LIGHTWEIGHT IOT SECURITY WITH DEEP LEARNING-DRIVEN BIOMETRIC FOR HUMAN AUTHENTICATION

BY

GIRMA ALEMU BIRBIRSA

ADVISOR: HENOCK MULUGETA (PhD)

MASTER OF SCIENCE IN CYBERSECURITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY - AAiT

SCHOOL OF INFORMATION TECHNOLOGY AND ENGINEERING –SiTE

ADDIS ABABA UNIVERSITY

Feb, 2025

LIGHTWEIGHT IOT SECURITY WITH DEEP LEARNING-DRIVEN BIOMETRIC FOR HUMAN AUTHENTICATION

BY

GIRMA ALEMU

EXAMINERS' COMMITTEE

Dr. Henock Mulugeta	_____	_____
[Thesis Advisor]	(signature)	(date)
Dr. Elefelious Getachew	_____	_____
[Dean of the School]	(signature)	(date)
Dr. Seleshi Demise	_____	_____
[Internal Examiner]	(signature)	(date)
Dr. Fitsum Assamnew	_____	_____
[External Examiner]	(signature)	(date)

A Thesis Submitted in Partial Fulfillment of the requirements for Master of Science in Cyber Security

Addis Ababa Institute of Technology

School of Information Technology and Engineering

Feb, 2025

ABSTRACT

Now today the number of Internet of Things (IoT) devices increases in number, as the number of IoT device increase there is also a rise in risk with these IoT devices. IoT devices have a great impact on daily lives of human being. Huge number of data can be stored, transmitted and used through IoT devices. Some of the data are very sensitive which are vulnerable to different attacks. To protect IoT devices from these attacks, different counter measures are conduct through previous researches. Conventional biometric authentication methods like possession-based (tokens) and knowledge-based (passwords/PINs) are used to tackle the problem of access control which are prone to loss, duplication, guesswork, and forgetfulness. Similarly, single-modality biometric identification—like fingerprint or facial recognition—is insufficient due to its susceptibility to spoofing attacks. When merging and comparing large amounts of biometric data, it is important to consider variations in the quantity and caliber of data sources, even though multi-biometric systems improve security. Our proposed solution to these problems combines a lightweight deep learning algorithm designed for Internet of Things devices with multimodal biometrics that are using fingerprint and face. By conducting an experiment on both training and unseen datasets, the model demonstrated good classification ability with 82.5% validation accuracy and 99.3% training accuracy. The suggested solution addresses the security issues of IoT devices through modeling and experimental validation. Through hands-on testing, we assessed the system's performance, and the outcomes showed a robust IoT security solution. In the end, the combination of deep learning algorithms and dual biometric modalities has greatly improved secure authentication procedures for IoT applications. At the end, secure authentication techniques for IoT applications have advanced significantly with the combination of deep learning algorithms and dual biometric modalities.

Keywords: Biometrics, Deep Learning, IoT, Light weight CNN, MobileNetV2

ACKNOWLEDGMENT

First and foremost, I give my deepest gratitude to God Almighty for His guidance, strength, and countless blessings throughout this journey. His wisdom and grace have been my source of inspiration, and without His divine support, this work would not have been possible. I am immensely grateful to my advisor, Henock Mulugeta (PhD), for his invaluable guidance, encouragement, and patience throughout this research. My heartfelt appreciation goes to my family, whose love, prayers, and sacrifices have been my greatest motivation. Their constant encouragement and belief in me have given me the strength to persevere. To my friends and colleagues, thank you for your support, thoughtful discussions, and encouragement. Your presence has made this journey more meaningful and rewarding. This thesis is a result of the collective efforts of many, and I am deeply grateful to each and every one of you.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AA Authentication Accuracy

AI Artificial Intelligence

CNN Convolutional Neural Network

DL Deep Learning

FAR False Acceptance Rate

FRR False Rejection Rate

IOHT Internet of Healthcare Things

IoT Internet of Things

KNN K-Nearest Neighbor

MFFA Multi-Factor Fingerprint Authentication

MFA Multi Factor Authentication

PIN Personal Identification Number

CHAPTER ONE: INTRODUCTION

1.1. Background

Vehicles, home appliances, and other connected devices with sensors, software, electronics, and other components that enable data collection and sharing are collectively referred to as the "Internet of Things" (IoT). The Internet of Things (IoT) is an emerging field that combines everyday objects with internet connectivity and data analysis capabilities, transforming the way we live and work. It has gained significant attention due to its technical, social, and economic implications[1]. Now todays the number of IoT devices increase fastly and over 75 billion of IoT devices will be in use by 2025[2]. The increasing number of these IoT devices can be led to security concerns of data generated and stored by the IoT devices. The IoT devices collect, store and transmit sensitive data, which is important to overcome some security concerns. Some of them are listed below:

- Unsecured connections: unsecured connection is a big issue when transmitting data between IoT devices, which is vulnerable to attacks.
- Weak authentication: authentication mechanisms like PIN and password are used in IoT device, which are easily compromised.
- Vulnerability to malware: many IoT devices are vulnerable to malware in which the attacker gain access to the data stored by IoT devices.
- Data privacy: these IoT devices contain huge personal and sensitive data, which is a big concern about the personal privacy.
- Interoperability: different manufactures produce different IoT devices which is not compatible and this leading to security gaps.
- Insider threats: some employees intentionally or unintentionally compromising the security of IoT devices. So, it needs strong authentication mechanism to ensure the protection of data stored and transmitted by these devices.

Some traditional authentication mechanisms have their own limitations when used for IoT devices. Some them are:

- Passwords: it is easily compromised by hackers or social engineering techniques, which is not reliable for IoT devices.

- PIN codes: it is similar to password which is easily compromised and it is not preferable for use with large number of IoT devices.
- Biometric authentication methods: biometric authentication method is good compared to password and PIN, but still there is a limitation with this mechanism, because of quality image captured and can also be easily spoofed.

One technique for confirming or identifying users based on their physical or behavioral traits, such as their voice, face, iris, or fingerprint, is biometric authentication[3]. Biometric authentication is preferable when compared to traditional authentication methods such as password and PIN for IoT devices from the perspectives of security. The process of biometric authentication is collecting biometric data using sensors and camera, biometric data preprocessing to remove noisy from the data, feature extraction, template storage to verify the identity of the users. If collected biometric data is matched with the stored template, the user gain to access to the IoT devices. There are several biometric modalities used for authentication such as fingerprint, face recognition, iris, palm print, voice and gesture. These biometric modalities have their own strengths and weaknesses and the choice of modalities will rely on user needs as well as inherent device limitations. Even though, biometric authentication is more secure compared to traditional methods, it has some challenges like false positive and false negative matches. Even if with these challenges, biometric authentication method is familiar method for authentication in IoT devices, but still needs further research to improve the reliability and security of biometric authentication method.

When it comes to controlling access to both digital and physical resources, such as doors, ATMs, and various embedded devices, biometric authentication systems are crucial[4]. Biometric working principle is typically divided into different stages; biometric data collection, preprocessing, feature extraction, template generation, template storage and matching[5]. Biometric authentication depends on different biometric characteristics like fingerprint, hand geometry, retina scans, and face recognition to verify an individual's identity[6]. It is a process of identifying a person's identity based on their physiological and behavioral features[7].

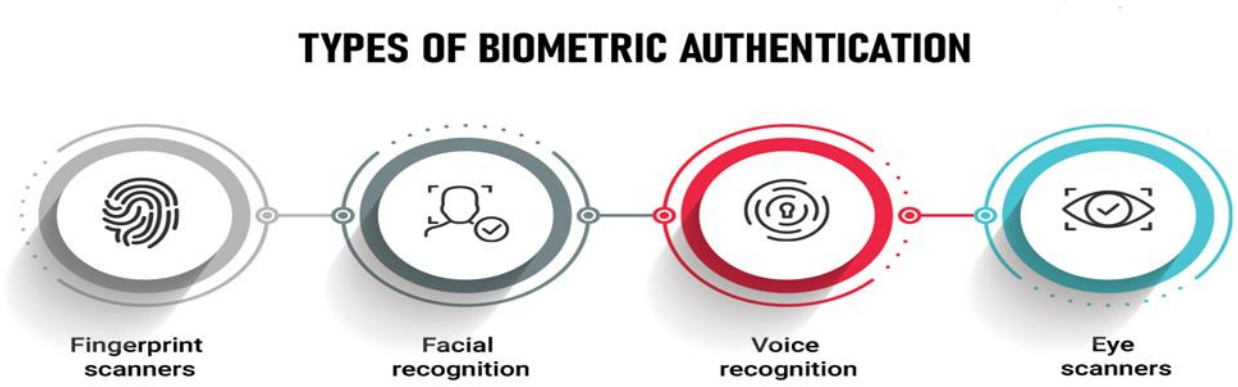


Figure 1: Types of Biometric Authentication[8]

A type of machine learning known as deep learning (DL) that uses many layers of algorithms to process input data and produce output that imitate human thinking process[9]. Deep learning nowadays become an important tool for different domain areas like computer vision, natural language processing (NLP) and many. Deep learning's ability to understand intricate relationships between input and output data is one of its main advantages. Deep learning also has the benefit of automatically identifying intricate patterns in data after being trained on big datasets. When it used with biometrics authentication, it has an advantage for extracting features from input data and do classification task to improve the performance of authentication process. When compared to more conventional authentication methods, biometric authentication performs better with deep learning. Even though, deep learning has a great role in biometric authentication method, there are challenges like the availability of large amount of trained and diversified data. Regardless these challenges, deep learning is a promising tool for biometric authentication system that can play an important role in the development of secure and reliable authentication methods for IoT devices. A technique used in deep learning is artificial neural networks, with multiple processing layers to gradually extract higher-level features from data[10].

1.2. Motivation of the study

Our everyday lives are nearly entirely dependent on IoT devices; we utilize them to exchange data and store private information. Our sensitive data is exposed to attackers due to inadequate security measures on IoT devices, which directly affects our day-to-day lives. So, it is critical to protect the IoT devices using state-of-the-art solution which is our proposed solution. Our proposed solution

leverages light weight deep learning with multimodal biometric (face and fingerprint) to highly secure these devices. So, security is a big driving force.

1.3. Statement of the problem

The Internet of Things' (IoT) rapid expansion has resulted in a massive increase in the amount of private and sensitive data being exchanged and kept on IoT devices. Consequently, the security of IoT devices has been investigated, and strong authentication protocols need to be put in place to safeguard the data they contain. Conventional authentication methods like passwords and PINs were employed in the early testing, however it has subsequently been shown that these are unreliable and subject to attack. Token-based authentication poses a security risk in the event of card loss or theft, making it an unreliable technique. Because biometric identification is based on your identity, it is the most secure way for Internet of Things devices. Research on single and multi-modal biometric authentication has already been conducted to address the authentication problem with IoT device security. Studies on single-modal biometrics were susceptible to spoof attacks, which resulted in FAR and FRR[11]. A promising approach to IoT device security was also investigated using multi-modal biometric authentication. From their perspective, the multi-modal biometric authentication-based systems that have been presented are not user-acceptable, and part of their performance is affected by external and man-made elements that affect security, performance, and user acceptability[11]. Therefore, multimodal biometric authentication (facial and fingerprint) with deep learning is required for more secure authentication techniques. One potential solution to this problem is to use multi modal biometric authentication, fingerprint recognition and face recognition with light weight deep learning to secure IoT devices. To provide a more secure and convenient authentication process, the system will combine multi-modal biometrics with a lightweight deep learning algorithm. Evaluation of the suggested system will be done in terms of performance, security and compared with state-of-the art authentication methods and other related works.

1.4. Research questions

1. How can accuracy be increased with deep learning and reliability of biometric authentication in IoT devices?
2. How to fuse multiple forms of different biometric technologies, such as fingerprint and face, for IoT device security?

3. How does the proposed deep learning-driven multi-factor biometric authentication system compare with state-of-the-art biometric authentication methods?

1.5. Objective of the study

- General Objective: The main objective of this research work is to enhance the security of IoT devices through the development and implementation of a light weight deep learning-driven multi-factor biometric authentication system.
- Specific Objectives:
  1. To integrate light weight deep learning with multimodal biometric authentication system to improve the accuracy and the performance of the IoT device security.
  2. To fuse multiple forms of biometric modalities, fingerprint and face in order to improve security, accuracy and performance of the IoT device.
  3. To explore architectural design optimizations, such as lightweight network architectures or model parameter sharing, to reduce the computational and storage demands of deep learning models in biometric IoT device security systems.
  4. To compare the proposed solution with state-of-the-art solutions method using different metrices.

1.6. Contribution of the study

- The proposed lightweight deep learning model is designed to consume less memory and reduce execution time, making it ideal for deployment on IoT devices.
- This study explores advancements to improve IoT device security by incorporating lightweight deep learning methods with combined biometric modalities, such as fingerprints and facial recognition.

1.7. Scope/delimitation

This study mainly focused on the integration of lightweight deep learning algorithms and multimodal biometrics to secure IoT device. Specifically, the study integrated fingerprint and face recognition biometrics with a lightweight deep learning system tailored for IoT devices.

Scope:

- Biometric data collection (fingerprint and face images)
- Lightweight deep learning model selection
- Model training and evaluation

- Testing the model on android device (smart phone)

Delimitations:

- Testing on other types of phones (apple phone, Windows phone)
- Testing on different IoT hardware
- Different attack scenarios are out of the work;

1.8. Organization of the document

This section describes about what would the structure of the thesis looks like. Chapter One is Introduction; focuses on the background, motivation, statement of the problem, research questions, research objective, expected contribution of the study and scope/delimitation. Chapter Two is Literature Review and Related Works on IoT security, Biometrics access control and authentication, Deep learning and Related works are presented. Chapter Three is about Methodology includes Research Approach, Data collection Techniques, Sampling Method, Sample Size, Data Analysis method is clearly stated. Chapter Four is about Proposed Solution; Chapter Five is focused Experiments and Analysis; Chapter Six focus on Result and Discussion and Chapter Seven is about Summary and Future Work.

CHAPTER TWO: LITERATURE REVIEW AND RELATED WORKS

2.1. Literature Review

2.1.1. Introduction

In this chapter we present previous research works that were conducted for the last many years in order to secure IoT devices. The reviewed points mainly focus on lightweight IoT security through deep learning and biometrics authentication method. Here are the points that the literature review focus on : An overview of the vulnerabilities and challenges related to IoT security, Unauthorized Access in IoT, Data Breaches in IoT, Biometric Modalities, Biometric Authentication System and Deep learning.

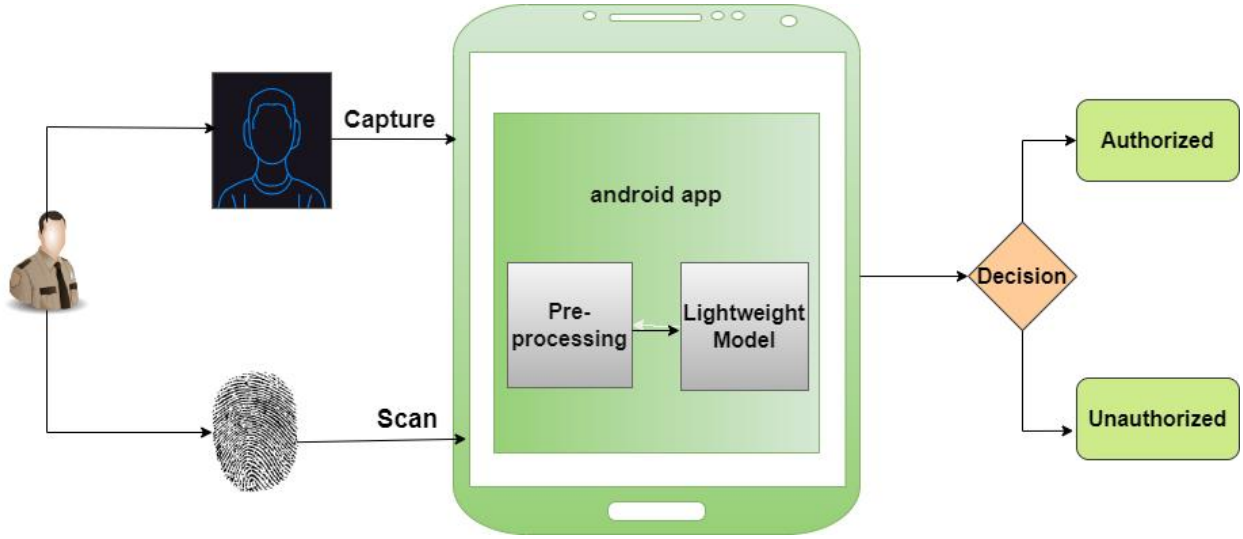


Figure 2: Android Smart Phone Scenario

Figure 2 illustrate that the scenario considered for this study. The diagram illustrate that the lightweight face and fingerprint identification system experimented on android smartphone. The system designed to provide secure authentication using lightweight deep learning and multi-modal biometrics (face and fingerprint) for resource constraint IoT devices.

Components

Data capture: The system captures user face using camera and scan user fingerprint using fingerprint scanner (sensor)**, Preprocessing:** The captured data (face and fingerprint images) undergoes pre-processing techniques to improve the quality of data that is captured. This involves

image resize and normalization tasks, **Lightweight Model:** Using mobilenetV2 we can extract important local features from fingerprint and face images, **Decision:** The model's output is utilized to categorize the user as an Authorized or Unauthorized to access the IoT device. As illustrated in the Figure 2, if the captured data is Authorized data, then the user is granted to access the IoT device. If the captured data is Unauthorized user data, then the user is rejected to access the device.

In this chapter, the overview of lightweight IoT security deep learning-driven biometrics for human authentication is reviewed. The reviewed points are: An overview of the vulnerabilities and challenges related to IoT security, Unauthorized Access in IoT, Data Breaches in IoT, Biometric Modalities, Biometric Authentication System and Deep learning.

