Development of Framework for Decision Making in Biometric Authentication

A THESIS

SUBMITTED TO THE DELHI TECHNOLOGICAL UNIVERSITY FOR THE AWARD OF THE DEGREE OF

DOCTOR OF PHILOSOPHY

AMITABH THAPLIYAL

(Roll No. 2K12/PHD/CO/07)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

DELHI-110042 (INDIA)

2023

Development of Framework for Decision Making in Biometric Authentication

By

AMITABH THAPLIYAL

(Roll No. 2K12/PHD/CO/07)

A thesis submitted in fulfillment of the requirement of the Degree of

Doctor of Philosophy

Prof. O.P. Verma
(Supervisor)
Department of Electronics &
Communication Engineering
Delhi Technological University

Dr. Amioy Kumar
(Co-Supervisor)
Technical Lead
Intel Corporation
Bangalore, Karnataka

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
DELHI-110042 (INDIA)

2023

DECLARATION

I hereby declare that the thesis entitled **"Development of Framework for Decision Making in Biometric Authentication"** submitted by **Amitabh Thapliyal** (**Reg. No.: 2K12/PHD/CO/07**), for the award of the degree of *Doctor of Philosophy* to Delhi Technological University is a record of bonafide work carried out under the supervision of Dr. OP Verma, Professor, Department of Electronics and Communication, Delhi Technological University, Delhi. I further declare that the work reported in the thesis has not been submitted and will not be submitted, either in part or full, for the award of any other degree or diploma in this institute or any other institute or University.

Date: ……/……/……

Place: …….

Amitabh Thapliyal
Reg. No. 2K12/PHD/CO/07
Department of Computer Science & Engineering
Delhi Technological University, Delhi
E-mail: amitabh.thapliyal@gmail.com

CERTIFICATE

This is to certify that the thesis under the title **"Development of Framework for Decision Making in Biometric Authentication"** is being submitted by **Mr. Amitabh Thapliyal** (**Reg. No.: 2K12/PHD/CO/07**) for the award of the degree of Doctor of Philosophy to Delhi Technological University is based on the original research work carried out by him. He has worked under our supervision and has fulfilled the requirements, which to our knowledge have reached the requisite standard for the submission of the thesis. This is further certified that the work embodied in this thesis has neither partially nor fully been submitted to any other university or institution for the award of any degree or diploma to the best of our knowledge.

Prof. O.P. Verma
(Supervisor)
Department of Electronics &
Communication Engineering
Delhi Technological University

Dr. Amioy Kumar
(Co-Supervisor)
Technical Lead
Intel Corporation
Bangalore, Karnataka

ACKNOWLEDGMENT

First and foremost, I would like to thank my parents Late Shri Jitendra Kumar Thapliyal and Late Smt Urmila Thapliyal for their blessings. Without their support and encouragement at crucial periods of my life, it would not have been possible for me to pursue studies and aim higher in life. Their hard work and values always inspired me. I proudly dedicate this thesis to them.

I would like to express my sincere gratitude and thanks to my research supervisor Dr. O.P Verma, Prof. Department of Electronics and Communication for his valuable guidance, motivation, and constant encouragement throughout my research work. He has always been my pillar of strength.

I am extremely thankful to my co-supervisor Dr. Amioy Kumar for his valuable comments, and suggestions that have greatly enhanced and shaped this research work.

Special thanks also go to Samsung R&D Institute India – Noida management and staff members where most of the research work was carried out. I owe a debt of gratitude to all the members of SRI-Noida for providing the facilities, equipment, and labs needed to complete this research work.

I would like to express thanks to the faculty members of the Department of Computer Science & Engineering, Delhi Technological University for their encouragement and support.

Finally, I would like to thank my wife Pooja Thapliyal, and daughters Shreyasi and Vidushi for their constant encouragement and moral support.

Date: ……/……/…… Amitabh Thapliyal

Place: ……. Reg. No. 2K12/PHD/CO/07

Department of Computer Science & Engineering

Delhi Technological University, Delhi

E-mail: amitabh.thapliyal@gmail.com

ABSTRACT

Mobile phones are widely utilized for high-security applications, such as financial transactions, where personal authentication with a high degree of accuracy and precision is needed. Therefore, biometrics-based authentication solutions are required to avoid security breaches and attacks during high-security transactions.

Nowadays, mobile phones have many biometric authentication systems like iris, fingerprint, and face recognition. However, fingerprints or facial recognition-based systems in mobile phones may not be as applicable in pandemic situations like Covid-19, where hand gloves or face masks are mandatory to protect against unwanted exposure of the body parts. The biometric research literature has shown relatively few efforts focused on providing an effective authentication system that supports the user samples impacted by external factors (like gloves, wet hands, face masks) and contextual factors (location, time, and network connection).

Therefore, this thesis focuses on investigating methods and evaluating frameworks for effective biometric authentication in mobile phones in the presence of such external and contextual factors.

In our work, we propose a multimodal biometric authentication framework for smartphones utilizing touchscreen swipe and keystroke dynamics that can handle the input biometric samples impacted by external factors (like wet hands, and gloved hands). This system uses machine learning-based classifiers to lessen the impact of hand gloves and sanitized wet hands during the authentication process. An experiment employing several classifiers yielded the best authentication accuracy of about 99 percent with 197 users on the Samsung Galaxy S20 device. In light of the COVID-19 pandemic, the proposed multimodal behavioral biometric authentication framework could be widely applicable to smartphones.

Another proposed system in our work is the use of keystroke dynamics for feature phones. We have suggested an approach to incorporate the user's typing patterns to enhance the security of the feature phone. We have applied the k-Nearest Neighbours classification with fuzzy logic and achieved an Equal Error Rate of 1.88%.

The experiments are performed with 25 users on the Samsung On7 Pro C3590 device.

Finally, methods for face recognition with masked faces are investigated as part of this research study. Through this work, we present an approach using the Haar cascade classifier for face detection with Local Binary Patterns Histograms (LBPH) face recognizer. In this proposed work for masked face recognition, an accuracy of 86% is achieved when a Haar feature based cascade classifier with LBPH face recognizer is used which further improves to 97% when used in conjunction with fuzzy logic.

TABLE OF CONTENTS

LIST OF TERMS AND ABBREVIATIONS

AAM	Active Appearance Model
ANFIS	Artificial Neuro-Fuzzy Inference System
ANN	Artificial Neural Network
ATM	Automated Teller Machine
BPNN	Back Propagation Neural Network
CNN	Convolutional Neural Network
CPU	Central Processing Unit
DNA	Deoxyribonucleic Acid
EER	Equal Error Rate
FAR	False Acceptance Rate
FMR	False Match Rate
FRR	False Rejection Rate
GAR	Genuine Acceptance Rate
GE	Gaussian Estimation
GMR	Genuine Match Rate
GPS	Global Positioning System
HTC	High Tech Computer Corporation
IOS	IPhone Operating System
KDA	Keystroke Dynamics-based Authentication
k-NN	k-Nearest Neighbor
LBPH	Local Binary Pattern Histogram
LCD	Liquid Crystal Display
LDA	Linear Discriminant Analysis
LFW	Labelled Faces in the Wild
LLE	Locally Linear Embedding
MFDD	Masked Face Detection Dataset
MLERPM	Metric Learned Extended Robust Point Matching
ML	Machine Learning
NG	Not Good
OS	Operating System

OSIRIS	Open Source Iris Recognition Software
PCA	Principal Component Analysis
PDA	Personal Digital Assistants
PIN	Personal Identification Number
PSO	Particle Swarm Optimization
RBFN	Radial Basis Function Network
RMFRD	Real-world Masked Face Recognition Dataset
RNN	Recurrent Neural Network
ROC	Receiver Operating Characteristic
ROI	Region of Interest
SD	Standard Deviation
SIFT	Scale Invariant Feature Transform
SMFRD	Simulated Masked Face Recognition Dataset
SVM	Support Vector Machine
ZS	Z-score

LIST OF FIGURES

LIST OF TABLES

PUBLICATIONS & PATENTS

Publication in Scopus/ESCI Journals:

1. Amitabh Thapliyal, Om Prakash Verma, Amioy Kumar, "Behavioral biometric based personal authentication in feature phones", *International Journal of Electrical and Computer Engineering*, ISSN: 2088-8708, Vol 12, Issue 1, February 2022.

   DOI: http://doi.org/10.11591/ijece.v12i1.pp802-815
   URL: http://ijece.iaescore.com/index.php/IJECE/article/view/25466/15431

2. Amitabh Thapliyal, Om Prakash Verma, Amioy Kumar, "Multimodal Behavioral Biometric Authentication in Smartphones for Covid-19 Pandemic", *International Journal of Electrical and Computer Engineering Systems*, ISSN: 1847-6996, Vol 13, Issue 9, 6th December 2022.

   DOI: https://doi.org/10.32985/ijeces.13.9.6
   URL:https://ijeces.ferit.hr/index.php/ijeces/issue/view/36

3. Amitabh Thapliyal, Om Prakash Verma, Amioy Kumar, "Mask Covered Face Recognition Using Haar Cascade Classifier and Fuzzy Logic", *International Journal of Emerging Technology & Advanced Engineering*, ISSN: 2250–2459, Vol 12, Issue 8,August 2022.

   DOI: https://doi.org/10.46338/ijetae0822_19
   URL: https://ijetae.com/Volume12Issue8.html

Patent Published :

1. Indian Patent Application number: 202011025242, Published Date: 17th December 2021

   Patent Title: "Method and System of Authenticating a User in an Electronic Device"

   Authors: Amitabh Thapliyal, Prof O.P. Verma, Dr. Amioy Kumar

Chapter 1: Introduction

Biometric authentication is a machine learning based technique that is used for identifying individuals based on their physiological and behavioral characteristics. These characteristics are called “biometric traits” or “biometric identifiers”. In contrast to the traditional way of identifying people, a biometric authentication system doesn’t use secret information like passwords, smartcards, or tokens to figure out who someone is. As a result, biometric authentication systems use attributes that are unique to an individual and cannot be replicated.

1.1 Functioning of Biometric Authentication System

A biometric authentication system mainly has 4 entities: the sensor that captures raw data, the features extracting unit, a unit for matching features, and the authentication system database [1]. The sensor module gets basic information from the user, either physically or behaviorally. During the user registration phase, a biometric template is created from the user's raw biometric data by the feature extractor. This template is saved in the authentication database and can be compared to the template that is generated when the user logs in.

