ahamad, D., Hameed, S.A. and Akhtar, M., 2022. A multiobjective privacy preservation model for cloud security using hybrid Jayabased shark smell optimization. Journal of King Saud UniversityComputer and Information Sciences, 34(6), pp.23432358.

Ahsan, M., Based, M.A., Haider, J. and Kowalski, M., 2021. An intelligent system for automatic fingerprint identification using feature fusion by Gabor filter and deep learning. Computers and Electrical Engineering, 95, p.107387.

Alam, T., 2020. Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), pp.108115.

An S, Leung A, Hong JB, Eom T, Park JS. Toward automated security analysis and enforcement for cloud computing using graphical models for security. IEEE Access. 2022 Jul 13;10:7511734.

Barra, Silvio, et al. "Biometric data on the edge for secure, smart and user tailored access to cloud services." Future Generation Computer Systems 101 (2019): 534541.

Bello, S.A., Oyedele, L.O., Akinade, O.O., Bilal, M., Delgado, J.M.D., Akanbi, L.A., Ajayi, A.O. and Owolabi, H.A., 2021. Cloud computing in construction industry: Use cases, benefits and challenges. Automation in Construction, 122, p.103441.

Edrah, A. and Ouda, A., 2024. Enhanced Security Access Control Using StatisticalBased Legitimate or Counterfeit Identification System. Computers, 13(7), p.159.

G. Panchal, D. Samanta, A. K. Das, N. Kumar and K. K. R. Choo, "Designing Secure and Efficient BiometricBased Access Mechanism for Cloud Services," in IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 749761, 1 AprilJune 2022, doi: 10.1109/TCC.2020.2987564.
Gumaei, Abdu, et al. "Antispoofing cloudbased multispectral biometric identification system for enterprise security and privacypreservation." Journal of Parallel and Distributed Computing 124 (2019): 2740.
Hindi, A., Dwairi, M.O. and Alqadi, Z., 2020. Analysis of procedures used to build an optimal fingerprint recognition system. International Journal of Computer Science and Mobile Computing, 9(2), pp.2137.
Islam, R., Patamsetti, V., Gadhi, A., Gondu, R.M., Bandaru, C.M., Kesani, S.C. and Abiona, O., 2023. The future of cloud computing: benefits and challenges. International Journal of Communications, Network and System Sciences, 16(4), pp.5365.
J. Ezeobiejesi and B. Bhanu, "Patch Based Latent Fingerprint Matching Using Deep Learning," 2018 25th IEEE International Conference on Image Processing (ICIP), Athens, Greece, 2018, pp. 20172021, doi: 10.1109/ICIP.2018.8451567.
Kousalya, A. and Baik, N.K., 2023. Enhance cloud security and effectiveness using improved RSAbased RBAC with XACML technique. International Journal of Intelligent Networks, 4, pp.6267.
Liu, Chun, et al. "An efficient biometric identification in cloud computing with enhanced privacy security." IEEE Access 7 (2019): 105363105375.
Militello, C., Rundo, L., Vitabile, S. and Conti, V., 2021. Fingerprint classification based on deep learning approaches: experimental findings and comparisons. Symmetry, 13(5), p.750.
Mostafa, A.M., Ezz, M., Elbashir, M.K., Alruily, M., Hamouda, E., Alsarhani, M. and Said, W., 2023. Strengthening cloud security: an innovative multifactor multilayer authentication framework for cloud user authentication. Applied Sciences, 13(19), p.10871.
Prabhu, D., S. Vijay Bhanu, and S. Suthir. "Privacy preserving steganography based biometric authentication system for cloud computing environment." Measurement: Sensors 24 (2022): 100511.
Sandhu, A.K., 2021. Big data with cloud computing: Discussions and challenges. Big Data Mining and Analytics, 5(1), pp.3240.
Seth, B., Dalal, S., Le, D.N., Jaglan, V., Dahiya, N., Agrawal, A., Sharma, M.M., Prakash, D. and Verma, K.D., 2021. Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm. Computers, Materials & Continua, 67(1).
Shen, W., Su, Y. and Hao, R., 2020. Lightweight cloud storage auditing with deduplication supporting strong privacy protection. IEEE Access, 8, pp.4435944372.
Sudhakar, Tanuja, and Marina Gavrilova. "Cancelable biometrics using deep learning as a cloud service." IEEE Access 8 (2020): 112932112943.
Sureshkumar, V. and Baranidharan, B., 2021, July. A study of the cloud security attacks and threats. In Journal of Physics: Conference Series (Vol. 1964, No. 4, p. 042061). IOP Publishing.
Tarawneh, A.S., Hassanat, A.B., Alkafaween, E.A., Sarayrah, B., Mnasri, S., Altarawneh, G.A., Alrashidi, M., Alghamdi, M. and Almuhaimeed, A., 2022. Deepknuckle: Deep learning for finger knuckle print recognition. Electronics, 11(4), p.513.
Uliyan, D.M., Sadeghi, S. and Jalab, H.A., 2020. Antispoofing method for fingerprint recognition using patch based deep learning machine. Engineering Science and Technology, an International Journal, 23(2), pp.264273.
Uslu, Utku, Özlem Durmaz İncel, and Gülfem Işıklar Alptekin. "Evaluation of Deep Learning Models for Continuous Authentication Using Behavioral Biometrics." Procedia Computer Science 225 (2023): 12721281.
Yan, H. and Gui, W., 2021. Efficient identitybased public integrity auditing of shared data in cloud storage with user privacy preserving. IEEE Access, 9, pp.4582245831.
Yang, Linlin, et al. "Efficient Biometric Identification on the Cloud With Privacy Preservation Guarantee." IEEE Access 10 (2022): 115520115531.
Zhu, Jinting, Julian JangJaccard, and Paul A. Watters. "Multiloss siamese neural network with batch normalization layer for malware detection." IEEE access 8 (2020): 171542171550.