2.1.2. An overview of the vulnerabilities and challenges related to IoT security

A s ate-of-the-art review of IoT security and its challenges is provided, which summarizes legal and technical solutions that are beneficial to businesses, organizations, and the government. and offers potential solutions to address the security challenges discussed [12]. [13] This paper will analyze existing literature related to various privacy threats in IoT, privacy issues in different applications of IoT and present summary of the study. A network of linked devices having the ability to share data and communicate with one another is known as the Internet of Things (IoT). Security is essential since these devices are a highly-targeted attack vector due to their vulnerability and spread [14]. The difficulties with IoT security range from preventing malevolent insiders from protecting against attacks by nation-states [14, 15]. Several prevalent difficulties and risks related to IoT security include:

2.1.2.1. **Software and firmware vulnerabilities**: because of the limited processing power and resource constrained, it is hard to apply strong security measures for IoT devices[12].

2.1.2.2. **Lack of standardization**: lack of standardization for IoT devices due to different devices, protocols and platforms, it is a big problem to ensure compatibility and interoperability which lead to vulnerabilities that can be exploited by attackers [13].

2.1.2.3. **Weak password protection**: using default password for IoT devices that can easily guessed, can make the IoT device vulnerable to different attacks[14].

2.1.2.4. **Absence of frequent updates and patches**: if IoT devices cannot receive regular security updates, they are vulnerable to known vulnerabilities [14].

2.1.2.5. **Insecure interfaces**: if the interface of IoT device is not secure, Attackers can readily use them to obtain access to the device[14].

2.1.2.6. **Insufficient data protection**: IoT devices gather and communicate vast amounts of sensitive data, which make them a target for cybercriminals[14].

2.1.2.7. **Inadequate handling of IoT devices**: IoT devices are not managed using tools and process need to manage them and this leading them to vulnerable attacks[14].

2.1.2.8. **Limited physical security**: IoT devices are small in size and easily security breaches are performed on, leading them to physical attacks[13].

Organizations must put strong IoT security mechanisms in place to address these issues, including as patching vulnerabilities, monitoring, updating firmware, access control, threat response, and hardening components [15]. To obtain an in-depth comprehension of cybersecurity concerns pertaining to the Internet of Things and implement a plan to alleviate associated hazards[14].

2.1.3. Unauthorized Access in IoT

Unauthorized access control in IoT is a crucial matter that must be handled to guarantee the security of connected devices and networks. Here are some insights from the search results: IoT devices are susceptible to unauthorized access, with some APIs being unverified, which allows unauthorized users to access cloud resources or control devices, posing a threat to the security of the system[16]. Weak passwords and other security flaws give hackers IoT device access, giving them the ability to take over the device or steal personal data. This can involve utilizing the device to initiate DDoS attacks or gaining access to the camera or microphone[17]. By guarding IoT devices from unwanted access, you can prevent them from leaking private data or acting as a backdoor to other areas of the network. Everything from watches and smart home appliances to cars and smart grids has IoT security flaws[15]. Physical security is essential to avoiding unwanted access to a device, especially since IoT applications are often remote. It is valuable to use encryption and secure data transmissions in order to guarantee that devices and users possess the ability to access network resources without allowing hackers access[18]. IT administrators must only deploy authenticated devices and only allow authorized and authenticated device access.

Without visibility into shadow IoT devices, IT admins can't ensure the hardware and software have basic security functionalities or monitor the devices for malicious traffic[19].

2.1.4. Data Breaches in IoT

Because there are an increasing number of interconnected devices, there is a growing fear about data breaches in the Internet of Things because of these vulnerabilities. Several important discoveries were made based on the search results. 84% of Internet of Things (IoT) devices are susceptible to network attacks, which include phishing, spoofing, incidents of denial of service (DDoS) and theft of data [20],[21]. During 2021's first half, there were 1.5 billion assaults on smart devices by hackers attempting to steal confidential information[22],[23]. Top IoT cyber security risks for 2022 include insufficient password strength, out-of-date software, improper IoT connectivity management, ignorance of IoT security, and more [24]. The Mirai Botnet is one of the most illustrative cyber-attacks demonstrating IoT vulnerabilities[21],[25]. IoT devices can corrupt whole networks and lead to data theft, severe disruptions in operations, or even endanger human lives[24]. Although the advantages and promising future of IoT, there are still certain security flaws and applicable network and device security laws that require attention[21],[22].

2.1.5. Biometric Modalities

Based on the search results, here is a literature review of different biometric modalities used in IoT:

2.1.5.1. **Fingerprint**: The most popular biometric modality for IoT device security is fingerprint recognition. Fingerprint recognition is used for access control, authentication and identification of users. Fingerprint recognition system is perfect to implement it on small devices like IoT devices [26]

2.1.5.2. **Face**: Face recognition is another biometric modality used in IoT environment. Like for surveillance and access control face recognition is preferable. But this biometric modality performance is affected by different factors like lighting condition and pose. Nowadays, deep learning can improve the accuracy of face recognition by tackling the above challenges [26]

2.1.5.3. **Electrocardiogram (ECG)**: another biometric modality is ECG, which identifying users based on the heart electrical activity[26].

2.1.5.4. **Voice**: voice recognition is one type of behavioral biometrics that identify users based on user's voice. This biometric modality is affected by some noises and speech patterns decrease the precision of recognition[26]

2.1.5.5. **Behavioral biometrics**: there are mainly two category of biometrics, physical biometric and behavioral biometric. Behavioral biometrics is used to identify users based on persons' behavioral patterns[26].

2.1.6. Biometric Authentication System

A biometric identity verification system is an authentication method that is used to verify or identify users based on persons' behavioral and physiological traits. Different biometric modalities are used such as fingerprint, face, voice, gestures, palm print and iris. Since they are convenient and secure, they are preferable than traditional authentication method[27]

2.1.7. Deep Learning (DL)

IoT device security is enhanced by biometric authentication system that incorporates different biometric modalities[26][28]. When deep learning models are highly applied on face recognition, state-of-the-art performance is achieved, which is well suited for the deployment on embedded devices[29]. Biometrics authentication system utilizes different biometric modalities like the iris, fingerprint, and face to verify their identity[26][30].

There is a limitation with traditional biometric authentication like poor accuracy, FRR, FAR and vulnerable to spoofing attacks[31][32]. To overcome these limitation deep learning models come in to place by deeply training biometric data and extract complex pattern features from biometric data to increase the precision and performance of the authentication system [33][32].

Recently deep learning models or algorithms are applied on different domain area like computer vision, speech recognition and natural language processing (NLP)[34][35]. It can also use in biometric areas for fingerprint verification, face recognition and iris recognition [34][36][37].

[38] is suggested biometric authentication for private and secure communication between Industry 4.0 and Internet of Things edge devices. This paper proposes a BioSec architecture for biometric authentication to enable private and secure communication between edge devices in Industry 4.0 and the Internet of Things. The introduction of encryption techniques to safeguard biometric data has further raised the IoT's security level. This research work needs improvement on performance

metrics by using other biometric modalities like Iris with fingerprint. Another thing is that it needs other solutions for solving the key distribution problem. The paper focus on a single biometric modality which is susceptible to spoofing attacks.

[39] created deep learning of electrocardiography dynamics for biometric person identification in the Internet of Things era, With a 99.0% detection rate on the MIT-BIH Normal Sinus Rhythm Database. The proposed research is focus on the data sets that were used by the previous works and could not include new data sets. Additionally, the paper could not mention the way how to handle the computational complexity and storage issues. From the perspectives of user acceptability this research work is not feasible. This research did not fully address how the ECG-based deep learning model can be optimized to run efficiently on resource constrained IoT devices.

In [40], In the medical setting, where healthcare facilities became the primary target of cybercriminals during the COVID-19 outbreak, they assess the existing MFA practices. Cyberattacks against MFA in medical settings are examined. By raising knowledge of the elements and tenets of MFA, the paper highlights and elaborates on the difficulties in IoHT. They also go over the difficulties and restrictions associated with authentication security. FIDO2 and WebAuthn technologies, as well as physical key devices and biometrics, have been demonstrated to be superior alternative MFA solutions to static password usage when healthcare shifts to online or telehealth services. The report identifies a number of future projects, including the necessity for strong and portable authentication security mechanisms in IoHT and the importance of a password-free authentication regime. The research work's shortcoming is that deep learning, which is currently the most crucial technique for spoof detection, is not included.

In research [41] a survey on Deep learning-based security behavior analysis in IoT environments, which seeks to offer a comprehensive analysis of deep learning applications in the Internet of Things for security and privacy issues and the primary focus is on deep learning enhanced IoT security is done. The primary focus of this survey is the application of deep learning technology to examine device security aspects within the context of the Internet of Things. Specifically, deep learning-based device profiling and fingerprinting were comprehensively discussed. There is an issue concerning efficient resource for deep learning. Additionally, adaptive and heterogeneous data is identified as a challenge for this paper.

[42]suggested Biometrics for Internet-of-things Security, which suggests providing a comprehensive review of the current status of biometrics research in IoT security, focusing on two important areas: authentication and encryption. This review study looks at a range of biometric systems or techniques for fixing vulnerabilities in different IoT architectural levels. The authentication and encryption capabilities of biometric-based systems are taken into account for the purpose of IoT security. To further the study of IoT, a number of research challenges need to be addressed, such as device power consumption, battery constraints, memory storage capacity, performance costs, security, and convenience. This paper review highlights the need for additional study on storage and computational complexity.

Deep learning-driven biometric authentication may offer a more dependable and secure method of safeguarding IoT devices in the realm of IoT security. Multi-factor authentication systems can offer an extra degree of protection by combining several types of biometric information, like fingerprints and facial recognition. However, there is limited research on the integration of deep learning and multi-factor biometric authentication for IoT security.

This research summary highlights the potential of deep learning to enhance IoT device security using biometric authentication. It also highlights the need for additional research on the subject of this proposed study, which is the combination of deep learning and multi-factor biometric authentication for IoT security.

2.2. Related works

[43] focuses on machine learning-based techniques and provides a taxonomy of IoT authentication and authorization systems. The present problems and reasons for IoT authentication and authorization are covered in the paper, along with the reviews that have already been done. Along with a taxonomy of various IoT authentication and authorization methods, the authors provide an overview of security and privacy issues. The difficulties and potential research areas for machine learning-based IoT authentication and authorization systems are also discussed in the article. Articles and papers that address machine learning-based authentication and authorization schemes in the Internet of Things, such as a lightweight, machine learning-based authentication framework for smart IoT devices, recent IoT security research, and machine learning-based IoT security techniques, are among the related works cited in the paper. The paper provides useful details regarding the current state of machine learning-based authorization and authentication systems in

the Internet of Things, along with the difficulties and potential avenues for further study in this field.

The paper [44] provides an overview of the current state of machine and deep learning-based security and privacy solutions for IoT devices. The use of deep learning and machine learning in IoT security and privacy, the difficulties in implementing these solutions, and potential avenues for further research are all covered in this paper.

[32] suggests a system that makes use of deep learning-based continuous authentication for an IoT-enabled healthcare service. The paper highlights the importance of continuous authentication in IoT-enabled healthcare services and displays the findings of tests carried out to assess the suggested system's performance.

[33] presents a thorough analysis of the use of machine learning and deep learning in biometric smartphone authentication. It highlights the potential of these methods to improve the efficacy and security of mobile authentication systems and talks about their benefits, drawbacks, and future possibilities.

[45] offers a thorough analysis of deep learning-based biometric recognition, covering various modalities, techniques, and challenges. It is a priceless resource for academics and professionals involved in biometrics and deep learning.

The integration of deep learning and authentication via biometrics has been widely researched in recent years, but there is limited research on the application of deep learning-driven multi-factor biometric authentication in the field of IoT security. In this section, I will review some of the related works in the field of deep learning and biometric authentication, as well as in the area of IoT security.

In the domain of deep learning and biometric authentication, there have been several studies that have applied deep learning algorithms in order to increase the precision and reliability of biometric authentication systems.

In [46], the authors suggested a lightweight, cloud-based method for cancelable biometric authentication in Internet of Things applications. Cancellable biometric templates solve the privacy concerns that underlie the use of biometrics for authentication. They attempted to illustrate

the accuracy, security, and lightweight nature of their suggested solution. Future research will entail implementing a prototype of the recommended approach in order to scale up their system. The problem with this research work is that they use single modal biometrics that is only fingerprint that raise performance and security problem.

Other authors [11] proposed Multimodal biometrics for improved IoT security, which suggest a multimodal biometric approach for the Internet of Things based on voice and face modalities that is intended to scale to the constrained resources of an IoT device. The method was examined using a dataset of voice files and face images taken with a Samsung Galaxy S5 cellphone in practical situations, including noisy environments and dark rooms. According to the findings, fusion improved recognition accuracy by 81.62% when compared to voice alone and 52.45% when compared to face alone. The gap of this research is they use KNN which used for simple classifier. So, it needs deep learning approach to handle large amount and complex data to improve the safety of IoT device. For two reasons KNN is not considered as lightweight. The first one is high memory usage, it means that it stores the entire training dataset[47]. The second one is, it is computationally expensive during prediction KNN calculates the distance between the new data point and every point in the training set[48].

[49] suggested Moving toward a multimodal biometric-based secure signature system: implementation for the Internet of Things Blockchain network, Through the extraction of a high-entropy private key, the approach proposed in this study applies multimodal biometrics to improve network security. Creating a safe, effective, and scalable signature system that combines many biometric modalities to offer strong security for blockchain networks and Internet of Things devices is the research gap.

Another authors, [50] proposed Strong multimodal biometric authentication using arm gestures and ear shapes on IoT devices, this study presents a robust and impenetrable multimodal authentication system that automatically verifies a user's identity based on their phone response, after extracting biometric modalities from arm and ear gestures. This study identified a gap by analyzing the proposed method's potential compatibility and interoperability with existing biometric modalities and authentication systems.

Table 1:Summary of Related Works

No	Research Title	Authors	Limitation
1	"Multimodal biometrics for enhanced IoT security"	O. Olazabal *et al*	The gap of this research is they use KNN which used for simple classifier. So, it needs deep learning approach to handle large amount and complex data to improve the protection of IoT device, not light weight
2	"BioSec: A Biometric Authentication Framework for Secure and Private Communication among Edge Devices in IoT and Industry 4.0"	M. Golec, S. S. Gill, R. Bahsoon, and O. Rana	The development of a lightweight and robust biometric authentication framework that can efficiently protect communication among edge devices in IoT and Industry 4.0, but the unimodal is used (fingerprint) which vulnerable to spoof attack
3	"Deep Learning of Electrocardiography Dynamics for Biometric Human Identification in era of IoT"	Q. Zhang	The development of a deep learning model that effectively extracts features from ECG data to accurately identify individuals in the field of IoT (CNN) is used which is not light weight, and single modal biometrics

4	"A review of multi-factor authentication in the Internet of Healthcare Things"	T. Suleski, M. Ahmed, W. Yang, and E. Wang	The development of more effective and reliable MFA techniques that meet the specific requirements of the IoHT and can provide robust security against various threats and attacks, deep learning is not used.
5	"Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey"	Y. Yue, S. Li, P. Legg, and F. Li	Developing a deep learning-based security behavior analysis in IoT environments that effectively identifies and addresses security vulnerabilities and threats while maintaining the performance efficiency of IoT systems
6	"Biometrics for Internet-of-Things Security: A Review"	W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli	Developing a more comprehensive and effective biometric authentication mechanism tailored to the specific requirements of IoT devices that can provide robust security and privacy protection against various threats and attacks.
7	"A lightweight machine learning-based authentication framework for smart IoT devices"	P. Punithavathi, S. Geetha, M. Karuppiah, S. H.	The evaluation of the proposed framework under real-world conditions and

		Islam, M. M. Hassan, and K. K. R. Choo	the ability to detect and resist different types of attacks targeted at IoT devices.
8	"Towards a Secure Signature Scheme Based on Multimodal Biometric Technology: Application for IOT Blockchain Network"	O. A. Hassen, A. A. Abdulhussein, S. M. Darwish, Z. A. Othman, S. Tiun, and Y. A. Lotfy	Developing a secure, optimal, and scalable signature scheme that integrates various biometric modalities that can provide robust security for IoT devices and blockchain networks
9	"Robust multimodal biometric authentication on IoT device through ear shape and arm gesture"	F. Cherifi, K. Amroun, and M. Omar	Exploring the potential interoperability and compatibility of the proposed approach with other biometric modalities and authentication mechanisms

Summary

Several research have used biometric authentication in the field of IoT security to improve the security of IoT devices. However, these studies have mainly focused on some biometrics technologies, in which some of them lack the basic characteristics of biometrics (Collectable, Universal, Unique, Permanent and Acceptable) and have not yet explored the potential of deep learning-driven multi-factor biometric authentication for IoT security. This proposed research is related to the works summarized in Table 1, as it aims to improve IoT device security through the integration of deep learning and multi-factor biometric authentication. This research is unique in that it focuses on the integration of deep learning and multi-factor biometric authentication for IoT security, which has not been explored in previous studies. As summarized in Table1, there are

many researches that are conducted on IoT device security. There are identified limitations for each reviewed papers which a base for my research problem. The identified gaps are as follows;

- Computational power and storage issues (light weight issue)
- Lack of using multimodal biometrics;
- Lack of using efficient deep learning for IoT environment;
- Lack of testing security measure on IoT device in the real world
- Problem of underfitting and overfitting
- Using heavy machine learning like KNN (for simple classification)

CHAPTER THREE: METHODOLOGY

3.1.Study Design

The quantitative approach will be used for developing a lightweight deep learning model for biometric authentication on resource-constrained IoT devices. We will measure the model's accuracy in user identification and assess its efficiency in terms of processing time and memory footprint on the target device.

In this paper quantitative approach is used, because the paper is mainly focus on experimental research. In this study light weight deep learning (MobileNetV2) leverages the feature extraction of both fingerprint and face images and fusion of both modalities for biometric authentication.

This study uses publicly available biometric datasets which is trained on light weight model that classify data to identify between authorized and unauthorized users. Multimodal biometrics is used in this approach that fuse fingerprint and face images. Different standard metrics are utilized to assess the model's effectiveness, and the result will compare with the state-of-the-art solutions.

3.2.Sample

In this study, fingerprint and face images are from public dataset. Fingerprint images are obtained from “kaggle”, which is publicly available dataset. Face images are obtained from Labelled Face Wild (LFW), which is also publicly available dataset. The fingerprint dataset contains 7,308 images. Image resolution is 96x103 pixels. The face image dataset contains 7,308 images. The image resolution is 250x250 pixels.