The next component is the matching identity unit. Its purpose is to help match user entries to inputs in the database, and to validate inputs about the user's existence in the database. It acts as a decision-making module. The last component, which is the system database, is like a repository where all the biometric data related to user input is stored and used during the authentication process. During the user registration phase, the user data is scanned by sensors and stored in the database under a particular user ID or by any other method adopted for future retrieval.

Figure 1.1 illustrates the biometric authentication system's operation and depicts all three processes – (a) Enrolment, (b) Identification, and (c) Verification using the four main modules (Sensor, Feature extraction module, Matcher module, and System database module) of Biometric authentication system. In the user registration mode, new users are registered to the authentication system. Features extracted from the raw data

(Physiological or Biological) of the user are checked for quality and then added to the database of the authentication system.

The biometric authentication system has two modes of operation: verification and identification. Verification mode is a "one-to-one" comparison. The system verifies a person's identity by comparing the biometric data entered against the biometric template for that individual recorded in the system's database. The identification mode is a "one-to-many" comparison in which the system identifies an individual by comparing it to all database records. Using this mode, one can determine whether or not a particular individual is already in the database. Thus, this technique entails linking identity with a specific individual.

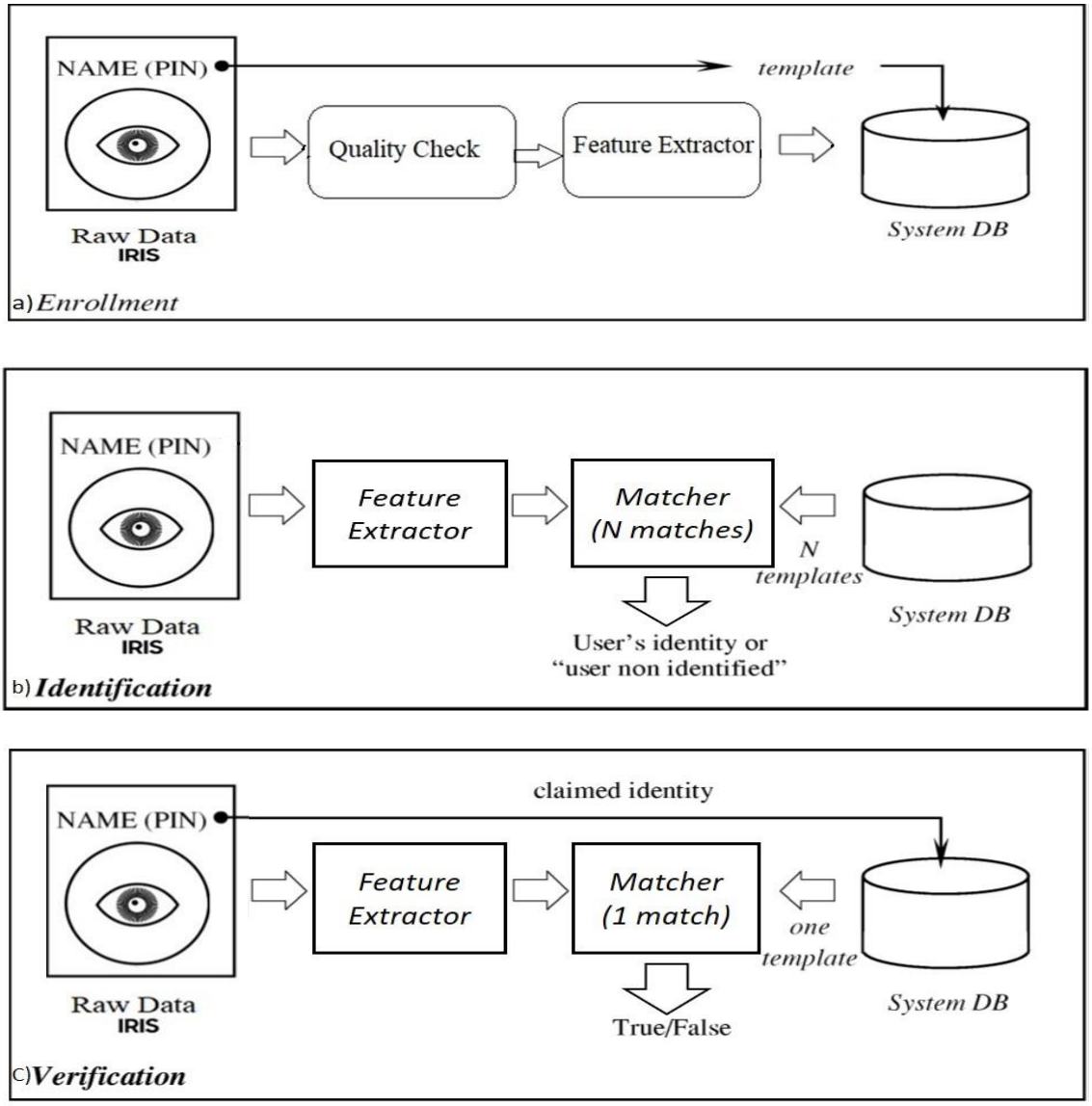

Figure 1.1: Biometric authentication system operation

1.2 Biometric Traits

Biometric authentication systems use biometric characteristics (i.e., identifiable and quantifiable biological qualities) to identify and verify individuals. There are two types of biometric traits or biometric features (or modalities): physiological and behavioral [2]. Physiological features are those associated with the biological and physical qualities of the human body which can be a fingerprint, iris, face, etc. In contrast, behavioral identifiers are those associated with a person's pattern of conduct that includes signature, keystroke, gait, touch dynamics and voice [3].

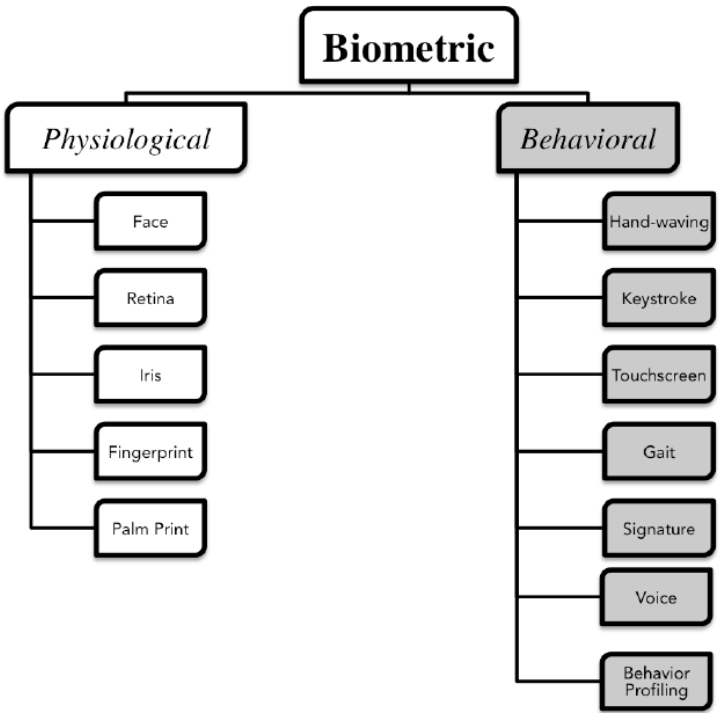

Figure 1.2: Biometric traits classification

1.2.1 Physiological Biometric Traits

(a) Fingerprint: These interlaced ridges and valleys on a fingertip determine the textural pattern. This biometric characteristic establishes uniqueness through the positions and directions of minutiae, which are small discontinuities created by abruptly broken or merged ridges [4]. The primary advantages of fingerprints as a biometrics trait are their high matching accuracy, low cost, multiple fingers, twin discrimination capability, and cost-effectiveness, making them the most widely used biometrics. As this method has many benefits, fingertip scanning for fingerprints is supported by smartphones such as

the Samsung Galaxy S9 and S9 Plus, HTC U11, Xiaomi Mix 2, Apple iPhone, Sony Xperia XZ2, and many more.

(b) Face: The placement of facial attributes, and the shape of facial features are characteristics of this biometric trait that ensure originality [4]. It can work with two-dimensional or three-dimensional images in static or moving images. It has a high level of user acceptance and reasonable accuracy, which means that facial images are probably the most frequently used biometric feature for human identification. The accuracy of this biometric feature is contingent upon controlled acquisition (background, light, etc.) and simple changes in appearance such as glasses, facial hair, emotions, and age. Face recognition systems operate best when the surrounding circumstances are correct [5]. Face recognition systems are available in smartphones such as the Samsung Galaxy S10, Huawei Y5 2019, Apple iPhone XS, Huawei Mate 20 Pro, OnePlus 6T, etc.

(c) Hand geometry: The features that make this biometric trait unique are the geometric structure of the hand, which includes the height, width, thickness, and surface area of the back of the hand and fingers. Commercial hand geometry-based verification systems capable of operating in highly hostile environments are simple to use and have a high level of user acceptance. Hand geometry information may not be invariant throughout a child's growth phase. Individuals' jewelry (e.g., rings) or dexterity impairments (e.g., arthritis) may complicate retrieving accurate hand geometry information. A hand geometry-based system is too large to fit in a smartphone or even other devices like laptops.

(d) Iris: The iris is the annular region, surrounded by the pupil and sclera (eye white) part of the eye. The complex texture pattern of the iris (i.e., the colored part of the eye: Iris Code, over 200 points) is the feature that ensures individuality. The Iris of an individual's eyesight is distinctive, and even the irises of identical twins are different. Iris-based recognition systems have high accuracy and low sensitivity to outside influences. Early iris-based recognition systems required considerable user participation and were expensive; the newer methods have become more user-friendly and cost-effective. Smartphones with built-in iris scanners include the Itel it1520, Samsung Galaxy S9 and S9+, LYF Earth 2a, and TCL 560, amongst other models.

(e) Retinal scan: The retinal scan is the distinctive pattern of blood veins in the human eye's retina. Each individual's retinal scan is unique. This biometric characteristic is challenging to obtain and requires considerable cooperation from the subject for the acquisition of the sample. Age-related eye illnesses such as cataracts can complicate the capturing process [6].