Table 2: Dataset Split

Dataset	Total
Train	13616
Test	1692
Validation	1692

The description of the split of the dataset is as follows;

Training data: The largest portion (70%) is dedicated to training the model. This is crucial for the model to learn the underlying patterns in the data.

Validation data: The 15% validation set is used to fine-tune the model's hyperparameters. This helps prevent overfitting to the training data and improves generalization to unseen data.

Test data: The final 15% test set provides an unbiased evaluation of the model's performance on completely new data. This mimics how the model will perform in real-world scenarios.

The reason of this ratio is to balance training and evaluation needs as well as to avoid overfitting and underfitting.

3.2.1. Inclusion Criteria:

- **Image Quality**: quality fingerprint and face images be included in the dataset in order for the model to extract features and identify the user correctly.
- **Diverse Representations**: for the strength of the model fingerprint and face images sample represent variety of lighting conditions, facial poses and different fingerprint impressions were included.
- **Complete Data**: fingerprint and face images for each category (authorized and unauthorized) were included to ensure the multimodal system could be effectively trained.

3.2.2. Exclusion Criteria**:**

- **Poor Quality Images**: images that affect the model's performance due to poor quality is excluded.
- **Incomplete Data**: for all the three datasets namely training dataset, testing dataset and validation dataset, categories with **missing** fingerprint or face images were excluded to maintain consistency.
- **Duplicates**: to avoid bias in model training process the redundant data were excluded.

3.2.3. Sampling Method

For this study, the stratified random sample approach is employed, and the data is split into two groups: authorized and unauthorized. Additionally, the two classes have train dataset, validation dataset and test datasets. The method ensures that, samples from both classes are well-represented.

3.2.4. Sampling Size

Kaggle dataset is used in which fingerprint images and face images are downloaded for deep learning model training.

- Classes: Authorized and Unauthorized. In each class there is 6 fingerprint images and 6 face images per person, which has 13616 images in total.
- Dataset split will be as follow;
    - 70% for training dataset
    - 15% for testing dataset
    - 15% for validation dataset

In this work, the population consists of **biometric data samples**—specifically **fingerprint and face images**—extracted from publicly available datasets on Kaggle. These images represent a diverse population in terms of biometric features, reflecting different age groups, ethnicities, genders, and environmental conditions. The chosen population simulates the types of users expected to interact with IoT security systems that rely on biometric authentication.

Recruitment of Participants (Data Selection)

Since this study utilizes publicly available datasets, no active recruitment of participants was required. Instead, the data was sourced from Kaggle's biometric datasets, which are extensively utilized in academic and industry research. The datasets were chosen on the basis of their quality, accessibility, and applicability to the multimodal biometric authentication challenge.

3.3.Instruments

Two biometric datasets from Kaggle that combine facial image and fingerprint datasets are used in this investigation. These publicly accessible datasets are frequently utilized for biometric analysis in the scientific community, guaranteeing that the information is trustworthy and pertinent to the goals of this investigation.

3.3.1. **Validity**

Since Kaggle datasets provide a thorough depiction of biometric data utilized in the real world, we chose it for this study. Both fingerprint and face images of this datasets include variations, lighting conditions and angles. Because of this reason these datasets are valid for training a robust authentication model that are able to handle the variability in biometric data collection. Additionally, these datasets provided sufficient diversity, which is essential for ensuring that the model generalizes well to unseen data in real world scenarios.

3.3.2. **Reliability**

The Kaggle datasets are known in consistency for both fingerprint and face image qualities and formats, which guarantee that the input data is reliable. These datasets were used before in many biometrics researches, implies their ability to produce consistent and reproducible results. In this research work, the reliability of the datasets was ensured through pre-processing and cross-validation techniques, further confirming the model's performance and the dataset's suitability for biometric authentication.

3.4.Variables

For this research different variables are identified. These variables are independent variables, dependent variables, intervening variables and Extraneous variables.

- Independent variable: input biometric data (face and fingerprint images)
- Dependent variable: the result of authentication (authorized or unauthorized)
- Intervening variable: preprocessing techniques like image normalization and augmentation
- Extraneous variable: face and fingerprint images quality and environmental factors are identified as extraneous variable.

3.5.Evaluation Mechanisms

In this study evaluation mechanisms are important to assess the effectiveness and performance of the developed authentication system. There are different metrics to assess the proposed solution. These metrics are accuracy, loss, precision, F1-score, validation accuracy and validation loss.

- Accuracy: measures how the input data correctly classified (authorized or unauthorized). Mathematically described as follows in Equation (1).

$$Acc = \frac{true\ positives\ (tp)\ +\ true\ negatives\ (tn)}{total\ inputs}$$

- Loss: measure the difference between actual target values and predicted values
- Precision: it is a metrics in which correctly classified authorized users are measured against all positive predictions presented in Equation (2).

$$Precision = \frac{true\ positives\ (tp)}{true\ positives\ (tp) +\ false\ positives\ (fp)}$$

- Recall: it is another metrics in which actual positives (authorized users) measured that is correctly classified by the model shown in Equation (3).

$$recall = \frac{true\ positives\ (tp)}{true\ positives\ (tp)\ +\ false\ negatives\ (fn)}$$

- F1-score: it is a mean of precision and recall (balanced measures when there is unbalanced class distribution) presented in Equation (4).

$$F1 - score = \frac{2\ *\ precision\ *\ recall}{precision\ +\ recall}$$

- Validation Accuracy and Validation Loss: for monitoring model performance on unseen validation data (to avoid overfitting during training)

Setup for training and testing

- Training dataset: used for training the model
- Testing dataset: used for final evaluation and
- Validation dataset: used for tune hyperparameters and check for overfitting
- Each dataset has authorized and unauthorized user, that contain face and fingerprint images.

Evaluation procedure

- **Model Training**: this is a process of training model by using training dataset, an epoch is a parameter in which loss and accuracy are monitored.

- **Validation**: this the model is assessed using the dataset for each epoch to check for overfitting or underfitting.
- **Testing**: this dataset is used to assess the trained model by using new biometrics images (new fingerprint and face images)
- **Confusion Matrix**: this is to visualize correct and incorrect predictions for the two classes (authorized and unauthorized)

3.6.Procedure

This paper use publicly available dataset from "kaggle" whereby biometric information is gathered or downloaded, the downloaded dataset is structured for model training. Once the model has been trained using datasets, performance evaluation is done using different metrics.

- Data Collection:

Dataset: fingerprint and face images datasets from Kaggle, the dataset is structured in two classes (Authorized and Unauthorized). Data Collection Method: The face and fingerprint images were downloaded directly from Kaggle's repositories. The images were categorized and stored in subfolders under two main categories: **Authorized** and **Unauthorized**, further split into face and fingerprint modalities. **Dataset structure:** C:\Users\HP\Desktop\FD\Train\Authorized and C:\Users\HP\Desktop\FD\Train\Unauthorized. **Inclusion**: valid fingerprint and face images are included. **Exclusion**: low quality or bad fingerprint and face images are excluded.

- Data Preprocessing**:**

This is a process of manipulating fingerprint and face images for the next process (for model training)**, Resizing**: all fingerprint and face images in dataset is resized to 224 pixels x 224 pixels which is mainly required by the model. **Normalization**: the process in which fingerprint and face images pixel values normalized between 0 and 1 to ensure model code converge more efficiently. **Labeling**: each fingerprint and face images are labelled as authorized and unauthorized. **Data Splitting**: this the structure of dataset used for training the model. Training dataset (70%), validation dataset (15%) and testing dataset (15%).

- Model Framework:

This study is using powerful machine learning models frameworks like tensorflow and keras. These tools are used to define, train and evaluate MobileNetV2 architecture. MobilenetV2 is a light weight architecture which is appropriate for Internet of Things devices because of its high efficiency and low computation cost.

Model Training: model training is performed on laptop machine using CPU for process acceleration. Loss function is used in this training is binary cross-entropy and Adam is used as an optimizer. The model has been trained using different epochs with image batch size of 32. Data augmentation technique is used for flipping image horizontal, for image zooming and rotation to enhance model generalization without creating additional images.

- Model Evaluation:

For this experiment the model's performance was evaluated using **accuracy**, **precision**, **recall**, **F1-score**, and **loss** on both the validation and test sets. After training, the model was tested on the **unseen test set** to assess its ability to generalize to new data and a **confusion matrix** was generated to visualize the number of correct and incorrect classifications.

- Results and Interpretation:

Key Findings: The model achieved high accuracy, suggesting that it was capable of distinguishing between **Authorized** and **Unauthorized** users. Precision and recall scores were balanced, indicating that the model did not heavily favor one class over the other.

Limitations: Some misclassifications occurred, particularly when images of poor quality were included or when the model faced variations in lighting or pose for face images.

3.7.Data Analysis

The data analysis method employed in this work is closely related to the nature of the biometric authentication problem using deep learning for IoT security and the research subjects. The selected analytical methods can effectively extract meaningful insights from the dataset and offer valuable responses to the research inquiries. First research question: What is the best method to use deep learning to improve biometric authentication in Internet of Things devices in terms of accuracy and reliability? Performance Measures for the Model: Metrics like accuracy, precision, recall, F1-score, and loss were tracked during the deep learning model's training, validation, and testing

stages. Confusion Matrix: The confusion matrix provided detailed insights into the number of true positives, true negatives and false positives

Method of Analysis:

- Descriptive Statistics: For the purpose of statistically assessing the model's capacity to authenticate users using biometric inputs (facial and fingerprint), the accuracy, precision, recall, and F1-score were determined. An evaluation of overall performance was given using these metrics.
- Comparison of Validation and Test Results: The model's performance was examined on both the validation and test datasets to guarantee its dependability. We were able to determine any possible overfitting or underfitting problems as a result.

Research Question 2: How to fuse multiple forms of biometric data, such as fingerprints and facial recognition, for IoT security?

Information Obtained: Information about the joint usage of fingerprint and facial photographs for authentication was gathered. A dataset with both modalities was used to train the model, and the outcomes of the multimodal and unimodal approaches—that is, utilizing only face or fingerprint images—were contrasted.

Research Question 3: How does the proposed deep learning-driven multi-factor biometric authentication system compare with state-of-the-art methods in terms of accuracy and security?

- Data Obtained:
  - **Model Accuracy**: trained model accuracy of biometrics system
  - **Security Metrics**: FAR and FRR

3.8.Ethical concerns

Conducting research on biometric authentication, particularly involving deep learning and IoT security, raises several ethical concerns that must be addressed to ensure the integrity of the study and the protection of participants' rights. Below are key ethical considerations:

- Informed Consent
  - **Description**: Participants must be fully informed about the nature of the study, its purpose, and the data being collected before they agree to participate.
  - **Implementation**: Provide a clear and concise consent form detailing the study's aims, procedures, potential risks, and benefits. Ensure participants understand they can withdraw their consent at any time without penalty.
- Confidentiality and Data Privacy
  - **Description**: Protecting participants' personal information is crucial, especially when dealing with sensitive biometric data such as fingerprints and facial images.
  - **Implementation**:
    - **Anonymization**: Remove personally identifiable information (PII) from the dataset, using unique identifiers instead.
    - **Data Encryption**: Use encryption methods to protect data during storage and transmission, limiting sensitive information access to authorized personnel only.
    - **Access Restrict**: Restrict access to data to researchers directly involved in the study, ensuring that unauthorized individuals cannot view or misuse participant information.
- Data Security
  - **Description**: putting strong security measures in place to protect gathered data from breaches or illegal access.
  - **Implementation**:
    - Use secure servers for data storage, implementing firewalls and intrusion detection systems.
    - Regularly update software and protocols to protect against vulnerabilities.
    - Conduct security audits to identify and mitigate potential risks.
- Participant Rights

- **Description**: Participants should understand their rights with regard to the research procedure and their data.
- **Implementation**:
    - Make sure that if a participant decides to leave the research, they have the option to view their data, ask for changes, or have it deleted.
    - Maintain transparency about how their data will be used and for what duration it will be stored.

- Bias and Fairness
    - **Description**: Address the potential for bias in the biometric data gathering process, which could lead to unequal treatment or discrimination.
    - **Implementation**:
    - Use diverse datasets that represent different demographic groups to minimize bias in model training and evaluation.
    - Analyze the model's performance across various demographic groups to ensure equitable outcomes.

CHAPTER FOUR: PROPOSED SYSTEM

The biometric authentication issue that we previously highlighted is resolved in this part by utilizing deep learning models and feature fusion approaches for IoT security. The solution addresses the challenges of lightweight biometric authentication systems appropriate for Internet of Things devices, where both fingerprint and face data are fused for robust identity verification. The theoretical framework, methods, and system we developed are described here, along with an explanation of the parts taken from previous research.

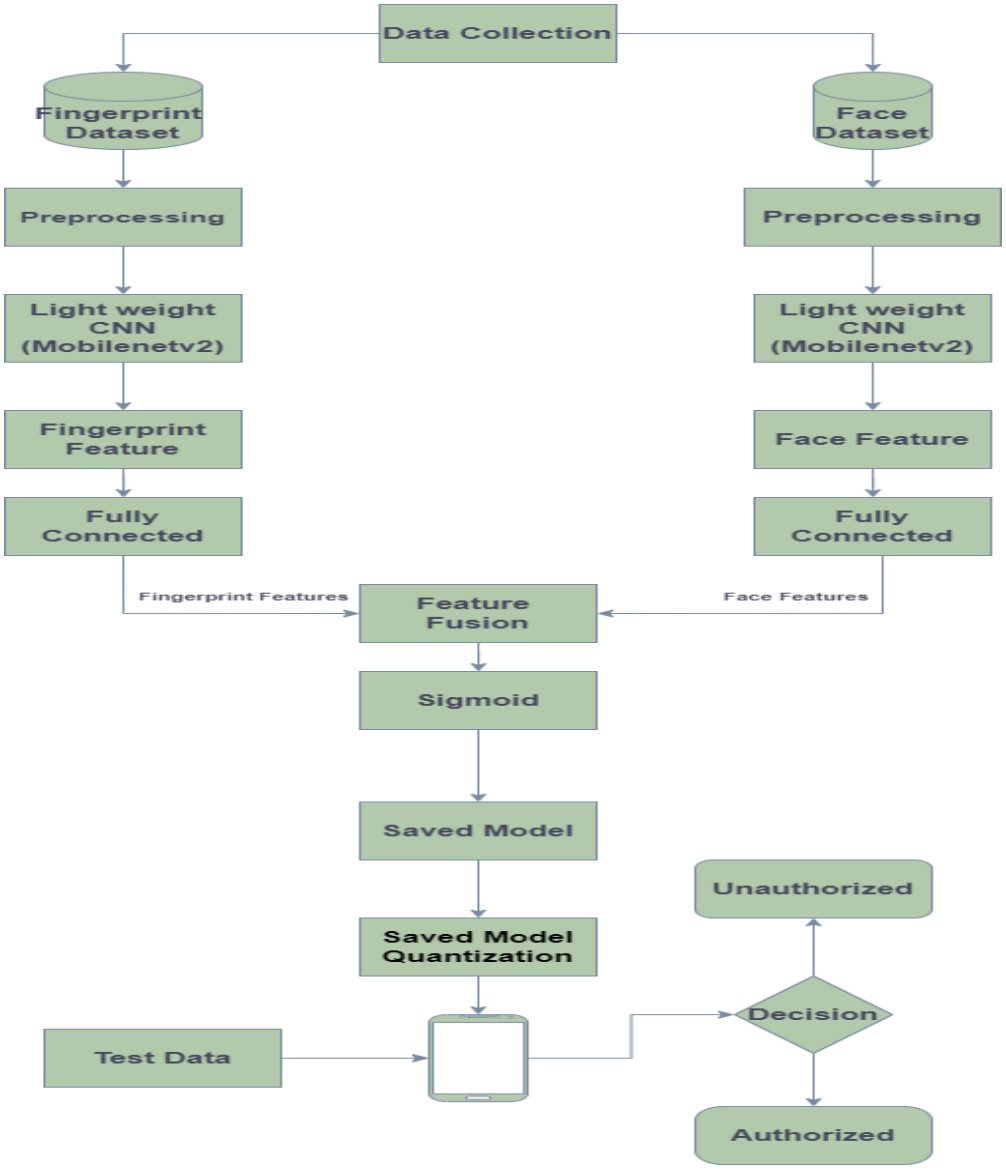


Figure 3: Proposed System Architecture

Theoretical Framework

Fingerprint and face data are used as a biometric authentication for the proposed solution. Features are extracted from both fingerprint and face images using light weight deep learning. For its efficiency in resource constrained environment MobileNetV2 is used.

System Architecture Components

- Fingerprint Processing Pipeline: fingerprint images are utilized as input and then easily extract features from fingerprint images using MobileNetV2, preprocessing like image resize is very important. Additionally, image normalization, image pixel size and noise removal are crucial for image quality to extract features easily. for feature extraction I use pretrained MobileNetV2 which extract high level features from fingerprint images that produce fingerprint vector.
- Face Processing Pipeline: face images are utilized as input and similar to fingerprint, face images are preprocessed to maintain good contrast and feature alignment like eyes, mouth and nose. I use pretrained MobileNetV2 which extract features from face images that produce a face feature vector.
- Preprocessing**:** is a process of image manipulation used to scale fingerprint and face images to the range [-1,1].
- Feature Extraction**:** I use MobilenetV2 to extract high-level features from both fingerprint and face image.
- Feature Fusion**:** after feature extraction take place, both fingerprint and face image features are fused. The concatenation of these biometrics modalities makes the biometric authentication system more robust which is one contribution of this study. The subsequent stage is to compute score value from the fused / concatenated features to distinguish the likelihood of an identity match.
- Decision Module**:** Finally, the computed score is compared the with the defined threshold value to ascertain if the person is authorized or unauthorized.
- Algorithms Used**:** different algorithms are utilized in MobileNetV2 model such as activation function, global average pooling and batch normalization. In neural networks, an activation function is a mathematical function that uses a neuron's input to determine its output. MobilenetV2 uses ReLU6 and its main function is to minimize the risk of overflow

in low precision hardware. MobilenetV2 uses ReLU6 and its main function is to reduce the risk of overflow in low precision hardware. Global Average Pooling is a technique often used in convolutional neural networks (CNNs) for extracting the spatial information from feature maps. Batch Normalization is a method used to make training of model faster and more stable through normalization of the layer's inputs. Dropout Regularization is mainly used to prevent overfitting by randomly dropout neurons during training. Concatenation is a process of combining fingerprint and face image features of an identity.

$$Y=[x^{fingerprint},x^{face}]$$

Where:

- Y is concatenated / fused feature

Each neuron in a fully connected layer neural network uses a weight matrix to apply a linear transformation to the input vector. For binary classification, Binary Cross-Entropy Loss is typically employed. Stochastic gradient descent with flexible learning rates is extended by the Adam optimizer. Lastly, we employ sigmoid for output layer binary classification.