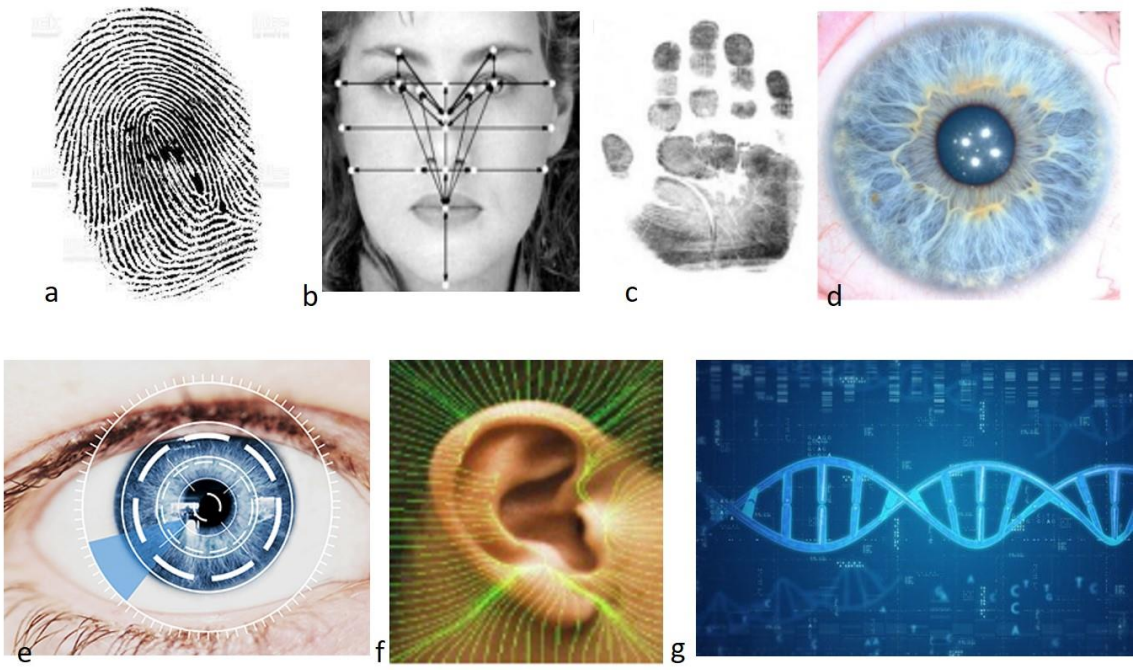

Figure 1.3: Physiological biometrics traits (a) Fingerprint (b) Face (c) Hand geometry (d) Iris (e) Retinal scan (f) Ear and (g) DNA.

(f) Ear: Ideally, the shape and structure of an individual's ear tissues make them suitable for use as a biometric for authentication purposes. It is not easy to recognize an ear covered with hair. On the other hand, the ear contains a small amount of biometric information, making it unsuitable for use with huge populations.

(g) DNA: Deoxyribonucleic acid (DNA) is the ultimate unique code for individuality. Only identical twins share the same DNA sequence. Any human body tissue can serve as a source of DNA for research. Forensic applications frequently use DNA as a biometric.

1.2.2 Behavioral Biometric Traits

Behavioral biometrics is the field of study that uniquely measures patterns of human activities and thereby identifies the user. Behavioral biometric authentication methods include Keystroke dynamics, Touch dynamics, Voice, Signatures, Gait, etc. In this

section, we introduce some of the most common behavioral biometric authentication techniques. Behavioral biometric authentication methods provide several benefits over physiological methods. Behavioral patterns can be collected continuously without user knowledge. They also usually do not require any additional hardware sensors to support them.

(a) **Keystroke dynamics recognition**: Keystroke dynamics is a behavioral biometric authentication technique that measures the time taken by an individual to type the character strings, passwords, etc. For some people, there may be considerable differences in how long it takes to type the password, how long it takes to hit each key, and how hard (pressure) the key is pressed [6]. These characteristics identify each user uniquely to the system like Mobile phones, personal computers, and so on.

(b) **Gait**: Gait is a term that relates to how an individual walks. Gait does not contain a high amount of biometric data. A person's gait may change as their body weight changes or as they get older.

(c) **Voice**: The voice is a biometric trait that is a combination of physiological and behavioral characteristics. The shape and size of the appendages involved in sound synthesis (e.g., vocal tracts, mouth, nasal cavities, and lips) determine the characteristics of an individual's voice. Additionally, voice is not particularly distinctive and may not be suitable for large-scale identification. A problem of voice-based recognition is that speech features are very susceptible to various circumstances, including background noise. While speaker recognition is most useful in phone-based applications, microphones and communication channels diminish the quality of the sound signal.

(d) **Signature recognition**: This method uses behavioral characteristics associated with the act of signing one’s name. This system dynamically captures data, such as the direction, speed, pressure, and form of the signature, as well as the signature itself. Long term reliability, expense, and lack of accuracy are the primary concerns this technology must overcome.

Figure 1.4: Behavioral biometrics traits (a) Keystroke dynamics recognition, (b) Gait, (c) Voice (d) Signature recognition.

1.3 Performance Parameters of Biometric Authentication System

Biometric authentication systems identify two types of users: "**genuine**" or "**imposter**". A biometric authentication system determines whether a user is authentic or a forger. In the case of each of these two decisions, there are two conceivable outcomes: the decision is either true or false. The acquisition of biometric characteristics is affected by factors (such as sensor imperfections acquisition environment conditions, and the way users interact with the sensor) in that case the two samples originating from the same user's biometric subject are generally not similar which can result in errors.

The performance of a biometric authentication system is generally measured by the below mentioned error rates:

1. False Acceptance Rate (FAR): FAR is a metric that indicates how often the system identifies an imposter individual as a genuine user.

$$FAR = percentage(\%)\ of\ imposter\ score > chosen\ decision\ threshold$$

2. False rejection rate (FRR): FRR is a metric that indicates the proportion of genuine users that are identified as imposters or not accepted by the system.

$$FRR = percentage(\%)\ of\ genuine\ score < chosen\ decision\ threshold$$

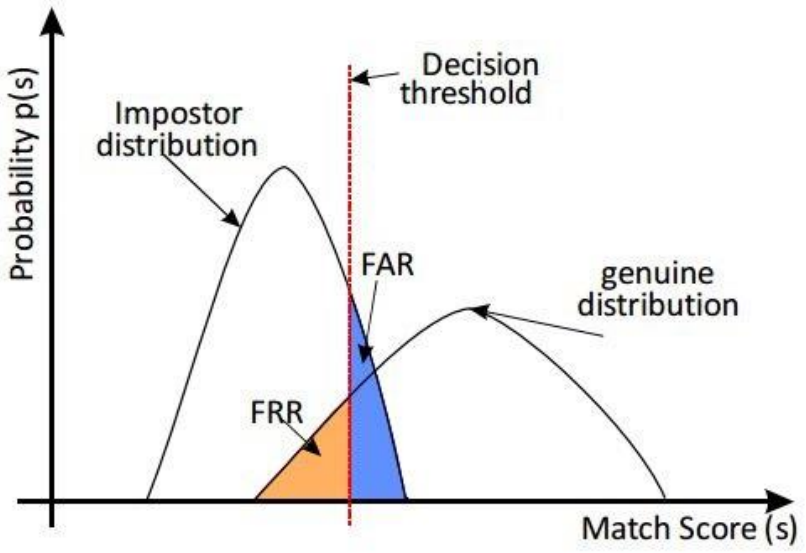

Figure 1.5: FAR and FRR rates are defined by genuine and imposter distributions

3. Genuine Acceptance Rate (GAR): The GAR is a metric that indicates how precisely the system determines a subject to be genuine.

$$GAR = percentage(\%)\ of\ genuine\ score > chosen\ decision\ threshold$$

4. Equal Error Rate (EER): EER is the most critical metric for evaluating a recognition system's performance. It ensures an equal number of false acceptance and rejection errors. In the biometrics literature, it is customary to compare the efficiency of proposed matching algorithms using this indicator. The efficiency of

the algorithm improves as the EER decreases. The EER value is the point at which FAR and FRR values equalize.

1.4 Biometric Authentication System in Smartphones

Last decade has seen many evolutions in smartphones with touch displays, bigger screens, large memory, and processors with high capability. The most powerful and advanced systems for smartphones in this decade are Android and iOS, developed by Google and Apple, respectively. In the report released from statcounter between June 2021 to June 2022, the mobile smartphone operating system market share worldwide from these smartphone platforms was 99% with Android (72%) and IOS (27%) [7]. As per the report from counterpoint research, there were 1.43 billion smartphones sold in the year 2018. According to a report from Strategy Analytics, major players such as Samsung which sold 291.3 million smartphone units, and Apple sold 215 million smartphones worldwide.

Smartphones have a huge impact on people's daily lives and are not limited to calls and messaging. Its utility has increased manifold with the availability of a huge number of diverse applications available for the user, including social networking, entertainment, shopping, and financial transactions. Smartphones today store and process a large amount of private and financial data, which can cause serious loss when it falls into the wrong hands. Therefore, a strong user authentication system is a critical requirement in smartphones.

Traditional authentication approaches in smartphones, such as PIN, password, and pattern, are prone to various attacks including shoulder surfing, guessing attacks, brute force attacks, and dictionary attacks [8][9]. Biometrics such as the face, fingerprints, voice, and iris are some of the authentication solutions that are the recent trends in Smartphones. It utilizes a physiological characteristic of the user that needs to be presented at the time of authentication; hence, it cannot be guessed or attacked through brute force and eliminates the possibility of shoulder surfing. However, face recognition also has several limitations, such as low light accuracy, spoofing attacks using photographs, and user inconveniences [10]. The adoption of behavioral biometrics-based systems for user authentication is possible from keystrokes, touches, and tapping patterns on a mobile device. Behavioral biometric methods have various advantages over physiological biometric methods, including the ability to gather behavioral patterns

continuously and without user knowledge; they also do not require any additional hardware sensors, which gives them an advantage.

1.5 Fuzzy Logic in Biometric Authentication Systems

Fuzzy logic is used in cases where an absolute measurement cannot be provided for a quantity [11]. This enables the modeling of ambiguous data. For example, a temperature that is 0.3 units warm and 0.7 units cold can be equated to the imprecise term "fairly cold."

In biometrics, fuzzy logic can be used to deal with the quality of samples that are affected by external factors (for instance, low-light conditions while taking pictures), and noise in the input sample collected (for instance, fingerprint samples impacted by dust, cuts, etc). It can also be applied in a multi-modal biometric system to do fusion of decisions made in individual biometric modes, thus improving the decision-making capabilities of the system [12].

Behavioral biometrics, by their very nature, are subject to variations. One of the primary sources of the variations is the inexactness of human behavior itself. Other sources of variation could be external and environmental factors. For example, the user's hand could be affected by sanitizer, dust, oil or grease, different kinds of gloves, and so on. This can add variations to the input presented by the user during the authentication phase resulting in high false-negative cases. In such scenarios, the conventional machine learning based classifiers may not be decisive and fail to handle the test input because their network is not trained for all variable factors. To handle such a situation, we can train a fuzzy classifier to minimize the effect of variable factors on authentication accuracy.

Another example is masked face recognition. Generalized training for masked faces isn't feasible because there is a very high degree of variability in the masks themselves as well as their ways of wearing them. Such variable factors reduce the accuracy of face recognition. This leads to the occurrence of high false negatives.

1.6 Challenges in Biometrics

Apart from their simplicity and integration capabilities, the fundamental advantage of passwords and tokens over biometrics is their cancellability. Biometric characteristics

can't be revised, unlike passwords and tokens, because they can’t be removed from the owner and replaced by other traits.

Unimodal biometric authentication systems are those that use a single biometric modality to identify an individual. A lack of invariant representation, circumvention, and universality are common problems with biometric authentication systems because there isn't much information in the samples used for biometrics [13]. When more than one biometric trait or sensor is used to obtain biometric data, and the system makes the decision by combining the information from more than one source [14], it is referred to as a multimodal biometric authentication system.

Fingerprints or facial recognition-based systems may not be available due to the use of hand gloves or face masks, particularly in healthcare environments and COVID-19 pandemic situations. Facial recognition based authentication is also prone to spoofing with images and photographs, and reduced accuracy in low light. Fingerprints are known to fade away in the working population that uses the palms, especially if they do heavy work. Fingerprint authentication also fails with wet, wrinkled fingers.

Like all authentication techniques, biometrics also suffers from the problem of specificity-sensitivity tension. Authentication requires high sensitivity, but it comes at the cost of reduced specificity, making it prone to focused attacks. Because of these reasons, there is always a need for multimodal biometrics. Multimodal biometrics means that multiple biometric features are used to improve the overall sensitivity and specificity of the authentication system.

When compared to unimodal biometric approaches, multimodal biometric methods provide superior performance in terms of accuracy, dependability, and success rate. Most of the available work explores a single-modal biometric approach for user authentication in smartphones. Multimodal systems are mostly not considered because of the complexity of the fusion of two different biometric traits in real-time in smartphones.

Over the last few years, the use of biometric-enabled mobile devices has gone up many times [15]. However, there are different kinds of problems that arise when you use mobile devices (smartphones, tablets, and pads) that have biometric security during pandemics like COVID-19 [16][17][18] when an individual has to cover their face with a mask[19] and use hand gloves in public places to protect against the virus. In such situations, the

use of traditional biometrics (like face recognition, and fingerprint) in smartphones becomes difficult.

1.7 Research Objectives

The basic aim of this research work is to provide a biometric authentication system for mobile phones while the input samples are impacted by external factors (like – hands with gloves, face masks, and sanitized hands). The goals of this work are as follows:

1. To propose a biometric authentication framework that can authenticate the users, while the input samples are impacted by external factors (like hands with gloves, and wet hands) and contextual factors (like user location and connected network provider).

2. To propose a multimodal behavioral biometric authentication system useful during the COVID-19 pandemic situation while the user input samples are impacted by external factors like water, sanitizer, and hand gloves. It's difficult for a legitimate user to authenticate using conventional biometric authentication methods like fingerprint recognition with a high rate of success during the COVID-19 pandemic situation while their hands are either covered with gloves or wet due to frequent sanitization.

3. To study the various behavioral biometric-based techniques and propose a method for recognizing mobile phone users on basis of their keystroke typing patterns using machine learning and fuzzy logic classifier.

4. To propose and investigate a method to recognize faces covered with a mask.

1.8 Thesis Organization

The thesis chapters are structured as follows:

Chapter 2 aims to provide a comprehensive insight into the literature review in the field of study. Literature studies related to biometrics in smartphones, behavioral biometrics, external factors affecting smartphone authentication, and research motivation are discussed.

Chapter 3 introduces the framework of a multimodal biometric authentication system, which can handle the input biometric samples that are impacted by external and contextual factors.

Chapter 4 presents an innovative multimodal behavioral biometric authentication system. The HandGlove mode is proposed for Smartphones considering the COVID-19 pandemic situation when the user input samples are impacted by external factors like Water, sanitizer, and surgical gloves, and it's difficult for a legitimate user to authenticate using conventional biometric authentication methods like face and fingerprint recognition. The design and implementation of a multimodal behavioral biometric authentication system based on keystrokes and touch swipes are discussed in this chapter.

Chapter 5 examines the application of keystroke dynamics on feature phones as a biometric framework that is both efficient and adaptable. In our research, we proposed a method for incorporating the user's typing patterns into the feature phone's security. A method based on k-NN with Fuzzy logic is applied to improve accuracy.

Chapter 6 gives an approach for face mask recognition systems based on the HAAR cascade and LBPH classifier. The design and implementation of the system are presented here.

Chapter 7 concludes the thesis. The effectiveness of a new biometric authentication framework for smartphones is talked about, and its use during a COVID-19 like pandemic is also explained and talked about. The performance of face mask recognition and how it could be used in the future are talked about. Keystroke-dynamics-based authentication for mobile phones is shown to be important.

Chapter 2: Literature Review

In this chapter, we study the published literature focusing on biometric authentication systems for mobile phones. Many problems arise during authentication with conventional biometric authentication systems during the COVID-19 pandemic. For instance, fingerprint inputs are impacted by sanitizers or hands covered with gloves, as well as facial recognition is impacted by faces covered with the mask. It can result in high error rates and difficult for a legitimate user to authenticate. Therefore, to improve the accuracy of biometric authentication systems while input samples are impacted by such external factors (gloved hands, face masks, sanitized hands) we have proposed and investigated a novel biometric authentication framework.

2.1 Biometric Authentication System in Smartphones

The global smartphone penetration rate reached 6 billion subscribers in 2022, according to Statista [20]. Another statistic [21] revealed that smartphone users are increasing exponentially. By the end of 2022, the number of global smartphone users is forecasted to reach 6.5 billion, an annual growth rate of 10.8 percent in Q2, 2021. Moreover, smartphone users have risen by 73.9 percent since 2016. Between 2016 and 2021, the overall number of global smartphone users climbed by an average of 11.84 percent per year, with 2017 experiencing the most significant growth. The number of smartphone users surged by 20.91 percent that year. This upward trend is projected to continue in the following years. As a result, smartphones are becoming increasingly popular as a necessary tool for accessing business and sensitive personal information. This has created a critical worldwide need for proper identification and authentication systems in smartphones [22][23]. Many researchers have attempted to provide innovative biometric authentication system in smartphones over the last decade. Mohamed Amine Ferrag *et al.* [24] discussed about the threat models, countermeasures of these threats and authentication schemes for mobile devices. Also, several smartphone manufacturing companies like Samsung and Apple have come out with commercial smartphone products with built-in biometric authentication systems like fingerprint [25], IRIS, and face recognition to provide a higher level of security.

2.1.1 Physiological Biometric Authentication System

Fingerprints, faces, iris, hand geometry, retina recognition, and other physical characteristics that differ from person to person are examples of physiological traits [26][27]. Multiple smartphone manufacturing companies have played their roles in incorporating biometrics into smartphones. OMRON Corporation, a global leader in automation, sensing, and control technology, introduced the "OKAO Vision Facial Recognition Sensor" (Figure 2.1). A camera-equipped PDA, smartphone, or other mobile devices can use this face recognition technology for the first time. Mobile devices and their data are expected to become more secure and safe due to face recognition's ability to identify and authenticate a user's identification [28].

Figure 2.1: OKAO by Omron

In a similar development, face-unlocking technology first appeared in Android 4 in 2011. At the time, it appeared to be a revolutionary feature. Unfortunately, it was a mediocre feature that did not have much security. It could be readily unlocked by using a photo of the person. When you register your face with an Android based smartphone, the device will take a 2D photo of your face and store it [29]. However, technology has progressed significantly since that time.

Figure 2.2: First Face unlock Android phone

Apple introduced Face-ID using face recognition on the iPhone X for the first time in 2017. The popularity of face-ID has led to various other Android-based smartphones introducing face recognition for user access. However, face recognition also has several limitations, such as low light accuracy, spoofing attacks using photographs, and user inconveniences [30].

In Japan, Fujitsu's Arrows NX F-04G smartphone was released, making it the first in the world to include built-in iris-scanning technology. The iris-scanning functionality, dubbed Iris Passport, was the prominent distinguishing feature. After completing the initial registration, the smartphone could be unlocked in half a second using an iris scan. Iris recognition could also substitute a password in any device's applications [31].

Figure 2.3: Fujitsu's Arrows NX F-04G smartphone

The Aadhaar biometric device using iris recognition technology was included with Samsung's Galaxy Tab Iris which was launched in 2016. The Galaxy Tab Iris's simple-to-use biometric technology was developed to support India's Digital India project [32], aiming to use technology to ensure that everyone has access to financial inclusion benefits. When applied in a secure device, the most recent iris recognition technology will give an integrated solution that will help minimize the challenges of using separate biometric identification devices.

Figure 2.4: Samsung Iris Scanner [32]

Among biometric identification technologies, fingerprint sensors are the most common. Pantech's GI100 was the world's 1st fingerprint phone when it was launched in 2004. Toshiba was the company that made fingerprint scanner phones popular. The Toshiba G500 and G900 were released and incorporated fingerprint scanners. HTC soon followed suit, releasing the HTC P6500 just a few months later. As the world's first fingerprint-sensing mobile phone, Toshiba launched the G500 and G900 in 2007 [33].

Figure 2.5: (a) Pantech GI100: The World's 1st Fingerprint Scanner Phone; (b) Toshiba G500

Users of the most recent smartphones can unlock their devices using various biometric verification techniques, including facial recognition, fingerprint scanning, and iris recognition, which shows how far mobile phone technology has progressed. Ashraf El-Sisi [34] designed a software application in Matlab and C# to implement algorithms for enhancement, minutiae extraction and matching processing that will be used as a method of identifying matching fingerprints, they used Gabor Filter for image enhancement. The method of authentication is constantly improving, with more powerful sensors and algorithms reducing false acceptance rates (FAR) and limiting hacker attacks.