Table 3: MobileNetV2 Architecture

Input	Layer	t	c	N	s
224x224x3	Conv2d	-	32	1	2
112x112x32	Bottleneck	1	16	1	1
112x112x16	Bottleneck	6	24	2	2
56x56x24	Bottleneck	6	32	3	2
28x28x32	Bottleneck	6	64	4	2
14x14x64	Bottleneck	6	96	3	1
14x14x96	Bottleneck	6	160	3	2
7x7x160	Bottleneck	6	230	1	1
7x7x320	Conv2d 1x1	-	1280	1	1
7x7x1280	GlobalAvgPool	-	1280	1	-

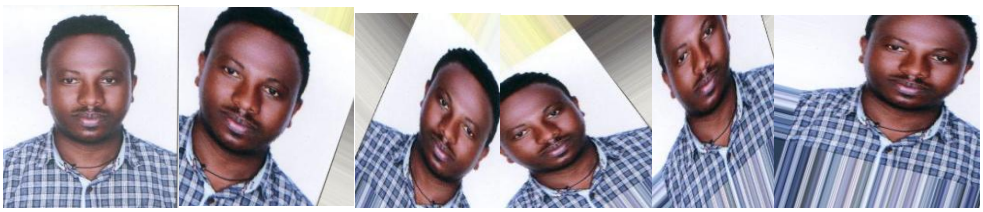
Data Augmentation

The code uses ImageDataGenerator to augment the images before training. The augmentation operations include random transformations such as rotations, shifts, zooms, flips, and brightness

changes. Mathematically, for an image transformation, the augmented image x′ is obtained from the original image x via a transformation matrix T:

$$X^{'}=T(x)$$

Where T could represent a combination of affine transformations like rotation, translation, scaling, and flipping.



a) original b) augmented0 c) augmented1 d) augmented2 e) augmented3 f) augmented4

Figure 4: Augmented Face Image

a) original b) augmented0 c) augmented1 d) augmented2 e) augmented3 f) augmented4

Figure 5: Augmented Fingerprint Image

Trained Model Conversion

Model Quantization

A trained machine learning model's size and computational complexity can be decreased in this study without noticeably affecting its accuracy by using the post-model quantization technique. It's particularly beneficial for deploying models on resource-constrained devices like smartphones and embedded systems. Additionally, this contributes to the model's increased lightweight.

Quantization Process

- **Training:** Train the MobileNetV2 model on your target dataset.
- **Full-precision Inference:** Evaluate the model's performance using full-precision (32-bit floating-point) weights and activations.

- **Quantization:** Chosen schemes are 8-bit integer quantization and 16-bit mixed-precision quantization.

We develop application that convert Trained model to TensorFlow lite (tflite). Then this TensorFlow lite is run on android IoT devices like smart phone. By using TensorFlow lite model we develop android application to test the trained model. Figure 6 show that how trained model can be converted to tensorflow lite and then deployed to android device.

Table 4: Base Model Vs Quantized Model

Metric	Base Model (MobileNetV2)	Quantized Model (Lightweight Model)
Model Size	53.88 MB	4.90 MB
Inference Time	3878.13 ms	1561.52 ms
Accuracy	0.912	0.890

This table (Table 4) contrasts the performance and size of a standard MobileNetV2 model with a quantized, streamlined version of the same architecture. The evaluation is conducted across three

major criteria: model size (indicated in megabytes), inference time (indicated in milliseconds), and accuracy.

The findings clearly illustrate the effect of quantization on the efficiency of the model. The quantized version shows a significant reduction in size, decreasing from 53.88 MB to just 4.90 MB. This equates to approximately a 90% reduction in model size, making the quantized model much more adaptable for storage and better suited for deployment on devices with limited resources.

Inference time also experiences considerable enhancement. The quantized model records an inference time of 1561.52 ms, in contrast to 3878.13 ms for the original model. This results in a reduction of over 59% in inference time, suggesting that the quantized model can handle data much more quickly, which is vital for real-time applications.

Although quantization considerably enhances model size and inference efficiency, there is a minor compromise in accuracy. The original model reaches an accuracy of 0.912, while the quantized model has a slightly reduced accuracy of 0.890. This indicates a decline of roughly 2.4%. Nonetheless, despite this minor accuracy loss, the significant improvements in size and speed may render the quantized model a more attractive option based on specific application demands and the relative importance of accuracy against efficiency.

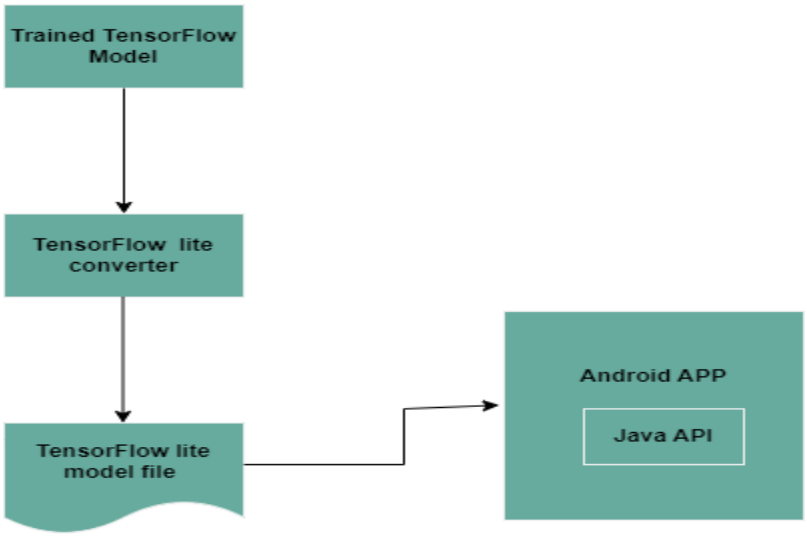


Figure 6: Tensorflow lite process

Implementation of the proposed system

The proposed system consists of different components that ensure the IoT device authentication using biometrics and lightweight deep learning.

1. Data collection

Two datasets are collected, fingerprint dataset and face dataset.

$X_{fingerprnt} = \{x_{finger1}, x_{finger2}, x_{finger3}, \ldots\ldots\ldots, x_{fingern}\}$ and

$X_{face} = \{x_{face1}, x_{face2}, x_{face3}, \ldots\ldots\ldots, x_{facen}\}$

Where:

$X_{fingerprint}$ is fingerprint images

X_{face} is face images

2. Preprocessing

The goal of this preprocessing is to resize and normalize the input fingerprint and face images dimensions.

2.1.Resizing

$X'_i = R(x_i)$, where R is the resizing function to fixed dimension dxd. For both face and fingerprint images we resize them to 224x224 resolution.

2.2.Normalization

Each image of fingerprint and face (x_i) are normalized to range between [0,1]

$X_i'' = \frac{xi}{255}$ for each pixel intensity in the image

3. Lightweight CNN (MobilenetV2)

This lightweight deep learning model use depthwise separable convolutions to reduce the computational cost.

3.1.Standard Convolution

$$Y=\sigma(W*X+b)$$

Where:

X is input feature map (preprocessed face and fingerprint images),
W is the learned weight,
b is the bias,
σ is an activation function,
* denotes convolution

3.2. Depthwise Convolution

$Y_{dw}=X*W_{dw}$, where W_{dw} are the depthwise filters

3.3. Pointwise convolution

A 1x1 convolution applied after the depthwise convolution to mix the channels.

$$Y_{pw}=Y_{dw}*W_{pw}$$

Each Mobilenetv2 model for face and fingerprint images will learn feature maps (fingerprint features and face features).

$$F_{finger}=\text{MobileNetV2}(X_{finger}),\ F_{face}=\text{MobileNetV2}(X_{face})$$

Where F_{finger} and F_{face} learned features for fingerprint and face images respectively.

Table 5: Model Selection Criteria

Feature	MobileNetV2[51]	ResNet[52]	EfficientNet[53]
Efficiency	Highly efficient, designed for mobile and embedded devices.	Less efficient, computationally intensive.	More efficient than ResNet, but less than MobileNetV2.
Accuracy	High accuracy, especially considering its efficiency.	Very high accuracy, but computationally expensive.	Very high accuracy, but more computationally intensive than MobileNetV2.
Model Size	Small model size, suitable for IoT devices with limited memory.	Larger model size.	Larger model size than MobileNetV2.
Inference Speed	Fast inference speed, ideal for real-time applications.	Slower inference speed.	Faster inference speed than ResNet, but slower than MobileNetV2.

Table 5 shows the comparison of lightweight models used for IoT devices. Based on the feature shown in table 4 MobileNetV2 is preferable in terms of efficiency, accuracy, model size and inference speed. So, in our proposed solution we use MobileNetV2 because good performance on the feature listed in the table 4.

4. Feature Fusion

There are different fusion techniques that fuse different biometrics modalities. By conducting an experiment on different fusion techniques, the following result is observed.

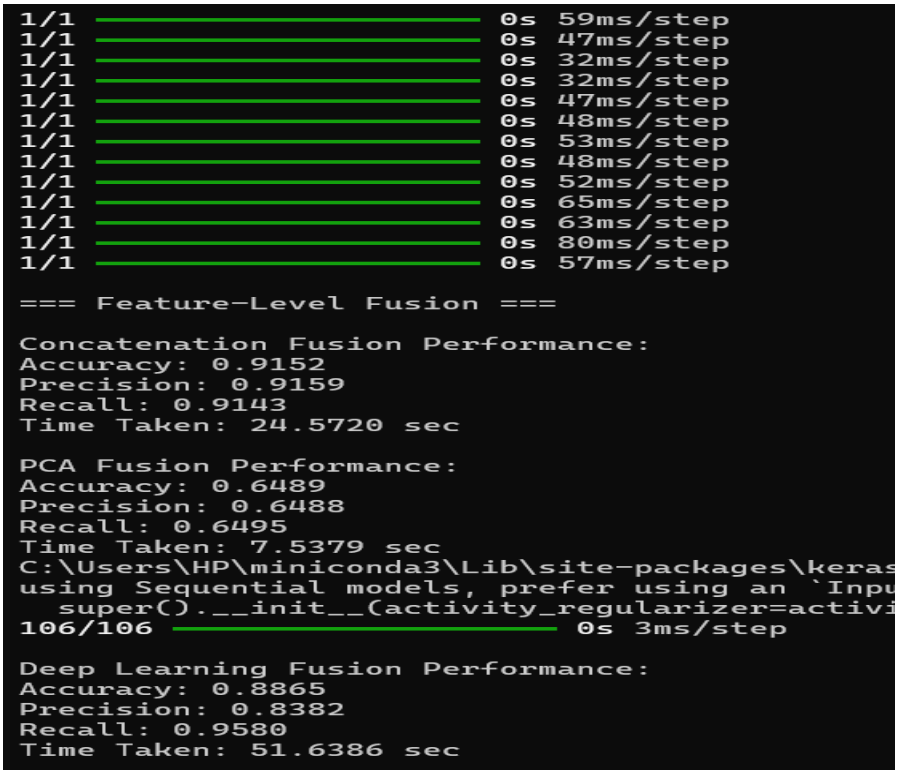


Figure 7: Feature-Level Fusion Techniques

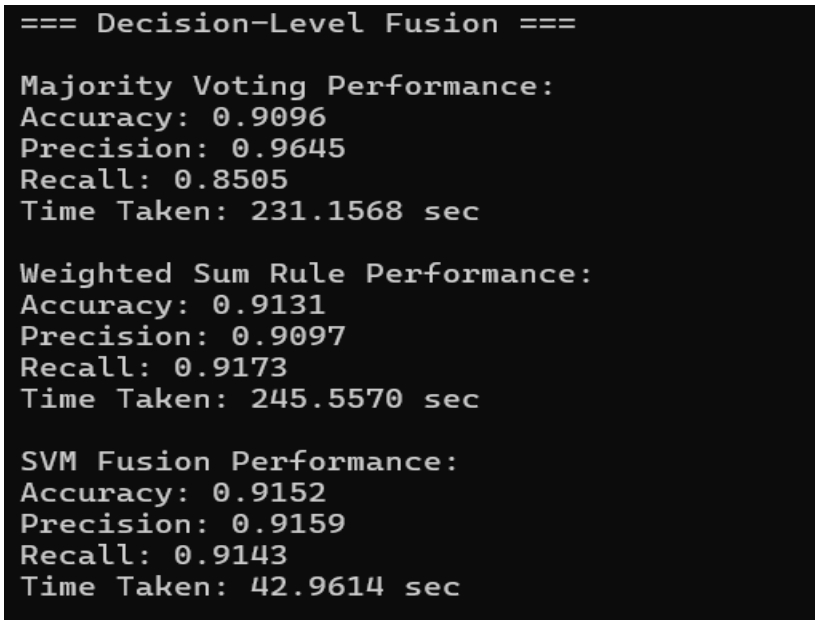


Figure 8: Decision-Level Fusion Techniques

From the results obtained, a number of important conclusions can be made about the efficacy of various biometric fusion methods for the specified task of recognizing fingerprints and faces.

Concatenation (Early Fusion) stands out as a notably effective method, showing a solid equilibrium of accuracy, precision, and recall. Its results indicate that merging features from both modalities directly yields a comprehensive representation for the classifier, successfully encapsulating complementary information.

PCA-based fusion shows a notably reduced performance when compared to concatenation. This considerable decrease in accuracy implies that utilizing PCA following feature concatenation may be eliminating important discriminative details, indicating that the selected principal components may not be well-suited for the classification objective.

Deep learning-based fusion delivers satisfactory results, although it doesn't quite match the performance of concatenation. This suggests that although deep learning models are capable of understanding intricate relationships among features, they might need additional architectural adjustments or a larger dataset to fully utilize the information from both modalities in this particular scenario.

Decision-level fusion methods, such as majority voting and the weighted sum rule, deliver performance that is on par with concatenation. This underscores the success of merging decisions made by independently trained classifiers, suggesting that each modality contributes important and fairly independent insights. The comparable outcomes of majority voting and the weighted sum rule (when using equal weights) imply that, in this instance, aggregating decisions is just as effective as applying equal weights.

To summarize, for the specific biometric recognition challenge at hand, utilizing simple feature-level fusion through concatenation is a strong and effective strategy. Although other methods like decision-level fusion also demonstrate impressive results, they do not considerably exceed the performance of the straightforward concatenation approach. In this case, PCA appears to hinder performance, indicating that applying dimensionality reduction after concatenation is not appropriate for this data. Deep learning has potential but requires additional exploration to achieve the performance metrics set by concatenation. These results emphasize the significance of careful

selection of techniques and point to the necessity for extensive testing when developing a biometric fusion system.

Table 6: Different Fusion Techniques

Fusion Technique	Accuracy	Precision	Recall	Time Taken (sec)
Concatenation	0.9152	0.9159	0.9143	24.572
PCA Fusion	0.6489	0.6488	0.6495	7.5379
Deep Learning Fusion	0.8865	0.8382	0.958	51.6386
Majority Voting	0.9096	0.9645	0.8505	231.1568
Weighted Sum Rule	0.9131	0.9097	0.9173	245.557
SVM Fusion	0.9152	0.9159	0.9143	42.9614

Concatenation fusion techniques is used that fuse both features modalities which are represented as follows;

$$F_{concat}=[F_{finger}||F_{face}]$$

Where || denotes Concatenation.

5. Classification

After feature fusion of both fingerprint and face features, then pass it to fully connected layer for classification. The fully connected layer maps the concatenated feature vector F to a binary output (Authorized/Unauthorized).

For classification we use sigmoid function, because it is used for binary classification (in our case Authorized and Unauthorized)

5.1.Fully connected layer

$$Z=W_f \cdot F+b_f$$

Where:

- W_f are the learned weights for the fully connected layer,
- F is the concatenated feature vector,
- B_f is the bias.

5.2.Binary classification

The binary classification output is given by;

$$Ý = \sigma(Z)$$

where σ is the sigmoid activation function:

$$\sigma(Z)=\frac{1}{1+e^{-z}}$$

This will output a value between 0 and 1, which represents the probability of the input being **Authorized** or **Unauthorized**.

6. Loss Function and Optimization

Since we use binary classification, the appropriate loss function used is Binary Cross-Entropy;

$$L(y,ý) = -[y\log(ý)+(1-y)\log(1-ý)]$$

Where:

y is the true label (Authorized/Unauthorized)

ý is the predicted probability.

7. Model Quantization for IoT deployment

We use post-quantization techniques to reduce the precision of weights and activations from 32-bit floating point to lower precision to make the model more lightweight.

7.1.Quantization Function

$$Q(x)=\text{round}(x\times\text{scale}+\text{zero\_point})$$

where:

- x is the floating-point value,
- scale and zero_point are parameters used to map the floating-point range to integer values.

For IoT devices, this minimizes the model size and inference time.

8. Deployment and decision making

Once the quantized model is deployed on the IoT device, the system inputs test data (a pair of fingerprint and face images) and the final decision is based on the model's output ý.

If:

ý >0.5, classify as Authorized,

ý<0.5, classify as Unauthorized

This decision-making process can trigger access to resources (unlocking a device) or deny access based on the prediction.

Table 7: Fusion Techniques

Fusion Techniques	Advantages	limitations
Sensor-level fusion[54]	The information content is the largest and the richest at this level.	Multimodal biometric systems require samples from different modalities to be combined which may not be compatible and hence, cannot be used for SLF
Feature-level fusion[54]	Feature vectors contain second richest level of information as compared to the raw	Concatenation of feature vectors results in an increase in number of feature vector dimensions

	biometric data.	
Match-score level fusion [54]	Match scores are the smallest in size compared to the raw data and feature vector.	Match scores are required to be normalized before fusion.
Decision-level fusion [54]	Fusion of decisions allows for the use of independent, unimodal biometric authentication products off-the-shelf.	Relative performances of the matchers must be taken into consideration while forming the final decision.