Face Recognition is a technique of biometric authentication of an individual based on the visual pattern of their face. Today's world necessitates modern security measures like facial recognition that can be used for several purposes, particularly in presence of a face mask. For this, Hariri [35] proposed a quantization-based deep learning method called "Bof" paradigm in association with the Multilayer Perceptron (MLP) classifier. This proposed technique was responsible for improvising the quickness and accuracy of the rapid technological methods to use the same in applications like online surveillance, video retrieval, etc. A similar technique called MAFA was proposed by Shiming Ge *et al.* [36] combined with CNN as well as a locally linear embedding (abbreviated as LLE) algorithm. This technique was systematically implemented using a mix of classification and regression tasks, which made it possible to discover and fine-tune potential areas of the face. With the first automated system based on a feature vector of a person's face, Kanade [37] made further breakthroughs in 1977.

Sirovich *et al.* [38] developed principal component analysis (PCA) with feature extraction in 1983. The next technical advancement came in 1991 in Eigenfaces [39]. Local binary pattern analysis (LBPH) was developed in 1994 for texture recognition and was subsequently revised for facial recognition by adding histograms [40][41]. In [42], Kwak and Pedrycz proposed an extension to the Fisherface approach developed by combining Linear Discriminant Analysis (LDA) along with fuzzy integral as well as wavelet decomposition. It was able to recognize faces in a variety of lighting conditions, something that the eigenface method [43] could not do. Even to the present day, this domain has been continuously evolving, with new technologies ranging from artificial neural networks [44], PCA [45], and SVM [46] being added over the last four decades. There have been numerous algorithms and works in this context, such as Ibrahim [47]. Suchitra *et al.* in their work used fuzzy logic [48] to improve face recognition results. People with different expressions are also detected, proving that with the help of the right features extracted. Face detection was done using the YCbCr color model by Yang *et al.*, and features were extracted by the method of AAM (Active Appearance Model), resulting in an accurate recognition rate of 90–95 percent, which was further enhanced through the Artificial Neuro-Fuzzy Inference System (ANFIS), resulting in the rate of recognition with 100 percent that is incompatible with some other techniques [49]. A combined feature search for face detection and a DCT-based hybrid approach was proposed by Henckaerts [50], which was implemented on FPGA and tested with the Yale database, giving a reasonable recognition rate of 96.3.

Renliang Weng *et al.* [51] worked on a partial face recognition system by robust feature set matching, they used local feature and these local feature point sets were matched by our Metric Learned Extended Robust Point Matching (MLERPM) approach. Dong Yi *et al.* [52] worked on a semi-automatic way to collect face images from Internet and builds a large scale dataset that containing 10,000 subjects and 500,000 images, they named this dataset to CASIAWebFace. They used 11-layer CNN to learn discriminative representation and obtain state-of-the art accuracy on Labeled Faces in the Wild (LFW) and YouTube Faces (YTF).

Raghavendra *et al.* use a light field camera to examine visible light iris recognition [53] as well as smartphones and tablets [54], with encouraging findings. Using an improved OSIRIS segmentation and a feature extraction approach that incorporates deep sparse

filtering, an EER (Equal Error Rate) of less than 2 percent can be attained. Raja, Raghavendra, and Busch also investigated K-means clustering as a potential recognition strategy for visible light images, with the best EER of 0.31 percent [55]. There is a 90 percent GMR (Genuine Match Rate), and 0.1 percent FMR (False Match Rate) for the innovative configuration for obtaining iris photographs in white LED light when using the Daugman method on the Nokia Lumia 1020 device [56]. Previous studies in visible-light iris recognition by Trokielewicz *et al.* [57] are discussed. With iris photos obtained using a smartphone camera, EERs of less than 8% were achieved for two commercial iris recognition algorithms. Rattani and Derakhshani [58] proposed leveraging the mobile face biometric features to provide security for mobile devices.

Traditional minutiae matching for fingerprint verification in smartphones was replaced with the SIFT (Scale Invariant Feature Transform) method by Yamazaki *et al.* [59]. Vincenzo Conti *et al.* [60] experimented with three algorithms for fingerprint authentication that is tested on LG Nexus 5. A deep analysis provided to evaluate the user reactions towards the delay time for acquisition, processing and verification of biometric authentication. Shaveta Dargan *et al.* [61] did a deep survey on unimodal and multimodal biometric systems and analyzes the feature extraction techniques, classifiers, datasets, results, efficiency and reliability of the system. An open source face recognition system named XFace [62] for Android Operating System for face detection and ROI (Region of Interest) preprocessing achieved the accuracy of 93.8% with Eignefaces and 96.0% with FisherFaces.

Several researchers have also studied multimodal biometric identification systems for smartphones. For authentication, Raja *et al.* [63] applied to face, iris, and periocular identification methods. They evaluated their system using a database of 78 people and appeared with an EER of 0.68 percent. But they adopted an RGB camera for iris imaging, which was constrained by the reflections in lighting settings. Rahman *et al.* [64] proposed a four-way multimodal framework that integrates linguistic and behavioral profiling, as well as dynamic keystroke features, in addition to other features.

Swati K. Choudhary *et al.* [65] provides a detail review on biometric authentication system with a lot complexities, Multimodal biometric systems are considered for their reliability and result oriented performance as compare to unimodal biometric system.

2.1.2 Behavioral Biometric Authentication System

A biometric authentication method that is relied on a user's classifiable behavior [66] is known as behavioral biometric authentication. Researchers have attempted to understand and learn user behavior patterns and how they interact with systems, such as keystrokes, touches, and tapping patterns on the device. These behavioral biometric methods provide several benefits over physiological methods, such as behavioral patterns that can be collected continuously and without user knowledge; they do not require any additional hardware sensors to support them.

- **Keystroke Dynamics:**

Biometric authentication using keystroke typing patterns is built on the idea that each user's pattern of typing is distinct and constant. Keystroke biometrics has been used to authenticate a variety of devices. Applying keystroke dynamics on mobile devices, Clarke and Furnell [67] investigated the application of user authentication. Their research differentiated users based on their key-typing patterns for 11-digit telephone numbers and 4-digit security PINs. EERs varied from 9 percent to 16 percent in their models, which were built using generalized regression networks. When using "Arthematic rhythms with cues," Campisi, Patrizio, *et al.* [68] obtained an EER of 13 percent in their research "User authentication using keystroke dynamics for cellular phones". Zheng *et al.* [69] extracted data from smartphone sensors by combining 4 features: pressure, size, acceleration, and time. According to experimental tests, their verification method attains precision with an average equal error rate of 3.65 percent. When arthematic rhythms with cues were used, Hwang, Cho, and Park [70] attained an EER of 13 percent. They classified users based on their key input 4-digit password. As part of their training process, their models include a mechanism that only implements valid user patterns. They had 25 users engage in their study, and they only collected 5 patterns from each user for registration. According to Motwani, Jain, and Sondhi [71], the database used in their study was continuously developed, and the impostors weren't engaged during the registration phase of the study. With only 27 features, the FRR (false rejection rate) was 3.2 percent. Sensor-assisted keystroke dynamic was studied by Stanciu *et al.* [72]. During their investigation, they used a variety of accelerometers, gyroscopes, and movement sensors. In their investigation, 20 people actively participated, and the researchers collected keystroke and sensor data from the Samsung Nexus S phone in a properly controlled environment.

According to their findings, basic keyboard authentication is susceptible to attack, but they achieved superior outcomes against statistical attacks when sensors are used. Huang *et al.* [73] attained an EER of 7.5 percent for Android-based smartphones. They built their model using statistical classification methods. They created an Android application to gather keystroke data on the client side and a database and authentication engine as a web service to gather information on the server side. Their experiments comprised 40 people ages ranging from 22 to 55 years.

Sowndarya Krishnamurty *et al.* [74] discussed about the behavioral access on keystroke dynamics that captures the user's behavioral biometric and applied machine learning to classify them. They also applied minimum redundancy maximum relevance (mRMR) feature selection to increase the classification performance metrics. A freely typed text-based Keystroke dynamics-based authentication (KDA) [75] method for mobile devices based on free text, accelerator, coordinate, and time which yields an error rate of <1% with only one reference keystroke set. Nataasha Raul *et al.* [76] had reviewed the keystroke dynamics methods and concluded that there is a need to strengthen the keystroke dynamics dataset which has all essential features. Also an efficient algorithm is required to obtain high accuracy to make authentication effective, as the performance of biometric keystroke authentication is still an open research.

Teh *et al.* [77] conducted a study in which they gathered information from 150 subjects and divided it into 3 packages of fifty each. Subjects are required to enter the same string ten times, resulting in the collection of 20 samples from each individual. During the subject interaction, time data and finger touch size attributes were recorded. The probability of a test sample was calculated using 3 matching functions. Standard deviation (SD), Gaussian estimation (GE), and Z-score (ZS) drift are the 3 functions. FAR and FRR are used to determine biometric authentication system reliability. EER values of 8.55 percent for a 4-digit input string and 5.49 percent for a 16-digit input string are obtained using the Gaussian estimator (GE). Tse and Hung [78] examined their method and developed a dataset of 31 subjects, each of whom was required to enter a password fifty times. The dataset contained temporal characteristics, spatial dynamics characteristics, and swiping attributes. They implemented and trained three distinct RNNs using the RNN approach. The final findings were obtained by combining the results of each model. The results reveal that late fusion produces better outcomes than early fusion, with spatial

characteristics achieving the best result of 83.91 percent. Zahid *et al.* [79] discovered that mobile phone users used dynamic keystrokes in 2009. On the front end, they applied fuzzy classifier particle swarm optimization. On the back end, they created a genetic algorithm that distinguished 3 different user identifying characteristics. The frequency with which the backspace key is released determines the error rate. Also, five classifiers are used to train these features: Radial Basis Function Network (RBFN), Back Propagation Neural Network (BPNN), Kstar, Naive Bayes, and J48. This study aims to determine the user's authority to access a bank account based on the PIN (Personal Identification Number) the user enters. Jatin Yadav *et al.* [80] implemented a keystroke dynamics based authentication system using fuzzy logic and discussed how it is beneficial as compared to other approaches implemented earlier, and how a continuous learning model improves accuracy over time. Yu Zhong *et al.* [81] proposed a distance metric that helps to decouple the correlated data, normalize the feature variations and suppress the outliers for keystroke dynamics data and provides the superior results as compare to traditional methods.

- **Touch Dynamics**

Frank *et al.* [82] have used the union of four features that is pressure, acceleration, time, and size pulled out from smartphone sensors. Experiments show that their verification process has an accuracy rate of 3.65 percent on average. To train different classifiers, including neural networks, Meng *et al.* [83] used touch behavioral patterns from touch gesture data obtained from 20 Android phone users. They also used Particle Swarm Optimization (PSO) to develop the neural network and reached an EER of 2.92 percent in their research. Elakkiya Ellavarason *et al.* [84] provides a data collection framework for touch-based behavioral biometric modalities like swipe, keystroke and signature and designed an android application "Touchlogger" that captures touch actions of the user on the mobile device. Meng *et al.* [85] worked on touch-dynamics-based authentication system that composed with 8 touch gesture features to authenticate a user on phone with average error rate of 2.46% with 50 users.

Inoue and Ogawa [86] studied the Android draw-and-lock pattern to investigate user identification through touch screen biometrics. Users were categorized by Angulo *et al.* depending on how much time they spent inside and outside of a dot. Kim *et al.* [87] examined the difficulties of adopting palm print biometrics in unrestricted environments.

They suggested utilizing a local illumination normalization approach to cope with the problems originating from diverse backgrounds and illumination conditions. Zaidi *et al.* [88] provides a detailed overview of underpin touch-based continuous mobile device authentication. They discussed methods in touch data acquisition, behavioral feature extraction, user classification, and evaluation methods with challenges and opportunities for touch-based continuous mobile device.

2.2 Factors Impacting Smartphone Biometric Authentication

This section discusses a research study on factors that can impact the smartphone Biometric authentication performance due to external factors (like a mask). The COVID-19 pandemic is currently affecting the entire world. People are using a variety of methods to stop the spread of the coronavirus. In the pandemic times to withdraw the cash from ATM machine there is chance of virus spread, Muhammad Irwan Padli Nasution *et al.* [89] proposed to do payment in the offline market by facial recognition instead of PIN. Jonathan S. Talahua *et al.* [90] developed a system to detect people wearing a mask or not from photographs. They used MobileNetV2 architecture and the OpenCv's face detector.

Numerous essential precautions must be taken to avoid contracting COVID-19, the most important of which is wearing a face mask. Many researchers concentrated their studies during the COVID-19 pandemic on whether or not people wear masks [91][92]. This pandemic has left us to focus more on studies that have considered "masks" as a requirement to fit into their face recognition systems [93]. Though the studies to improve face recognition have improved a lot, recognizing faces covered with masks has evolved into an all-new concern due to the sudden pandemic. Unfortunately, not many studies have been done in this area. There are only a few researches included in the next paragraph.

One such major study was conducted by Wang *et al.* [19], who achieved a 95 percent overall accuracy by adopting a face-eye-based multi-granularity masked face recognition model. To a certain extent, they addressed another insufficiency in this domain, which is the availability of a few public datasets for face recognition using mask datasets.

There have been negligible advancements in this regard till now. They used existing face recognition datasets as well as self-developed simulated masked faces integrated with masked faces from actual scenarios as the final database to train a face-eye-based recognition algorithm. Unlike the previous model suggested by Zhongyuan Wang *et al.*, which involves eliminating masked face regions and afterward implementing pre-trained deep convolutional neural networks (CNNs) to retrieve the best attributes from uncovered face regions, Hariri [35] developed a revised approach that relies on throwing away masked regions in combination with deep learning-based features (generally forehead regions and eyes). Cabani *et al.* [94] developed a technique for resolving the challenges associated with recognizing masked faces using the existing facial recognition system. They have developed an open-source tool called MaskTheFace, which can be used to mask faces.

Xinqi Fan *et al.* [95] proposed RetinaFaceMask, the first high-performance single stage face mask detector for assisting control of the COVID-19 Pandemic. Soad Almabdy *et al.* [96] has proposed a model which investigates the performance of the pre-trained convolution neural network (CNN) for face biometric system with AlexNet and ResNet-50 for extracting features and Support Vector Machine (SVM) as a classifier. Hazar Mliki *et al.* [97] has proposed an architecture composed of two networks, first one is the region proposal network that generates a list of regions of interest (ROIs) and a second corresponds to a network that use these ROIs for classification into face/non-face.

A table of comparisons for different techniques for recognizing masked faces has been covered in Table 2.1.

Table 2.1: Comparison of Masked Face Recognition Techniques

Author & Publication Year	Techniques used	Dataset used	Performance metric
Wang et *al.* [19],2020	the face-eye-based multi-granularity recognition model	MFDD, RMFRD, and SMFRD	95% accuracy
Hariri [35], 2020	Convolutional neural networks (CNN) + MLP	RMFRD	91.3% recognition rate
Shiming Ge *et al.* [36], 2017	LLE-CNN model	MAFA- Masked Faces	76.4% precision
Cabani *et al.* [94],2021	MaskTheFace tool to generate masked faces for better training of existing face recognition ML models	VGGFace2	+38% in true positive rate (highest recognition rate achieved is 93%)

2.3 Research Motivation

We have identified the following gaps in the literature as a result of the analysis of state-of-the-art biometric authentication system in smartphones. These research gaps have been examined in our study.

Based on the analysis of the literature study, we found that the impact of external factors and contextual factors on biometric authentication is relatively under-investigated in smartphones. Moreover, the impact of the COVID-19 pandemic on conventional biometric authentication techniques is not been explored much.

1. From the aforementioned literature review, we conclude that the effect of external factors (like the impact of hand gloves, wet hands, etc.) and contextual factors (like the location, time etc.) has not been studied in detail and there is a scope for providing

useful solution. For this purpose, our work describes the development of an intelligent multimodal biometric authentication system that is suitable for a variety of contextual and external factors.

2. Smartphone fingerprint or facial recognition systems may not be as effective in pandemic situations like COVID-19, where hand gloves or sanitized hands are required to protect against unwanted exposure of body parts. We propose and investigate a biometric authentication system for smartphones that is built on the multimodal swipe and keystroke dynamics patterns. This gives an alternative solution to biometric authentication during COVID-19 pandemic situations.

3. Feature phones are frequently keyboard-based or less advanced forms of touch-screen mobile phones, designed for basic calling and messaging. In contrast to smartphones, feature phones don't include a biometric mechanism for unlocking the device. According to the existing literature, there have been just a few attempts to design an effective biometric authentication system for low-cost feature phones. A biometric authentication system makes use of characteristics derived from an individual's behavioral or physiological characteristics. An effective and flexible biometric framework can be achieved by applying keystroke dynamics in feature phones. We propose and investigate one such framework in this study.

4. To curb the spread of COVID-19, every healthcare agency and civic body around the globe has been advised to wear masks. However, this necessary practice has posed a significant challenge for modern facial recognition technology, as it is applied in various applications, including face-identification-based attendance systems, security checks at city malls, airports, train and metro stations, and face unlocking systems in smartphones. There is a need to incorporate measures to recognize human faces even when wearing masks. Given the sudden challenge that human society is experiencing as a result of technological gaps, enhancing the performance of existing facial recognition systems has become a need of fundamental importance for the research community. Face recognition is a mature technology with many approaches built over the decades using different deep learning methods. These methods are continuously improving with advancements in the machine learning field. Face recognition finds significant security applications that simultaneously demand speed and accuracy. This requires the system to be highly optimized and efficient. In this

work, we propose a Face Mask recognition biometric authentication system to handle the COVID-19 pandemic face recognition problem when a significant part of the face is covered with a mask to protect from the virus.

2.4 Thesis Contribution

The major contributions from this research to various challenges of biometrics in mobile devices are summarized below:

1. A novel multimodal biometric authentication framework that has the capability to handle the input biometric samples that are impacted by external and contextual factors. A machine learning-based biometric authentication framework is proposed as part of the study.

2. To evaluate the proposed novel biometric authentication framework an innovative bi-modal system is proposed which can operate with high accuracy. A Handglove mode is proposed for smartphones considering the COVID-19 pandemic situation when the user input samples are impacted by external factors like water, sanitizer, and surgical gloves and it is difficult for a legitimate user to authenticate using conventional biometric authentication methods like fingerprint recognition. We develop a multimodal behavioral biometric authentication system based on keystroke and touch swipes that can also handle situations when the user samples are impacted by external factors like hands with gloves, water, and sanitizer. To test the system, data collection was performed with 197 users using an Android application developed on Android OS 11.0 and Samsung Galaxy S20 devices. The experimental results show an Equal Error Rate of 6.46% while samples are impacted by external factors (wet and sanitized hands).

3. In this work we have proposed a keystroke dynamics-based system for feature phones. In this work, we have utilized the user's typing patterns to enhance the security of feature phones. We have applied k-NN with fuzzy logic classifier and achieved an Equal Error Rate of 1.88%. The experiments are performed with 25 users on Samsung On7 Pro C3590.

4. In this work, we propose a solution for Masked face recognition system based on the HAAR cascade along with Local Binary Pattern Histogram (LBPH) and Fuzzy logic. Our work uses the Haar-feature-based cascade classifier and LBPH to determine the similarity between the presented face with the registered face. This work further goes on to address the problems due to variations that occur when the user wears a mask covering different areas and percentage coverage of the face on different occasions resulting in obvious inaccuracies resulting in too many false negatives or false positives depending on the threshold score. This problem is addressed by making use of a fuzzy-logic-based system that dynamically decides the "threshold confidence score" needed to pass the authentication. Our proposed model for masked face recognition achieves an accuracy of 86% when a Haar-feature-based cascade classifier and LBPH are used standalone which further increase to around 97% when used in conjunction with a fuzzy-logic-based system.

2.5 Conclusion

In this chapter, we studied the principles of biometric authentication systems, especially for mobile phones as well as examined the current state of the art. We also highlighted the impact that the current COVID–19 pandemic has on existing biometric authentication systems. We structured the research problem and identified the tools, techniques, methods, and processes for developing an effective biometric authentication system using the knowledge gained from the review. Most of the existing work in behavioral biometric authentication uses a single biometric. Thus, the advantages of multimodal biometrics aren't realized. Furthermore, none of the works that we studied incorporate variations in external factors like the use of hand gloves or sanitized hands while operating the smartphone. We believe that our proposed work can be an incremental contribution to the state of knowledge.

Chapter 3: Multimodal Biometric Authentication Framework for Mobile Phones in the presence of External and Contextual Factors

3.1 Introduction

Various methods exist for user authentication in a smartphone device. The commonly deployed methods are the use of a PIN type password access, pattern type access (Figure 3.1), and biometric type of access (e.g. IRIS, fingerprint, facial recognition, etc.), behavioral biometric type of access (for example swiping pattern, tapping speed, etc.). Such authentication usually provides an effective way of user verification. The existing approaches do not sufficiently consider a real-time scenario in which the user accessing a device may face various real-time issues while accessing it. While performing a biometric authentication (fingerprint) there can be a possibility the user encounters the presence of water droplets/film or dust particles, which we have referred to as external factors, on the touch screen of the electronic device. This may result in authentication failures with high false negatives. Such scenarios hamper the user experience of performing faster and more accurate authentication since the system is interrupted due to these external factors and it leads to longer response time and higher error rates. Overall, at least the limitations of the existing approach are that they are static and are not trained in real-time to identify various external factors.