Table 7 show that different fusion techniques used in biometrics. Sensor-level fusion is a fusion technique in which raw data are fused at sensor level [54]. In feature-level fusion the feature from different modalities data is fused to make one feature vector [54]. For our proposed system we use feature-level fusion in which rich of information is available from different biometric datas. Match-score level fusion is another fusion technique that contain small size information when compared to feature vector [54]. Decision-level fusion techniques is for the use of independent unimodal biometrics [54].

CHAPTER FIVE: EXPERIMENTS AND ANALYSIS

In this section, experimental setup and the conducted experiments are described, then the results are analyzed.

Experimental Setup

The system is implemented using Python, a programming language that is simple to use. Keras python library is used to develop the proposed model. This study uses SOCOFing (from Kaggle) dataset for fingerprint and LFW (from kaggle) dataset for face.

Hardware: The training was performed on a local machine with the following specifications:

- Processor: [12th Gen Intel(R) Core(TM) i7-1255U 1.70 GHz]
- RAM: [16 GB]

Software and Tools Used

- **TensorFlow**: The deep learning framework used to develop the model. Tensorflow is a popular open-source machine learning framework which is developed by Google. We use this framework in our experiment because of many reasons. Data preprocessing, model training and evaluation are the advantages of tensorflow. We can use this framework with different platforms to deploy our machine learning models on different environments.
- **Keras**: The high-level API for TensorFlow used for building the model. Keras is a valuable tool for building and training deep learning models because it offers simplicity, modularity, flexibility, ease of use, and integration with TensorFlow.
- **NumPy**: Used for data handling and array manipulation. The metrics like accuracy, precision, F1-score and recall are calculated using numpy.
- **Python**: The primary programming language used for implementing the model and running experiments.
- **Android Studio**: For integrating the TensorFlow Lite model into an Android application. We use this tool for testing our proposed system on android smartphone.

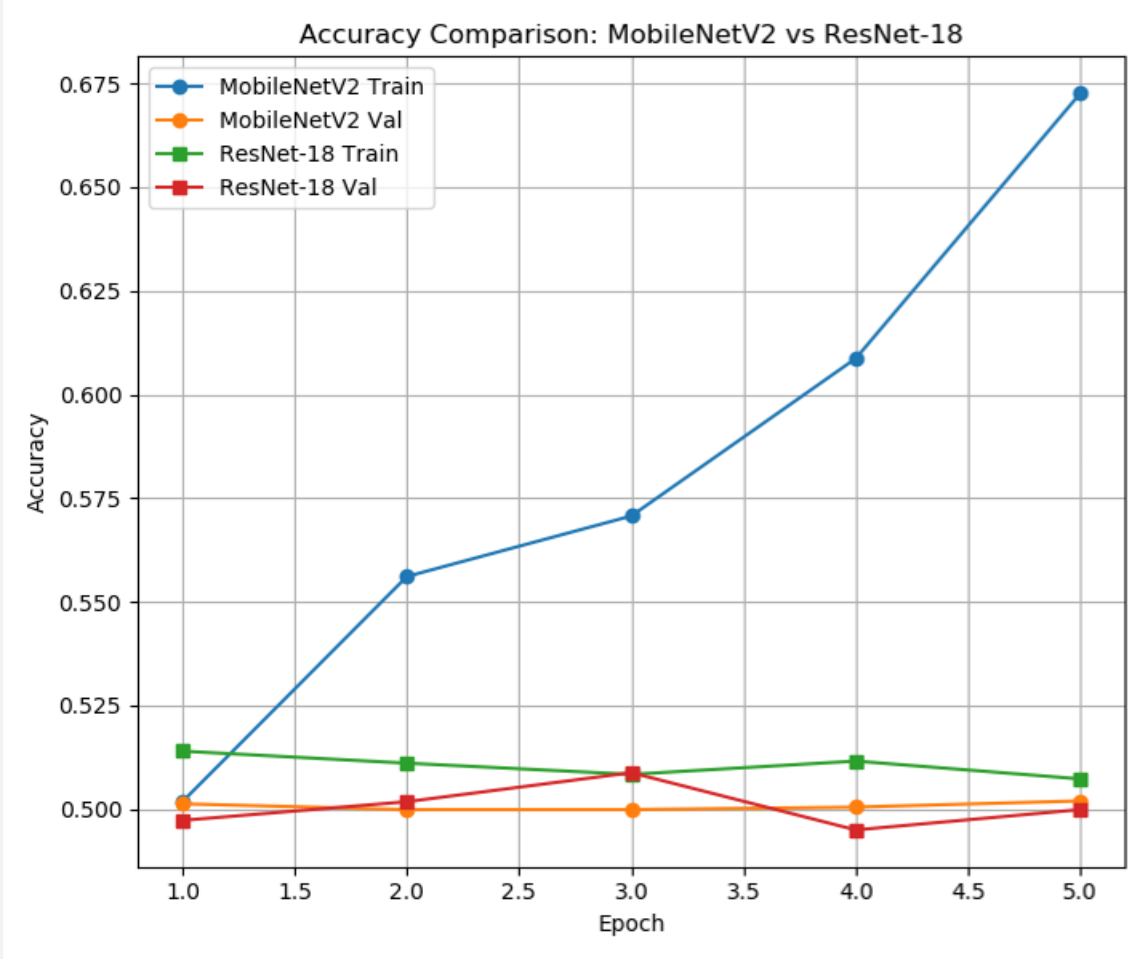


Figure 9:Model Accuracy of MobileNetV2 vs ResNet-18

The figure 9 above show that detail analysis of experimental results for MobilenetV2 and ResNet-18 on the dataset used in this work. The primary aim of this experiment is to compare the performance of MobileNetV2 and ResNet-18. In terms of accuracy, MobileNetV2 achieving higher accuracy in both training and validation sets compared to ResNet-18. This indicates that MobileNetV2 is better to generalize the unseen data. In terms of training convergence, MobileNetV2 is faster and smoother, reaching higher accuracy in fewer epochs than ResNet-18. Generally, MobileNetV2 emerged as a stronger performance demonstrating superior accuracy and faster convergence compared to ResNet-18 on the dataset. The depth-wise convolution of MobileNetV2 make it more efficient and less prone to overfitting.

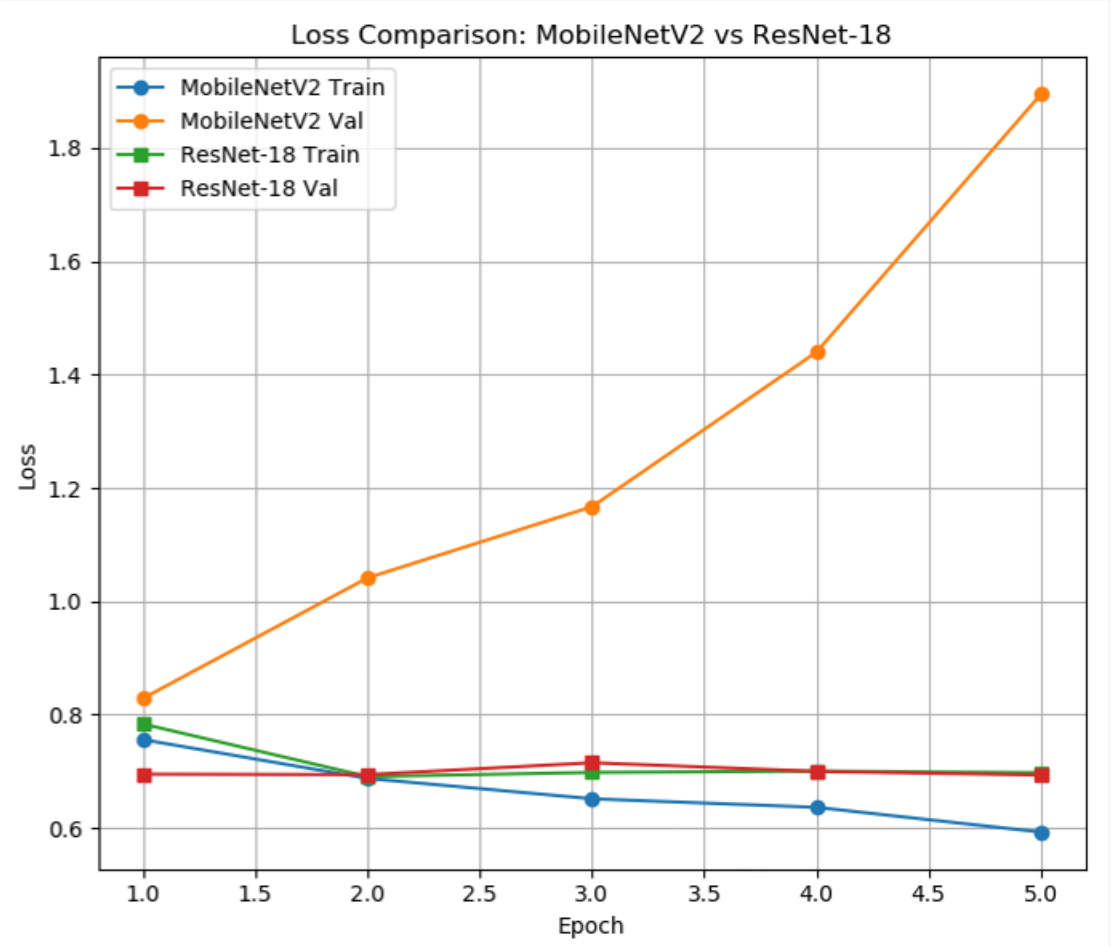


Figure 10:Model Loss of MobileNetV2 vs ResNet-18

In the above figure 10, MobileNetV2 shows a significant decrease in both training and validation loss over epochs indicating that the model is so effective in learning and generalization than ResNet-18. In ResNet-18, while the training loss decreases the validation loss remains high and fluctuates, which indicates overfitting. The gap between training and validation loss in MobileNetV2 is smaller, indicating that less overfitting. The large gap between training and validation loss in ResNet-18 suggest overfitting. The model is better in training data but struggles to generalize unseen data.

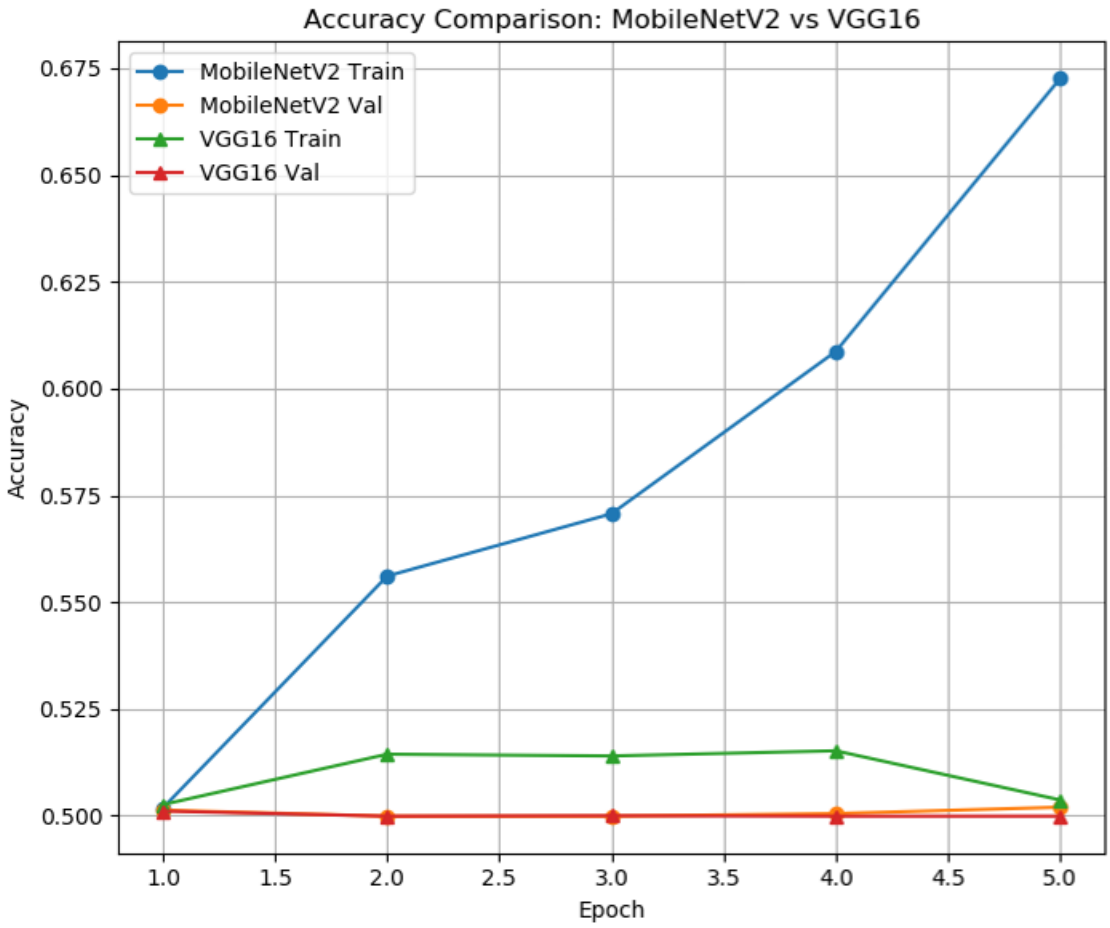


Figure 11:Model Accuracy of MobileNetV2 vs VGG16

Figure 11, demonstrates MobileNetV2 a significant improvement in accuracy over epochs, with both training and validation accuracy increasing substantially. While in VGG16 the training accuracy increases, the validation accuracy remains relatively low and stagnant, suggesting overfitting. MobileNetV2 consistently outperforms VGG16 in both training and validation accuracy. The gap between training and validation accuracy for MobileNetV2 is smaller, indicating less overfitting. The large gap between VGG16's training and validation accuracy suggests overfitting. The model is learning the training data too well but struggles to generalize to unseen data.

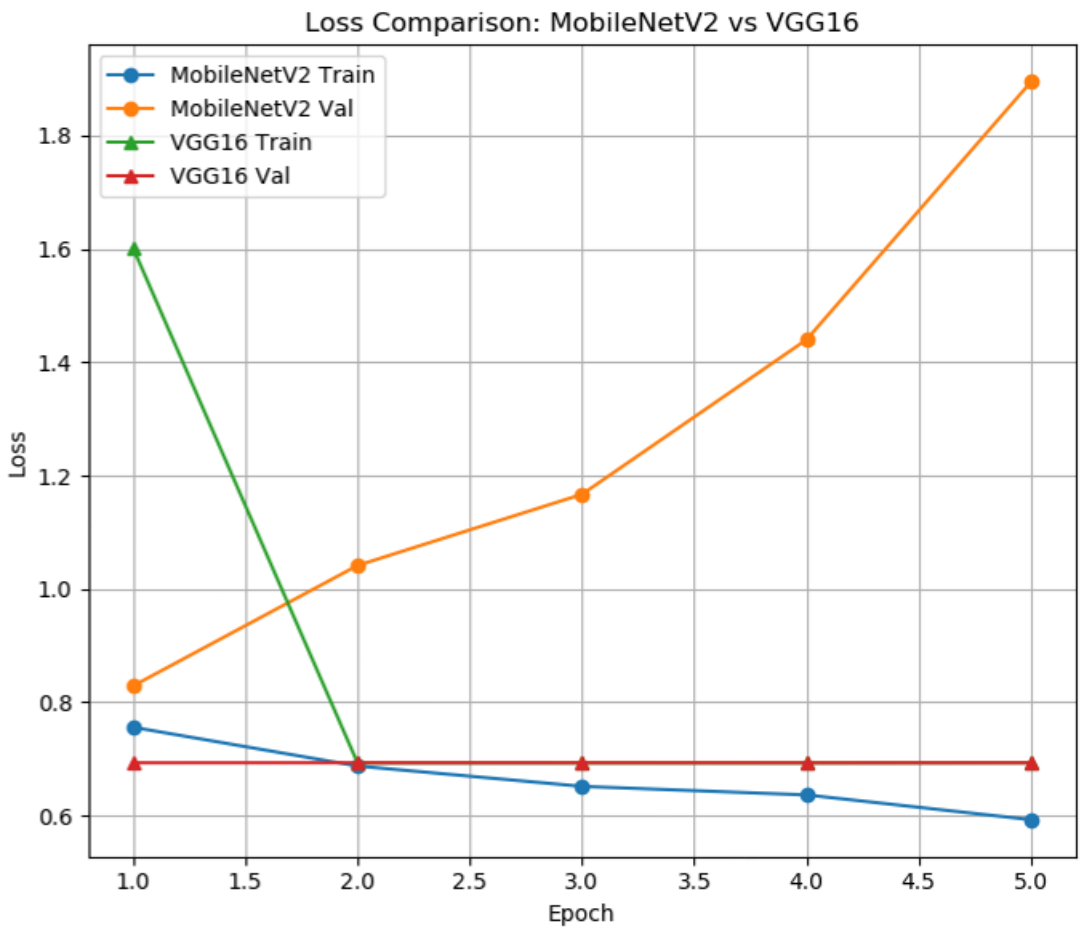


Figure 12:Model Loss of MobileNetV2 vs VGG16

The figure 12 shows that in MobileNetV2 there is a significant decrease in both training and validation loss over epochs, indicating effective learning and generalization. While in VGG16 the training loss decreases, the validation loss remains relatively high and fluctuates, suggesting overfitting. The gap between training and validation loss for MobileNetV2 is smaller, indicating less overfitting. The large gap between VGG16's training and validation loss suggests overfitting. The model is learning the training data too well but struggles to generalize to unseen data.

So based on the experiment conducted on the same dataset to compare the lightweight deep learning model, MobileNetV2 is better than the other models that is why we use it in our study.