Besides external factors, other contextual factors correlated with the authentication of the user could be, for example, user location, time, the network connectivity of the electronic device, or the behavioral pattern of the user, etc. The conventional approaches do not utilize the contextual factors appropriately while the user is performing authentication.

Thus, there is a need to implement an intelligent biometric authentication framework that takes care of the external factors while taking advantage of the contextual factors. This chapter introduces the proposed biometric authentication framework and elaborates in detail on the role of contextual factors in selecting the modality of the authentication model.

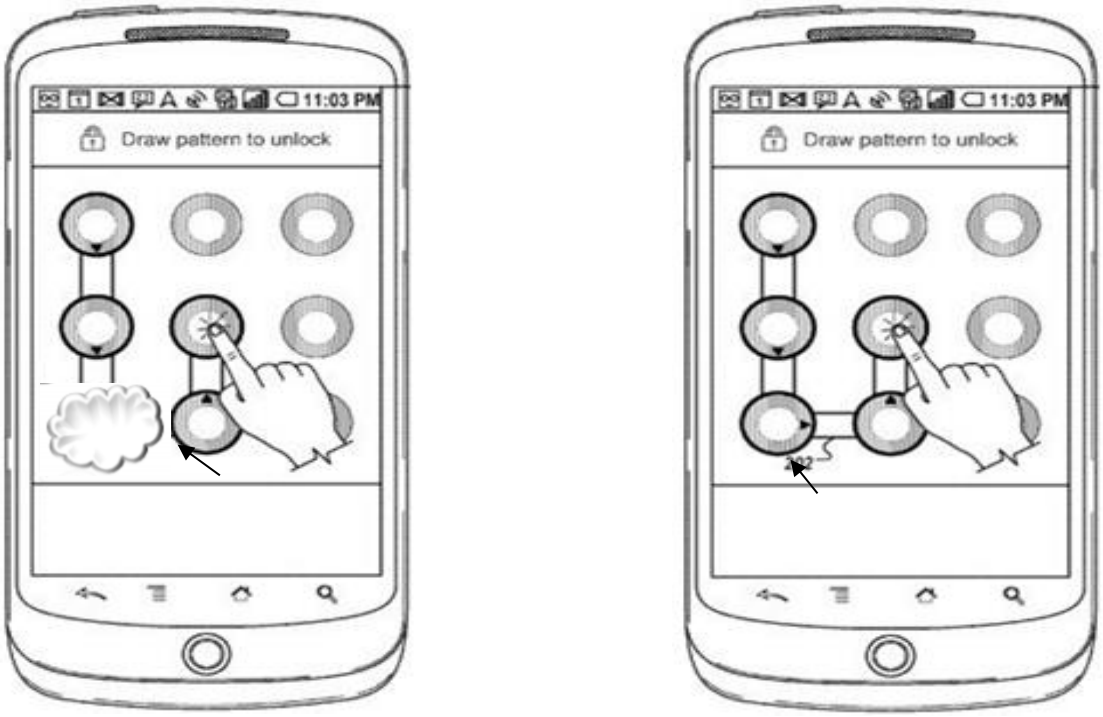

Figure 3.1: Pattern Lock Authentication

3.2 Proposed Multimodal Biometric Authentication Framework

We propose a method for authenticating the user in the presence of external and contextual factors. The method comprises identifying a user context from the plurality of contexts (user location, time, device connected, etc.). The presence of external factors (dust, water, glove, etc.) is determined on the touch screen from the dynamic external factor determination logic. An authenticating action is received from the user in the presence of the determined external factor. A selected authentication model is obtained from the trained authentication unit which is trained on the plurality of external factors, wherein for untrained similar clustered external factor authentication model from fuzzy logic is fetched. In a real-time situation, it is difficult to authenticate the user in the presence of various external factors for example dust, dirt, water, liquid, and gloves, owing to the low accuracy of authentication.

To enable this, the proposed system performs:

1. Detection of type of external factor
2. Authentication Model development and training on multiple samples.
3. Detecting Authentication by matching with the trained model within a threshold range along with matching contextual factors.
4. Fetching the next layer of the authentication model dynamically.

Figure 3.2 illustrates an exemplary block diagram of a system for authenticating a user in the presence of external factors using machine learning (ML).

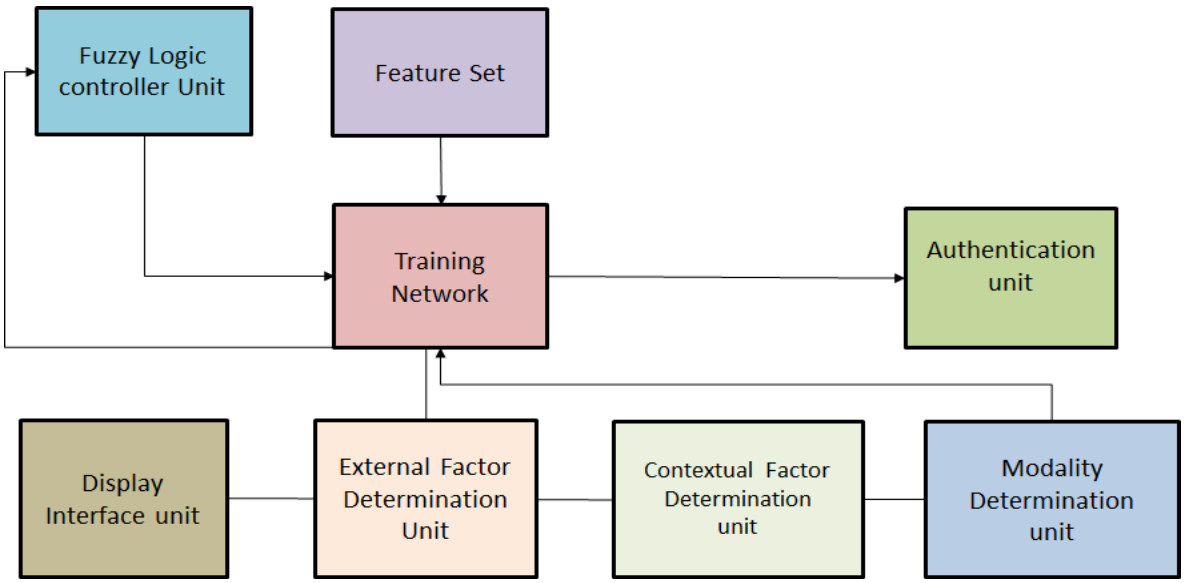

Figure 3.2: Proposed biometric authentication system

The system includes components such as a display interface unit, external factor determination unit, contextual factor determination unit, modality determination unit, authentication unit, training network, fuzzy logic controller, and feature set unit.

The display interface unit (smartphone touch display) is configured to display information to implement the authentication process. The External Factor Determination unit includes various sensors to detect external factors present on the display interface unit. The various external factors may include, for example dust, dirt, water, liquid, gloves, or artificial lens on IRIS.

The Contextual Factor Determination unit includes, for example, CPU or one or more processors, and various sensors like GPS to determine contextual information of the user as well as of the smartphone device [98]. The contextual information or contextual factor of the user as well as of the smartphone device includes, for example, network connectivity, user behavioral pattern, user location, time, etc. For example, the contextual information as represented in Figure 3.3 can be network connectivity or user location of the user may be determined whether the smartphone device associated with the user is connected with a public network or office network, or home network.

The system dynamically detects the contextual information from the aforementioned set for each level of the authentication process having varying complexity grades.

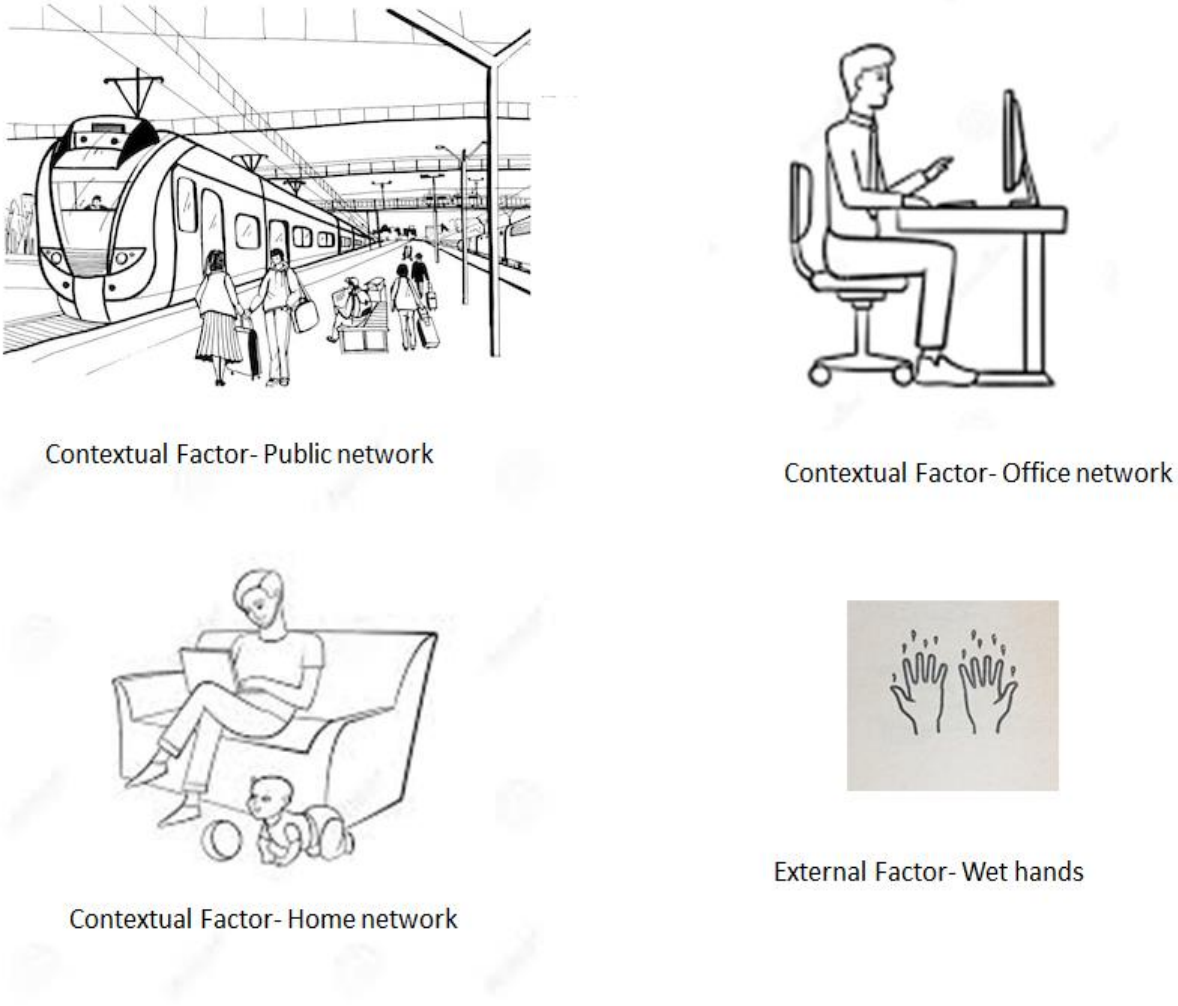

Figure 3.3: Examples – Contextual and External factors

Further, the display interface unit, an external factor determination unit, and a contextual factor determination unit form a part of an input module.