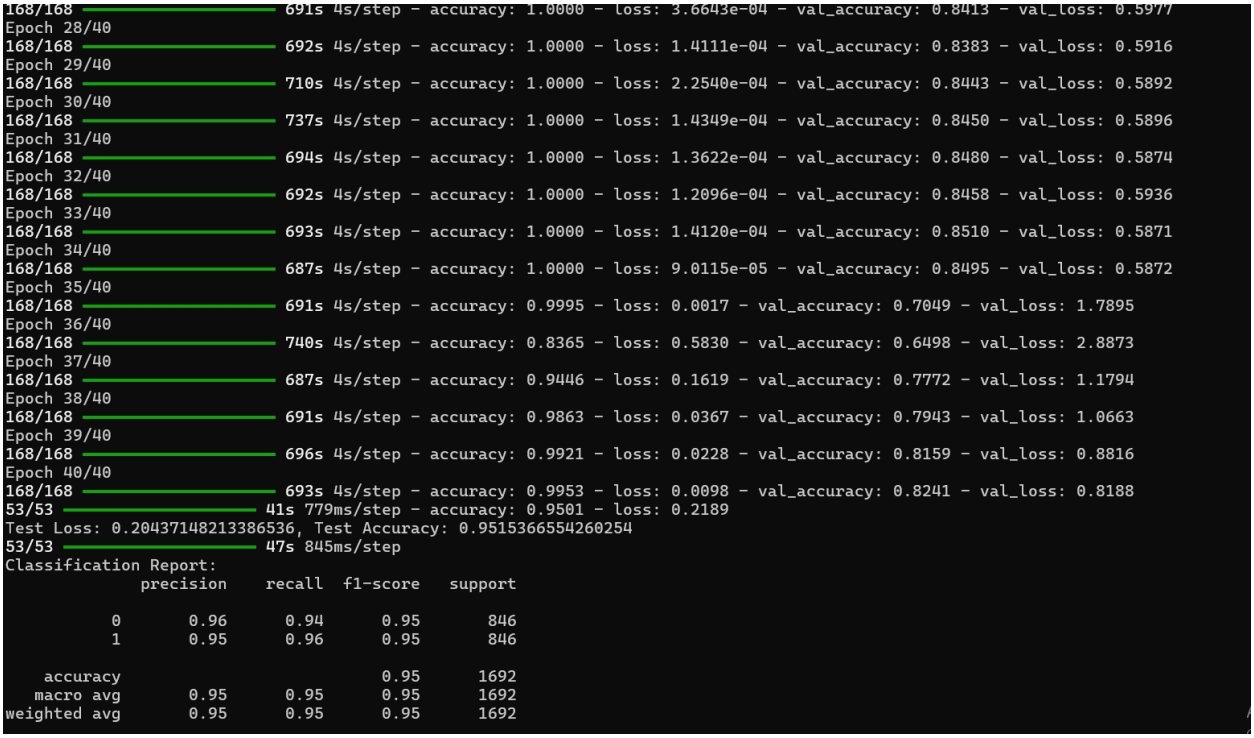


Figure 13:Model Training Results

In figure 13, despite some instability observed in the later epochs of the training process, the classification model showed encouraging performance overall. In particular, the model reached a commendable test accuracy of 0.9515 on a separate test dataset, reflecting its capacity to generalize effectively to new data. This implies that the model succeeded in extracting meaningful features from the training data, at least until a certain stage in the training regimen.

The classification report provides additional evidence of the model's efficacy, highlighting high precision (0.96 and 0.95) and recall (0.94 and 0.96) figures for both categories. This suggests that the model is proficient in accurately identifying instances from both classes, maintaining a solid balance between correctly identifying positive cases (precision) and capturing a significant proportion of real positive cases (recall). The F1-scores of 0.95 for each class further substantiate this claim, showcasing robust overall performance in terms of both precision and recall. The weighted and macro averages of 0.95 for precision, recall, and F1-score across all classes additionally validate the model's reliable performance and its capacity to manage a well-balanced dataset effectively.

To summarize, the favorable elements of the findings include:

High Test Accuracy: The model demonstrated a test accuracy of 0.9515, indicating strong generalization capability.

Robust Classification Metrics: The model achieved high precision, recall, and F1-scores for both classes, reflecting accurate and balanced classification performance.

Capable Feature Learning: The model identified distinguishing features that enabled acceptable performance on unseen data, despite some training instability.

Although further exploration and fine-tuning are required to tackle the training instability and potential for overfitting, the current outcomes suggest that the model has considerable potential for the classification task at hand. The obtained test accuracy and strong classification metrics establish a solid basis for additional development and enhancement.

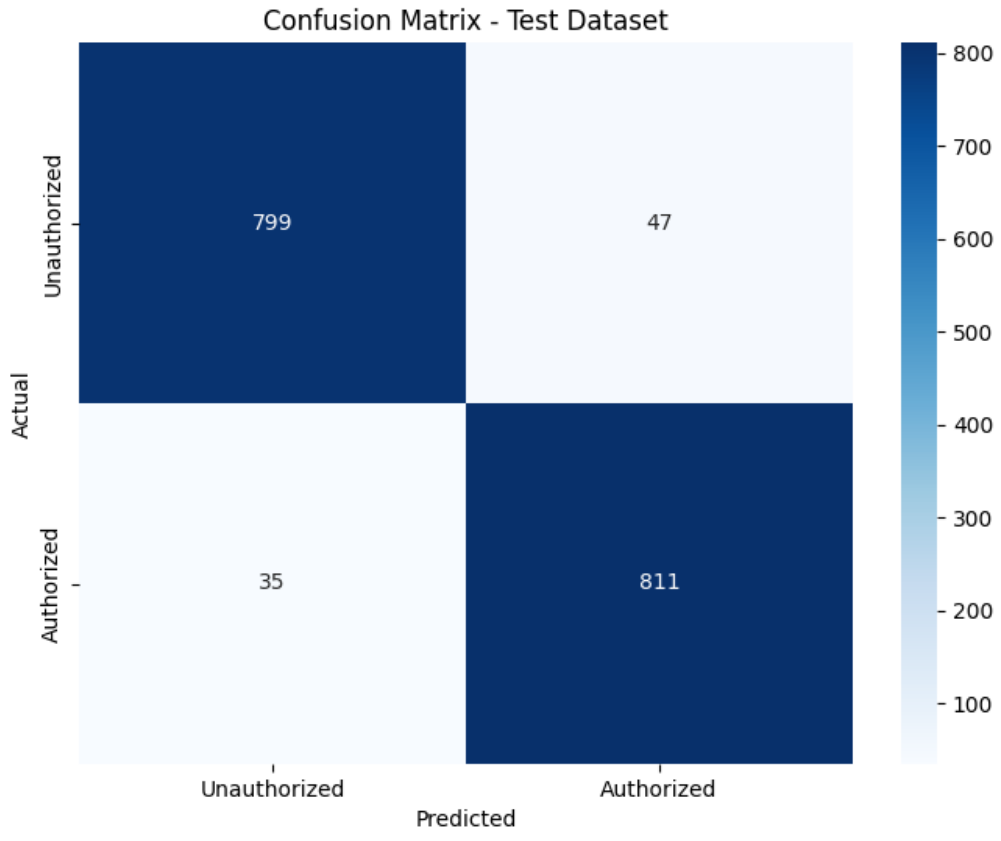


Figure 14: Confusion Matrix for Multi-Modal Biometric Authentication

The model shown in the matrix (Figure 14) exhibits strong effectiveness in distinguishing between "Unauthorized" and "Authorized" categories. For the "Unauthorized" category, the model accurately recognized 799 out of 846 actual "Unauthorized" cases, resulting in a significant number of true negatives. A smaller count of instances (47) was incorrectly categorized as "Authorized" (false positives). This reflects a minimal occurrence of inaccurately marking unauthorized actions as authorized, which is essential in applications where security is a priority.

In the same way, for the "Authorized" category, the model successfully identified 811 out of 846 actual "Authorized" instances as "Authorized" (true positives). Only 35 instances were mistakenly classified as "Unauthorized" (false negatives). This small number of false negatives indicates that the model performs well in detecting authorized activity, reducing the likelihood of obstructing legitimate users or actions.

The significantly higher values along the diagonal of the matrix (799 and 811) in contrast to the off-diagonal elements (47 and 35) suggest that the model exhibits robust predictive performance in both categories.

Summary of the results

Table 8: Performance Metrics of Authorized and Unauthorized Classes

Metrics	Authorized	Unauthorized
Accuracy	95.15%	95.15%
Precision	94.52%	95.80
Recall	95.86%	94.44%
F1-score	95.18	95.12

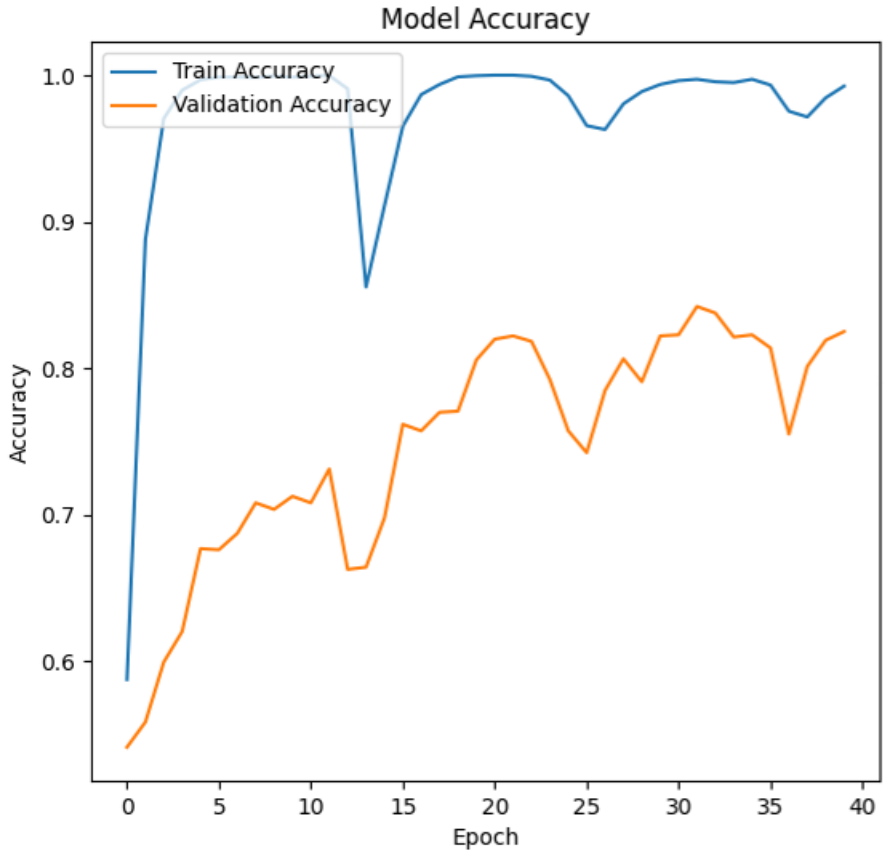


Figure 15: Model Accuracy Over Epochs

This graph (Figure 15) depicts the **model accuracy** over 40 epochs during the training of a machine learning model. It shows the changes in both **training accuracy** (blue line) and **validation accuracy** (orange line) as the number of epochs increases.

Description: Training Accuracy (Blue Line): Starts very low at the beginning (Epoch 0). Rapidly increases within the first few epochs, approaching 1.0 (or 100% accuracy). After around Epoch 5, it reaches near-perfect accuracy (close to 1.0) and stays relatively stable. There are minor dips around Epochs 15 and 30, but overall, it maintains high accuracy throughout the training process. **Validation Accuracy (Orange Line)**: Starts lower than the training accuracy. Increases gradually, improving consistently until around Epoch 20. Between Epochs 20 and 40, the validation accuracy fluctuates, reaching a peak and then dropping slightly multiple times. The

highest validation accuracy appears to be around 0.85 (or 85%) but never matches the training accuracy.

Key Observations: Overfitting: The training accuracy is almost perfect, while the validation accuracy is significantly lower and fluctuates more. This suggests that the model may be overfitting the training data, learning patterns specific to the training set that don't generalize well to new data (validation set). **Validation Accuracy Improvement**: Despite the fluctuations, the validation accuracy does improve gradually, showing that the model is learning, but it struggles to generalize as well as it performs on the training data. **Stability**: The training accuracy stabilizes quickly, while the validation accuracy shows more variance, indicating that while the model is learning, there might be room for improvement, such as better regularization or tuning of hyperparameters to avoid overfitting.

This line graph illustrates (Figure 12) the training and validation accuracy of a machine learning model over a series of epochs.

Key Elements:

- X-axis: Represents the number of epochs, or training iterations.
- Y-axis: Represents the accuracy, measured as a percentage.
- Lines: Two lines are plotted:
- Train Accuracy: demonstrates the model's performance on the training set of data.
- Validation Accuracy: Shows how well the model generalizes to unseen data (the validation set).

Interpretation:

- General Trend: Ideally, both the training and validation accuracy should increase as the model learns from the data. If the training accuracy increases significantly while the validation accuracy plateaus or decreases, it might indicate overfitting.
- Gap Between Lines: A large gap between the training and validation accuracy suggests overfitting. This means the model is learning the training data too well but struggles to generalize to new data.

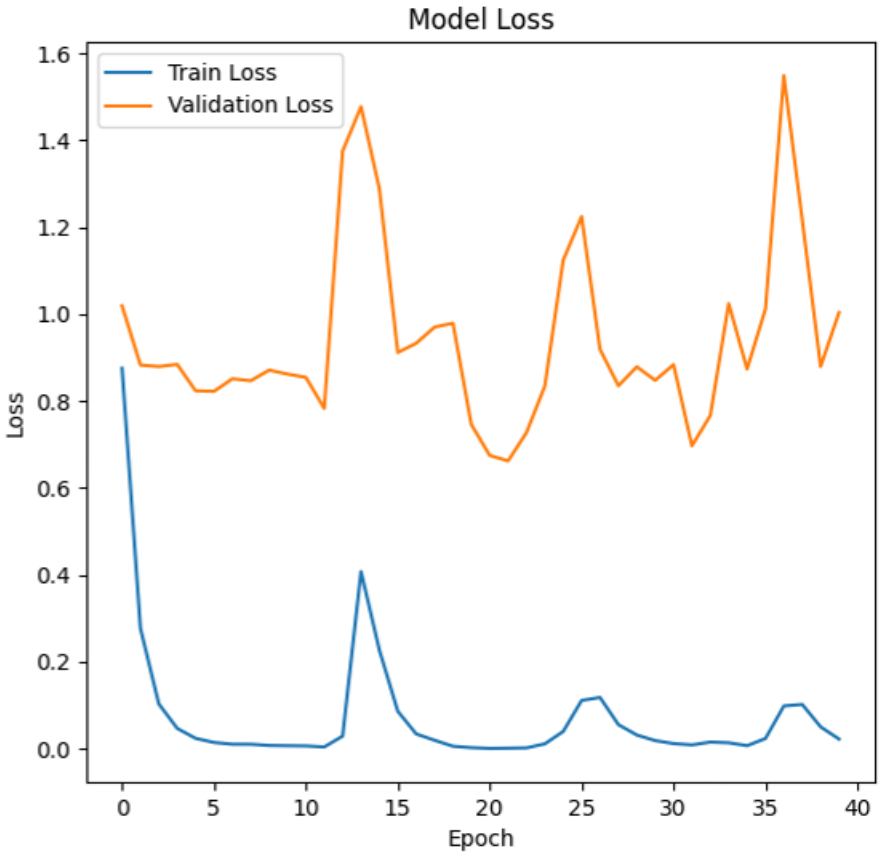


Figure 16: Model Loss Over Epochs

The provided graph (figure 16) illustrates the training and validation loss curves for a machine learning model over 40 epochs. The x-axis represents the number of epochs, while the y-axis represents the loss value.

Observations:

Training Loss: The blue line represents the training loss, which is the average loss calculated on the training dataset during each epoch. The training loss generally decreases as the model learns from the training data. In this case, the training loss shows a steady decline, indicating that the model is improving its performance on the training set.

Validation Loss: The orange line represents the validation loss, which is calculated on a separate validation dataset that the model hasn't seen during training. The model's generalization performance that is, its capacity to function well on unknown data is tracked using the validation

loss. As the model trains, it is ideal for the validation loss to also reduce. However, overfitting occurs when the model learns the training data too well but finds it difficult to generalize to new data, as evidenced by the validation loss beginning to rise while the training loss keeps falling.

Interpretation:

Model Convergence: The graph suggests that the model is converging, as both the training and validation loss are decreasing.

Overfitting Risk: While the overall trend is positive, there are some fluctuations in the validation loss. It's important to monitor these fluctuations to ensure that the model isn't overfitting.

Early Stopping: If the validation loss starts to increase significantly after a certain number of epochs, it might be beneficial to stop training early to prevent overfitting.

This line graph illustrates (Figure 13) the training and validation loss of a machine learning model over a series of epochs.

Key Elements:

- X-axis: Represents the number of epochs, or training iterations.
- Y-axis: Represents the loss, a measure of how well the model is predicting the correct outputs. Lower loss generally indicates better performance.
- Lines: Two lines are plotted:
- Train Loss: Shows the loss on the training data.
- Validation Loss: Shows the loss on the validation data, which is used to assess the model's generalization performance.

Interpretation:

- General Trend: Ideally, both the training and validation loss should decrease as the model learns from the data. If the training loss decreases significantly while the validation loss plateaus or increases, it might indicate overfitting.
- Gap Between Lines: A large gap between the training and validation loss suggests overfitting. This means the model is learning the training data too well but struggles to generalize to new data.

- Convergence: If both lines converge or become relatively stable, it indicates that the model has learned a good representation of the data and is likely to perform well on unseen data.

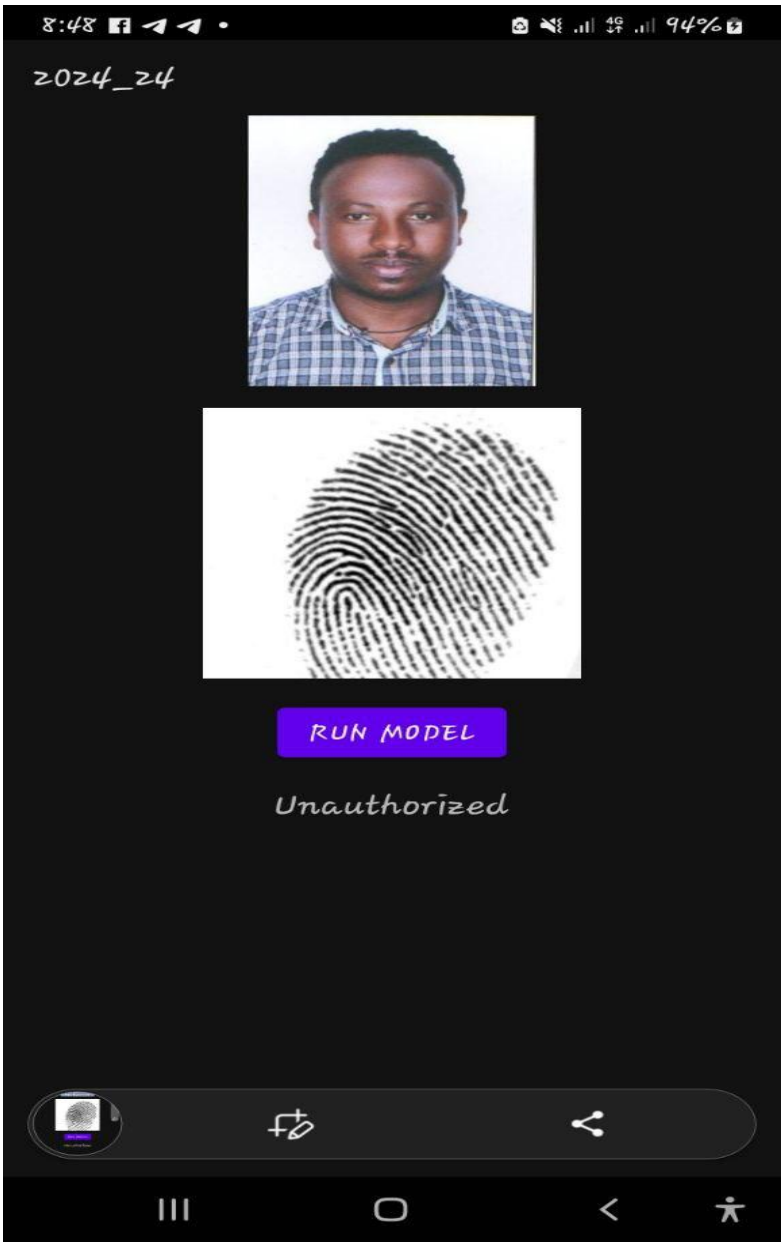


Figure 17: Biometric Authentication Interface for Unauthorized User

The experiment shown in Figure 17 is, testing biometric authentication system using face and fingerprint biometric modalities. The system attempts to identify whether the user has a grant to access IoT devices. The “Run Model” triggers the lightweight deep learning which was trained on

both fingerprint and face images categorized into “Authorized” and “Unauthorized” groups. Then the model performs prediction to classify the input data in to the two groups. After attempt to run the model, the result displayed as “Unauthorized” meaning that the input biometric data (face and fingerprint) did not match with the record in “Authorized” class. The result suggests that the person try to authenticate is not allowed to access the IoT device. This is model capability that differentiate legitimate and unauthorized users. The proposed system run on limited computational resources, ensure that both speed and accuracy are optimized for real time authentication. The proposed solution classifies the users on resource constraint IoT devices that reinforcing the practicality of using lightweight deep learning-driven biometrics.

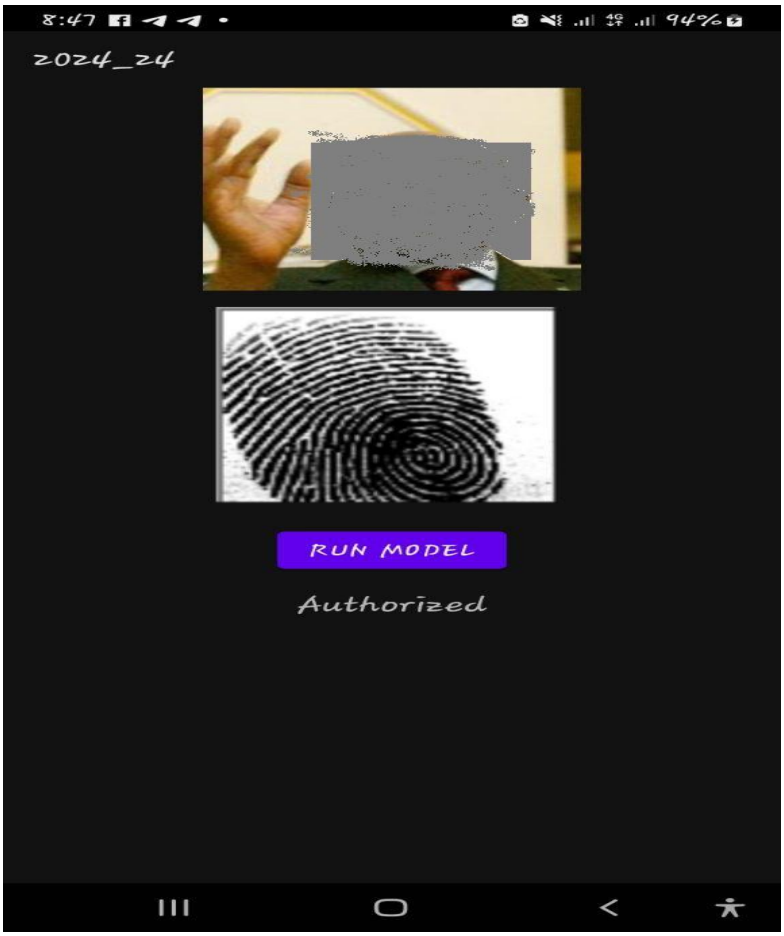


Figure 18: Biometric Authentication Interface for Authorized User

Figure 18 shows that another output of the authentication system of the proposed solution, in which the system classify the user as “Authorized”. The “Run Model” triggers the lightweight deep learning which was trained on both fingerprint and face images categorized into “Authorized” and

“Unauthorized” groups. Then the model performs prediction to classify the input data in to the two groups. After attempt to run the model, the result displayed as “Authorized” meaning that the input biometric data (face and fingerprint) did match with the record in “Authorized” class. The result suggests that the person try to authenticate is allowed to access the IoT device or service

CHAPTER SIX: RESULT AND DISCUSSION

6.1. Result

In this part we present our findings from the experiments conducted. First, we compare different lightweight deep learning models by conduction and experiment by using the dataset used in this research. The models are compared based on accuracy and their efficient. MobileNetV2 shows a significant decrease in both training and validation loss over epochs indicating that the model is so effective in learning and generalization than ResNet-18. In ResNet-18, while the training loss decreases the validation loss remains high and fluctuates, which indicates overfitting. When we compare MobileNetV2 and VGG16, there is a noteworthy improvement in accuracy over epochs, with both training and validation accuracy increasing substantially in MobileNetV2. While in VGG16 the training accuracy increases, the validation accuracy remains relatively low and stagnant, suggesting overfitting. MobileNetV2 consistently outperforms VGG16 in both training and validation accuracy. in MobileNetV2 there is a significant decrease in both training and validation loss over epochs, indicating effective learning and generalization. While in VGG16 the training loss decreases, the validation loss remains relatively high and fluctuates, suggesting overfitting. The conducted experiments are started with model training. Them model training task is carried out based on different parameters. We use different epochs in which training model is pass the entire training dataset through the learning algorithm. If the number of epochs is low, there is a problem of perfect learning. so, to avoid this problem we adjust the epochs parameter to gain perfect model training process and avoid overfitting and underfitting problem. Specifically, we use early_stopping concept for our model training to avoid overfitting. By using this parameter, model training overfit is prevented. Another parameter used in our conducted experiment is learning rate. This parameter tells us how quickly the model is learning feature from our dataset. We use 0.0001 learning rate value in our experiment, which is perfect for our model to learn enough features from both fingerprint and face images.

Practical experiment of lightweight deep learning driven-multimodal biometric authentication system is done in our thesis (Figure 17 and 18). For the authentication mechanism both fingerprint and face images are used. This multi-biometric approach strengthens security by leveraging the unique traits of each modality, thereby reducing prone to spoofing attacks that single-modality systems face. The deployed system to the IoT devices captures fingerprint and images, concatenate their feature and finally displaying the authentication result (“Authorized” or "Unauthorized"). In

the practical demonstration how the biometric authentication system with light weight deep learning operates in real-world scenario is observed. When the deployed system is tested with different data, especially with test data the result is displayed according to their respective class they belong to “Authorized” or "Unauthorized" this show that the model’s capability to effectively distinguish between authorized and unauthorized users.

6.2. Discussion

In regarding accuracy, MobileNetV2 achieving higher accuracy in both training and validation sets compared to ResNet-18. This indicates that MobileNetV2 is better to generalize the unseen data. In terms of training convergence, MobileNetV2 is faster and smoother, reaching higher accuracy in fewer epochs than ResNet-18. Generally, MobileNetV2 emerged as a stronger performance demonstrating superior accuracy and faster convergence compared to ResNet-18 on the dataset. The depth-wise convolution of MobileNetV2 make it more efficient and less prone to overfitting. The gap between training and validation loss in MobileNetV2 is smaller, indicating that less overfitting. The large gap between training and validation loss in ResNet-18 suggest overfitting. The model is better in training data but struggles to generalize unseen data. The gap between training and validation accuracy for MobileNetV2 is smaller, indicating less overfitting. he large gap between VGG16's training and validation accuracy suggests overfitting. The model is learning the training data too well but challenges to generalize to unseen data. The gap between training and validation loss for MobileNetV2 is smaller, indicating less overfitting. The large gap between VGG16's training and validation loss suggests overfitting. The model is learning the training data too well but struggles to generalize to unseen data. The performance of the proposed solution is a little bit quit when it is compared with the state-of-the-art methods. Using light weight deep learning, multimodal biometrics authentication system enhances the accuracy and reliability of biometric authentication in IoT devices. With high validation accuracy the proposed system effectively differentiates between authorized and unauthorized users, that solves the security concern of IoT device. By fusing multimodal biometrics data, the promising result were achieved. The use of a lightweight architecture facilitated the deployment of the model on resource-constrained IoT devices without sacrificing accuracy.

CHAPTER SEVEN: SUMMARY AND FUTURE WORK

7.1. Summary

In this work, we explored multimodal biometric authentication, combining fingerprint and face modalities, using a lightweight deep learning model. Our proposed solution addresses the critical challenge of IoT device security. Leveraging a comprehensive dataset of 17,000 images, we successfully trained a MobileNetV2-based model. This model achieved a training accuracy of 99.3% and a validation accuracy of 82.5%, demonstrating its ability to distinguish between authorized and unauthorized classes. The experimental results highlight the potential of integrating a lightweight deep learning model with multimodal biometrics as a promising solution for enhancing IoT device security.

A key aspect of our investigation was the exploration of feature-level fusion through concatenation. We concatenated the feature vectors extracted from fingerprint and face images using MobileNetV2. This approach allowed the model to learn relationships between the two modalities, contributing to robust identity verification. In addition to concatenation, we also experimented with other fusion techniques, including PCA-based fusion, deep learning fusion, and decision-level fusion methods such as majority voting, weighted sum rule, and SVM. Our comparative analysis demonstrated the effectiveness of concatenation as a strong baseline, while also revealing the limitations of PCA in this specific context and the potential of deep learning with further optimization. We further created a lightweight version of the MobileNetV2 model through techniques like quantization and filter reduction, achieving a substantial reduction in model size (from 53.88 MB to 4.90 MB) and inference time (from 3878.13 ms to 1561.52 ms), with a minor trade-off in accuracy (from 0.912 to 0.890). This lightweight model is particularly well-suited for deployment on resource-constrained IoT devices, addressing the limitations of computational power and memory.

Analysis of the confusion matrix on the test dataset provided further insights into the model's performance. For the "Unauthorized" class, the model correctly identified 799 out of 846 instances, with 47 false positives. For the "Authorized" class, the model correctly classified 811 out of 846 instances, with 35 false negatives. These results demonstrate the model's ability to effectively distinguish between authorized and unauthorized individuals, with a low rate of misclassifications. The high number of true positives and true negatives, coupled with the low number of false

positives and false negatives, confirms the model's efficacy in the context of our defined security application. The findings of this research support the feasibility and effectiveness of multimodal biometric authentication using lightweight deep learning models for securing IoT devices.

7.2. Future Work

Our work is basically focus on IoT device security using deep learning driven multimodal biometrics. While we are working on this area we face some challenges, further recognition accuracy improvement, the exploration of adversarial attacks. In the future it is better to consider to incorporate emerging biometric technologies to secure IoT devices.

REFERENCES

[1] R. A. R. A. Mouha, "Internet of Things (IoT)," *Journal of Data Analysis and Information Processing*, vol. 09, no. 02, pp. 77–101, Apr. 2021, doi: 10.4236/JDAIP.2021.92006.

[2] "IoT devices installed base worldwide 2015-2025 | Statista." Accessed: Jun. 04, 2023. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[3] "Biometrics (facts, use cases, biometric security)." Accessed: Jun. 05, 2023. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

[4] "What is Biometric Authentication? - Definition from SearchSecurity.com." Accessed: Jul. 11, 2023. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/biometric-authentication

[5] "Biometric Authentication: Literature Review." Accessed: Jul. 11, 2023. [Online]. Available: https://ukdiss.com/litreview/biometric-authentication-literature-review.php

[6] N. Subramanian, "Biometric Authentication," *Encyclopedia of Cryptography and Security*, pp. 86–90, 2011, doi: 10.1007/978-1-4419-5906-5_775.

[7] "What is Biometric Authentication? - iDenfy." Accessed: Jul. 11, 2023. [Online]. Available: https://www.idenfy.com/blog/what-is-biometric-authentication/amp/

[8] "What Is Biometric Authentication? Definition, Benefits, and Tools - Spiceworks." Accessed: Jun. 04, 2023. [Online]. Available: https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-biometric-authentication-definition-benefits-tools/

[9] "A Brief History of Deep Learning - DATAVERSITY." Accessed: Jun. 04, 2023. [Online]. Available: https://www.dataversity.net/brief-history-deep-learning/

[10] "What is Deep Learning and How Does It Work?" Accessed: Jul. 11, 2023. [Online]. Available: https://www.techtarget.com/searchenterpriseai/definition/deep-learning-deep-neural-network

[11] O. Olazabal *et al.*, "Multimodal biometrics for enhanced IoT security," *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, pp. 886–893, Mar. 2019, doi: 10.1109/CCWC.2019.8666599.

[12] "Internet of Things (IoT) Security: Challenges and Best Practices | Apriorit." Accessed: Jul. 23, 2023. [Online]. Available: https://www.apriorit.com/white-papers/513-iot-security

[13] "IoT Security: Navigating the Security Challenges & Solutions." Accessed: Jul. 23, 2023. [Online]. Available: https://www.peerbits.com/blog/biggest-iot-security-challenges.html

[14] “Top IoT security issues and challenges (2022) – Thales.” Accessed: Jul. 23, 2023. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats

[15] “IoT Security Challenges and Problems | Balbix.” Accessed: Jul. 20, 2023. [Online]. Available: https://www.balbix.com/insights/addressing-iot-security-challenges/

[16] Y. Li, Y. Yang, X. Yu, T. Yang, L. Dong, and W. Wang, “IoT-APIScanner: Detecting API Unauthorized Access Vulnerabilities of IoT Platform,” *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, vol. 2020-August, Aug. 2020, doi: 10.1109/ICCCN49398.2020.9209626.

[17] “IoT Security: Protecting Your Connected Devices - Nexusgroup.” Accessed: Jul. 20, 2023. [Online]. Available: https://www.nexusgroup.com/iot-security/

[18] “IoT Security: Risks, Examples, and Solutions | IoT Glossary.” Accessed: Jul. 20, 2023. [Online]. Available: https://www.emnify.com/iot-glossary/iot-security

[19] “Top 12 IoT security threats and risks to prioritize | TechTarget.” Accessed: Jul. 20, 2023. [Online]. Available: https://www.techtarget.com/iotagenda/tip/5-IoT-security-threats-to-prioritize

[20] “Gain Congnizance on IoT Device Security Risks & Solutions | Infosys.” Accessed: Jul. 20, 2023. [Online]. Available: https://www.infosys.com/insights/iot/security-iot.html

[21] “IoT Security: 5 cyber-attacks caused by IoT security vulnerabilities.” Accessed: Jul. 20, 2023. [Online]. Available: https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities

[22] “IoT Security and the Internet of Forgotten Things.” Accessed: Jul. 20, 2023. [Online]. Available: https://securityintelligence.com/articles/iot-security-internet-forgotten-thing/

[23] “IoT Cyberattacks Escalate in 2021, According to Kaspersky.” Accessed: Jul. 20, 2023. [Online]. Available: https://www.iotworldtoday.com/security/iot-cyberattacks-escalate-in-2021-according-to-kaspersky

[24] “Top 7 IoT Cyber Security Vulnerabilities for 2022 - Security Boulevard.” Accessed: Jul. 20, 2023. [Online]. Available: https://securityboulevard.com/2022/10/top-7-iot-cyber-security-vulnerabilities-for-2022/

[25] “5 INFAMOUS IOT HACKS AND VULNERABILITIES | IOT Solutions World Congress | MAY 21 – 23 BARCELONA.” Accessed: Jul. 20, 2023. [Online]. Available: https://www.iotsworldcongress.com/5-infamous-iot-hacks-and-vulnerabilities/

[26] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, “Biometrics for Internet-of-Things Security: A Review,” *Sensors (Basel)*, vol. 21, no. 18, Sep. 2021, doi: 10.3390/S21186163.

[27] A. Basare, D. Bhojak, and Dr. R. Solanki, “Biometric Authentication System,” *Int J Res Appl Sci Eng Technol*, vol. 11, no. 6, pp. 3232–3238, Jun. 2023, doi: 10.22214/ijraset.2023.54246.

[28] C. Lien, S. Vhaduri, T. of Biometric Authentications, and A. Comput Surv, “Challenges and Opportunities of Biometric User Authentication in the Age of IoT: A Survey,” *ACM Comput Surv*, Aug. 2022, doi: 10.1145/3603705.

[29] Z. Y. Deng, H. H. Chiang, L. W. Kang, and H. C. Li, “A lightweight deep learning model for real-time face recognition,” *IET Image Process*, vol. 17, no. 13, pp. 3869–3883, Nov. 2023, doi: 10.1049/IPR2.12903.

[30] S. Kloppenburg and I. van der Ploeg, “Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences,” *https://doi.org/10.1080/09505431.2018.1519534*, vol. 29, no. 1, pp. 57–76, Jan. 2018, doi: 10.1080/09505431.2018.1519534.

[31] S. Kloppenburg and I. van der Ploeg, “Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences,” *https://doi.org/10.1080/09505431.2018.1519534*, vol. 29, no. 1, pp. 57–76, Jan. 2018, doi: 10.1080/09505431.2018.1519534.

[32] A. K. Sahu, S. Sharma, and R. Raja, “Deep Learning-based Continuous Authentication for an IoT-enabled healthcare service,” *Computers and Electrical Engineering*, vol. 99, p. 107817, Apr. 2022, doi: 10.1016/J.COMPELECENG.2022.107817.

[33] S. Kokal, M. Vanamala, and R. Dave, “Deep Learning and Machine Learning, Better Together Than Apart: A Review on Biometrics Mobile Authentication,” *Journal of Cybersecurity and Privacy 2023, Vol. 3, Pages 227-258*, vol. 3, no. 2, pp. 227–258, Jun. 2023, doi: 10.3390/JCP3020013.

[34] “About Neurotechnology: company information and white paper.” Accessed: Jul. 19, 2023. [Online]. Available: https://www.neurotechnology.com/about.html

[35] K. Sundararajan and D. L. Woodard, “Deep Learning for Biometrics,” *ACM Computing Surveys (CSUR)*, vol. 51, no. 3, May 2018, doi: 10.1145/3190618.

[36] D. S. AbdELminaam, A. M. Almansori, M. Taha, and E. Badr, “A deep facial recognition system using computational intelligent algorithms,” *PLoS One*, vol. 15, no. 12, Dec. 2020, doi: 10.1371/JOURNAL.PONE.0242269.

[37] K. Sundararajan and D. L. Woodard, “Deep Learning for Biometrics,” *ACM Computing Surveys (CSUR)*, vol. 51, no. 3, May 2018, doi: 10.1145/3190618.

[38] M. Golec, S. S. Gill, R. Bahsoon, and O. Rana, “BioSec: A Biometric Authentication Framework for Secure and Private Communication among Edge Devices in IoT and Industry 4.0,” *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 51–56, Mar. 2022, doi: 10.1109/MCE.2020.3038040.

[39] Q. Zhang, “Deep Learning of Electrocardiography Dynamics for Biometric Human Identification in era of IoT,” *2018 9th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2018*, pp. 885–888, Nov. 2018, doi: 10.1109/UEMCON.2018.8796676.

[40] T. Suleski, M. Ahmed, W. Yang, and E. Wang, “A review of multi-factor authentication in the Internet of Healthcare Things,” *Digit Health*, vol. 9, Jan. 2023, doi: 10.1177/20552076231177144.

[41] Y. Yue, S. Li, P. Legg, and F. Li, “Deep Learning-Based Security Behaviour Analysis in IoT Environments: A Survey,” *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/8873195.

[42] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, “Biometrics for Internet-of-Things Security: A Review,” *Sensors 2021, Vol. 21, Page 6163*, vol. 21, no. 18, p. 6163, Sep. 2021, doi: 10.3390/S21186163.

[43] K. Istiaque Ahmed, M. Tahir, M. Hadi Habaebi, S. Lun Lau, and A. Ahad, “Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction,” *Sensors (Basel)*, vol. 21, no. 15, Aug. 2021, doi: 10.3390/S21155122.

[44] S. Bharati and P. Podder, “Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions”.

[45] S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, “Biometrics Recognition Using Deep Learning: A Survey,” Nov. 2019, Accessed: Jul. 19, 2023. [Online]. Available: http://arxiv.org/abs/1912.00271

[46] P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan, and K. K. R. Choo, “A lightweight machine learning-based authentication framework for smart IoT devices,” *Inf Sci (N Y)*, vol. 484, pp. 255–268, May 2019, doi: 10.1016/J.INS.2019.01.073.

[47] “What is the k-nearest neighbors algorithm? | IBM.” Accessed: Feb. 05, 2025. [Online]. Available: https://www.ibm.com/think/topics/knn

[48] “Deep Dive on KNN: Understanding and Implementing the K-Nearest Neighbors Algorithm - ML Course.” Accessed: Feb. 05, 2025. [Online]. Available: https://arize.com/blog-course/knn-algorithm-k-nearest-neighbor/

[49] O. A. Hassen, A. A. Abdulhussein, S. M. Darwish, Z. A. Othman, S. Tiun, and Y. A. Lotfy, “Towards a Secure Signature Scheme Based on Multimodal Biometric Technology: Application for IOT Blockchain Network,” *Symmetry 2020, Vol. 12, Page 1699*, vol. 12, no. 10, p. 1699, Oct. 2020, doi: 10.3390/SYM12101699.

[50] F. Cherifi, K. Amroun, and M. Omar, “Robust multimodal biometric authentication on IoT device through ear shape and arm gesture,” *Multimed Tools Appl*, vol. 80, no. 10, pp. 14807–14827, Apr. 2021, doi: 10.1007/S11042-021-10524-9/METRICS.

[51] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L.-C. Chen, “MobileNetV2: Inverted Residuals and Linear Bottlenecks,” Jan. 2018, Accessed: Oct. 25, 2024. [Online]. Available: http://arxiv.org/abs/1801.04381

[52] K. He, X. Zhang, S. Ren, and J. Sun, “Deep Residual Learning for Image Recognition.” [Online]. Available: http://image-net.org/challenges/LSVRC/2015/

[53] M. Tan and Q. V Le, “EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks”.

[54] “Sci-Hub | Multimodal biometrics: state of the art in fusion techniques. International Journal of Biometrics, 1(4), 393 | 10.1504/ijbm.2009.027303.” Accessed: Oct. 24, 2024. [Online]. Available: https://sci-hub.ru/10.1504/ijbm.2009.027303

APPENDIX A: ANDROID CODE FOR BIOMETRIC MATCHING

```
package com.example.a2024_24

import android.graphics.Bitmap

import android.graphics.BitmapFactory

import android.os.Bundle

import android.view.View

import android.widget.Button

import android.widget.ImageView

import android.widget.TextView

import androidx.appcompat.app.AppCompatActivity

import org.tensorflow.lite.Interpreter

import java.io.IOException

import java.nio.MappedByteBuffer

import java.nio.channels.FileChannel

class MainActivity : AppCompatActivity() {

    private var tflite: Interpreter? = null

    private var faceImageView: ImageView? = null

    private var fingerprintImageView: ImageView? = null

    private var resultTextView: TextView? = null

    private var runButton: Button? = null


    override fun onCreate(savedInstanceState: Bundle?) {
```

```
    super.onCreate(savedInstanceState)
    setContentView(R.layout.activity_main)
    faceImageView = findViewById<ImageView>(R.id.faceImageView)
    fingerprintImageView = findViewById<ImageView>(R.id.fingerprintImageView)
    resultTextView = findViewById<TextView>(R.id.resultTextView)
    runButton = findViewById<Button>(R.id.runButton)
    // Load the TensorFlow Lite model
    try {
        tflite = Interpreter(loadModelFile("model.tflite"))
    } catch (e: IOException) {
        e.printStackTrace()
    }
    // Set the button's click listener to trigger the match
    runButton?.setOnClickListener { performMatching() }
}
// Load the TFLite model from assets
@Throws(IOException::class)
private fun loadModelFile(modelPath: String): MappedByteBuffer {
    val inputStream = assets.openFd(modelPath).createInputStream()
    val fileChannel = inputStream.channel
    val startOffset = assets.openFd(modelPath).startOffset
    val declaredLength = assets.openFd(modelPath).declaredLength
    return fileChannel.map(FileChannel.MapMode.READ_ONLY, startOffset, declaredLength)
```

```
}
// Preprocess the image (resize and normalize)
private fun preprocessImage(bitmap: Bitmap): Array<Array<Array<FloatArray>>> {
    val resized = Bitmap.createScaledBitmap(bitmap, 224, 224, true)
    val input = Array(1) {
        Array(224) {
            Array(224) {
                FloatArray(3)
            }
        }
    }
    for (y in 0..223) {
        for (x in 0..223) {
            val pixel = resized.getPixel(x, y)
            input[0][y][x][0] = (pixel shr 16 and 0xFF) / 255.0f // Red
            input[0][y][x][1] = (pixel shr 8 and 0xFF) / 255.0f // Green
            input[0][y][x][2] = (pixel and 0xFF) / 255.0f // Blue
        }
    }
    return input
}
// Perform the matching on face and fingerprint images
private fun performMatching() {
```

```
        // Get face and fingerprint images
        val faceImage = BitmapFactory.decodeResource(
            resources,
            R.drawable.placeholder2
        ) // Replace with your actual images
        val fingerprintImage = BitmapFactory.decodeResource(
            resources,
            R.drawable.fingerprint_image
        ) // Replace with actual images
        faceImageView?.setImageBitmap(faceImage)
        fingerprintImageView?.setImageBitmap(fingerprintImage)
        // Preprocess the images
        val preprocessedFace = preprocessImage(faceImage)
        val preprocessedFingerprint = preprocessImage(fingerprintImage)
        // Prepare inputs
        val inputs = arrayOf<Any>(preprocessedFace, preprocessedFingerprint)
        // Prepare outputs as a MutableMap
        val output = Array(1) { FloatArray(1) } // Model output is a single float (Authorized: 1, Unauthorized: 0)
        val outputMap: MutableMap<Int, Any> = HashMap()
        outputMap[0] = output
        // Run inference
        tflite!!.runForMultipleInputsOutputs(inputs, outputMap)
```

```
        // Display the result
        val result = if (output[0][0] > 0.5) "Authorized" else "Unauthorized"
        resultTextView!!.text = result
    }
}
```

Appendix B: Model Training Process

```
C:\Users\HP\Desktop>python tt7.py
2024-10-04 05:58:41.182557: I tensorflow/core/util/port.cc:153] oneDNN custom operations are on. You may see slightly diffe
ating-point round-off errors from different computation orders. To turn them off, set the environment variable `TF_ENABLE_O
2024-10-04 05:58:43.666209: I tensorflow/core/util/port.cc:153] oneDNN custom operations are on. You may see slightly diffe
ating-point round-off errors from different computation orders. To turn them off, set the environment variable `TF_ENABLE_O
Authorized count: 3354, Unauthorized count: 3354
Loaded 6708 face images and 6708 fingerprint images.
C:\Users\HP\Desktop\tt7.py:76: UserWarning: `input_shape` is undefined or non-square, or `rows` is not in [96, 128, 160, 19
(224, 224) will be loaded as the default.
  face_base = MobileNetV2(weights='imagenet', include_top=False, input_tensor=face_input, name='face_mobilenet')
2024-10-04 05:59:19.173140: I tensorflow/core/platform/cpu_feature_guard.cc:210] This TensorFlow binary is optimized to use
rformance-critical operations.
To enable the following instructions: AVX2 AVX_VNNI FMA, in other operations, rebuild TensorFlow with the appropriate compi
C:\Users\HP\Desktop\tt7.py:80: UserWarning: `input_shape` is undefined or non-square, or `rows` is not in [96, 128, 160, 19
(224, 224) will be loaded as the default.
  fingerprint_base = MobileNetV2(weights='imagenet', include_top=False, input_tensor=fingerprint_input, name='fingerprint_m
Epoch 1/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 904s 5s/step - accuracy: 0.5604 - loss: 0.9535 - val_accuracy: 0.5410 - val_loss: 1.0190
Epoch 2/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 788s 5s/step - accuracy: 0.8736 - loss: 0.2994 - val_accuracy: 0.5581 - val_loss: 0.8828
Epoch 3/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 695s 4s/step - accuracy: 0.9726 - loss: 0.1039 - val_accuracy: 0.5991 - val_loss: 0.8794
Epoch 4/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 690s 4s/step - accuracy: 0.9915 - loss: 0.0425 - val_accuracy: 0.6200 - val_loss: 0.8843
Epoch 5/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 692s 4s/step - accuracy: 0.9960 - loss: 0.0248 - val_accuracy: 0.6766 - val_loss: 0.8235
Epoch 6/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 691s 4s/step - accuracy: 0.9992 - loss: 0.0137 - val_accuracy: 0.6759 - val_loss: 0.8222
Epoch 7/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 989s 6s/step - accuracy: 0.9986 - loss: 0.0119 - val_accuracy: 0.6870 - val_loss: 0.8512
Epoch 8/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 683s 4s/step - accuracy: 0.9986 - loss: 0.0101 - val_accuracy: 0.7079 - val_loss: 0.8467
Epoch 9/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 697s 4s/step - accuracy: 0.9991 - loss: 0.0088 - val_accuracy: 0.7034 - val_loss: 0.8711
Epoch 10/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 692s 4s/step - accuracy: 0.9996 - loss: 0.0049 - val_accuracy: 0.7124 - val_loss: 0.8619
Epoch 11/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 715s 4s/step - accuracy: 0.9987 - loss: 0.0085 - val_accuracy: 0.7079 - val_loss: 0.8545
Epoch 12/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 695s 4s/step - accuracy: 0.9993 - loss: 0.0048 - val_accuracy: 0.7310 - val_loss: 0.7830
```

```
168/168 ━━━━━━━━━━━━━━━━━━━━ 695s 4s/step - accuracy: 0.9993 - loss: 0.0048 - val_accuracy: 0.7310 - val_loss: 0.7830
Epoch 13/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 690s 4s/step - accuracy: 0.9960 - loss: 0.0144 - val_accuracy: 0.6624 - val_loss: 1.3750
Epoch 14/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 1356s 8s/step - accuracy: 0.8928 - loss: 0.3127 - val_accuracy: 0.6639 - val_loss: 1.4773
Epoch 15/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 698s 4s/step - accuracy: 0.9080 - loss: 0.2359 - val_accuracy: 0.6975 - val_loss: 1.2879
Epoch 16/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 716s 4s/step - accuracy: 0.9555 - loss: 0.1133 - val_accuracy: 0.7615 - val_loss: 0.9116
Epoch 17/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 692s 4s/step - accuracy: 0.9851 - loss: 0.0367 - val_accuracy: 0.7571 - val_loss: 0.9329
Epoch 18/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 692s 4s/step - accuracy: 0.9931 - loss: 0.0209 - val_accuracy: 0.7697 - val_loss: 0.9701
Epoch 19/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 699s 4s/step - accuracy: 0.9988 - loss: 0.0052 - val_accuracy: 0.7705 - val_loss: 0.9791
Epoch 20/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 692s 4s/step - accuracy: 0.9995 - loss: 0.0031 - val_accuracy: 0.8055 - val_loss: 0.7460
Epoch 21/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 699s 4s/step - accuracy: 1.0000 - loss: 8.9827e-04 - val_accuracy: 0.8197 - val_loss: 0.6748
Epoch 22/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 695s 4s/step - accuracy: 1.0000 - loss: 0.0013 - val_accuracy: 0.8219 - val_loss: 0.6622
Epoch 23/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 698s 4s/step - accuracy: 0.9994 - loss: 0.0015 - val_accuracy: 0.8182 - val_loss: 0.7274
Epoch 24/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 694s 4s/step - accuracy: 0.9986 - loss: 0.0062 - val_accuracy: 0.7921 - val_loss: 0.8347
Epoch 25/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 711s 4s/step - accuracy: 0.9910 - loss: 0.0223 - val_accuracy: 0.7571 - val_loss: 1.1242
Epoch 26/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 696s 4s/step - accuracy: 0.9721 - loss: 0.0870 - val_accuracy: 0.7422 - val_loss: 1.2244
Epoch 27/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 687s 4s/step - accuracy: 0.9626 - loss: 0.1188 - val_accuracy: 0.7846 - val_loss: 0.9189
Epoch 28/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 689s 4s/step - accuracy: 0.9802 - loss: 0.0663 - val_accuracy: 0.8063 - val_loss: 0.8351
Epoch 29/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 691s 4s/step - accuracy: 0.9875 - loss: 0.0372 - val_accuracy: 0.7906 - val_loss: 0.8788
Epoch 30/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 692s 4s/step - accuracy: 0.9940 - loss: 0.0172 - val_accuracy: 0.8219 - val_loss: 0.8476
Epoch 31/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 717s 4s/step - accuracy: 0.9951 - loss: 0.0119 - val_accuracy: 0.8227 - val_loss: 0.8838
Epoch 32/40
168/168 ━━━━━━━━━━━━━━━━━━━━ 722s 4s/step - accuracy: 0.9960 - loss: 0.0105 - val_accuracy: 0.8420 - val_loss: 0.6971
```

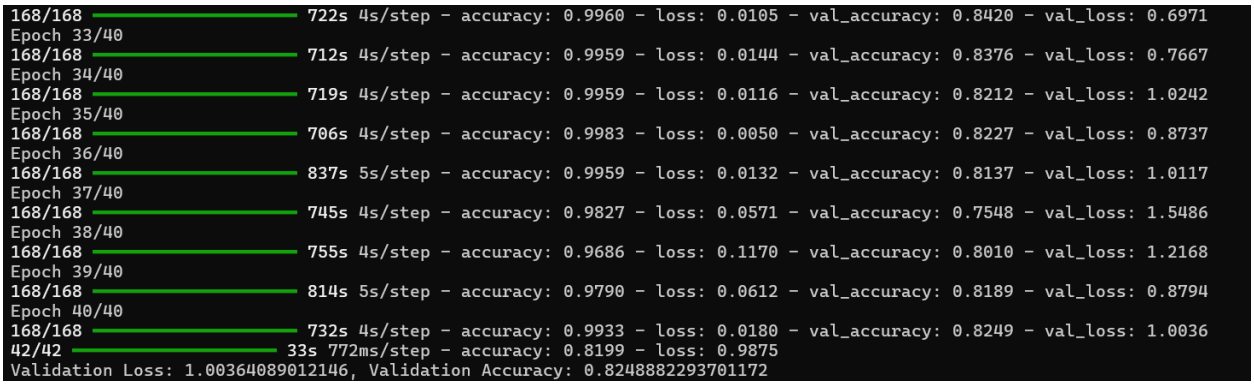


Figure 19: Multi-Modal Biometric Authentication Model Training Output