The modality determination unit is configured to determine a single modality or multi-modality authentication process based on the complexity grade of the authentication process. The complexity grade of the authentication process can be categorized as a low, moderate, or high complexity grade as explained in Table 3.1.

Table 3.1: Modality Determination – Based on Contextual Factors, and Threshold

Location Familiarity	Network Familiarity	Computed Contextual Confidence Score	Complexity	Modality
High	High	$X1 + \Delta$	Low	Single
High	Low	$X2 + \Delta$	Moderate	Dual
Low	High	$X2 + \Delta$	Moderate	Dual
Low	Low	$X3 + \Delta$	High	Multiple

Here,

$X1 : first\ threshold$

$X2 : second\ threshold$

$X3 : third\ threshold$

$where, X1 > X2 > X3$

Δ *: Positive number, small compared to the X1, X2, and X3 thresholds, showing that the calculated contextual confidence score is greater than the contextual confidence threshold. It is an attempt to show that the choice of multi-modality in insecure environments (in the 2nd, 3rd, and 4th rows of Table 3.1) results in stricter authentication regimes.*

The Training Network unit can be implemented with various machine learning models. Figure 3.4 and Figure 3.5 illustrate an authentication model trained through the training unit based on the data sets for Fair samples, Not Good samples (NG) for various biometrics such as (keystroke and touch swipe) obtained from the feature set unit. NG

samples are the ones impacted by external factors like Dust, Oil, Water, Hand Gloves, etc.

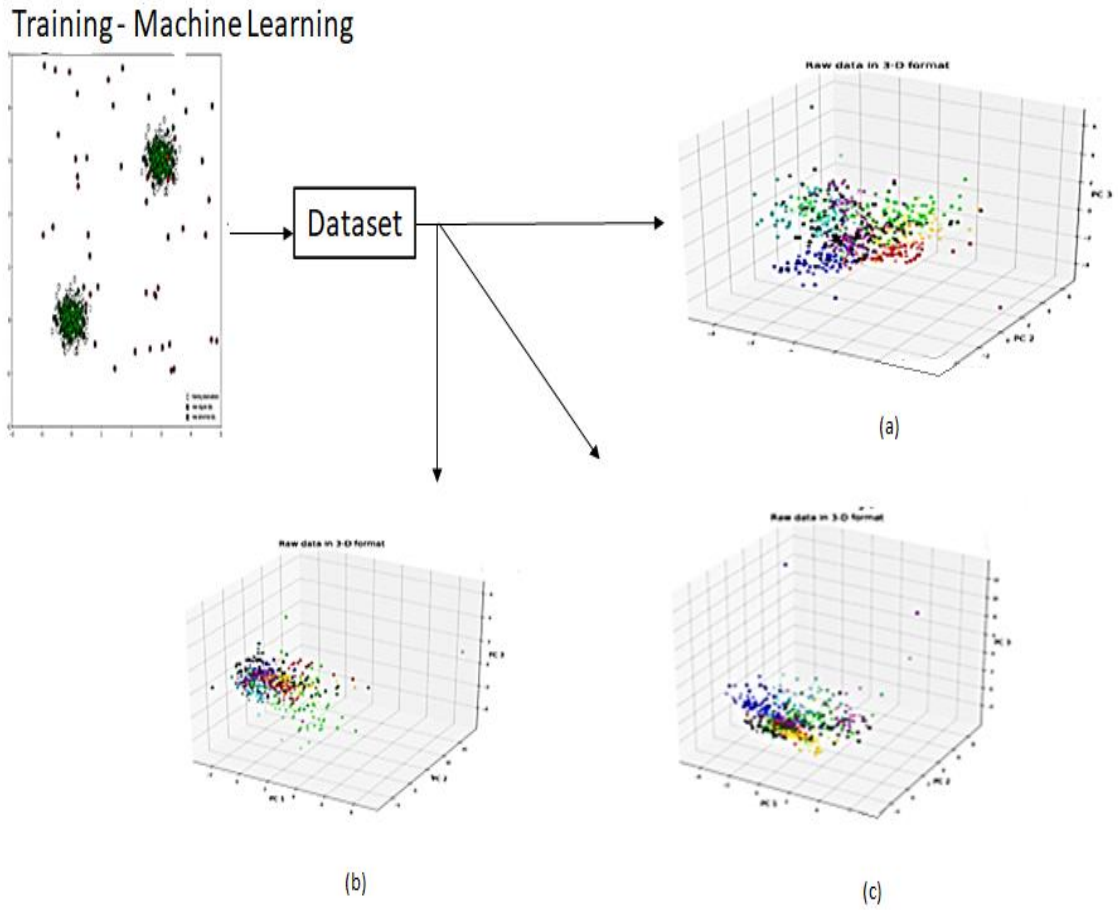

Figure 3.4: Trained Model – (a) fair samples (b) samples impacted with water (c) samples with gloves

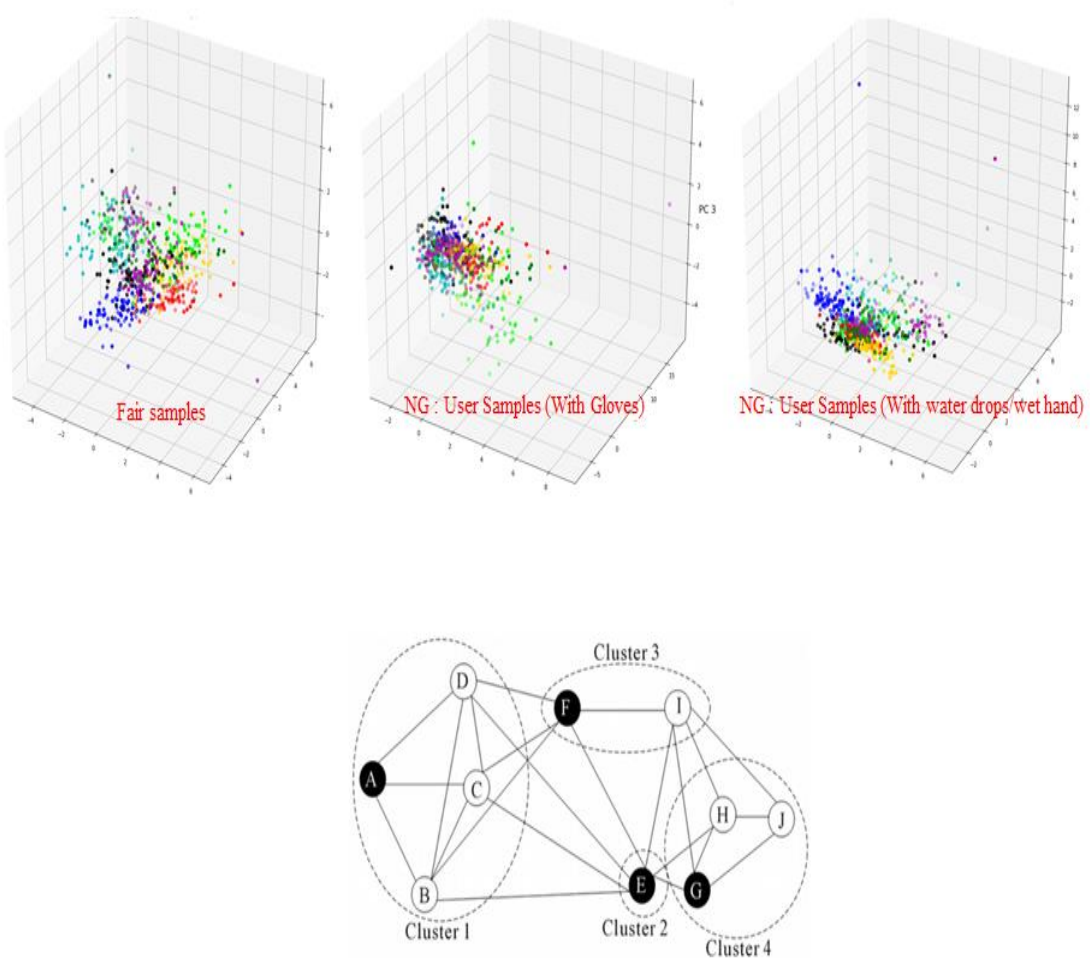

Figure 3.5: Trained model with correlated cluster

Such clusters as mentioned in Figure 3.5 facilitate fetching the right authentication model out of the available lot based on the determined external factor.

The Authentication unit is configured to authenticate the user in the presence of external factors by matching at least one contextual information determined by the Contextual factor determination unit with corresponding trained authentication models fetched from the Training Network unit. The authentication unit and modality determination unit form a part of the authentication module.

Figure 3.6 illustrates the block diagram of the Fuzzy logic controller unit. The fuzzy logic controller unit includes a rule-based engine, Fuzzifier unit, Inference engine unit, and De-fuzzifier unit. If the model is untrained for the determined external factor, then the Fuzzy framework is utilized to classify the NG samples. Let us consider the following cases of external factors (NG samples) on which Training is not performed - For example oil and cloth then the corresponding authentication model is fetched from the Fuzzy logic

controller unit. Based on the extracted features, a similar clustered external factor authentication model is fetched to act as an authentication model during the first authentication process.

The fuzzy framework classifies the NG samples with external factors for which a trained authentication model is not available. The advantage of applying a fuzzy framework is to deal with authentication in the presence of external factors which tend to reduce the accuracy of authentication.

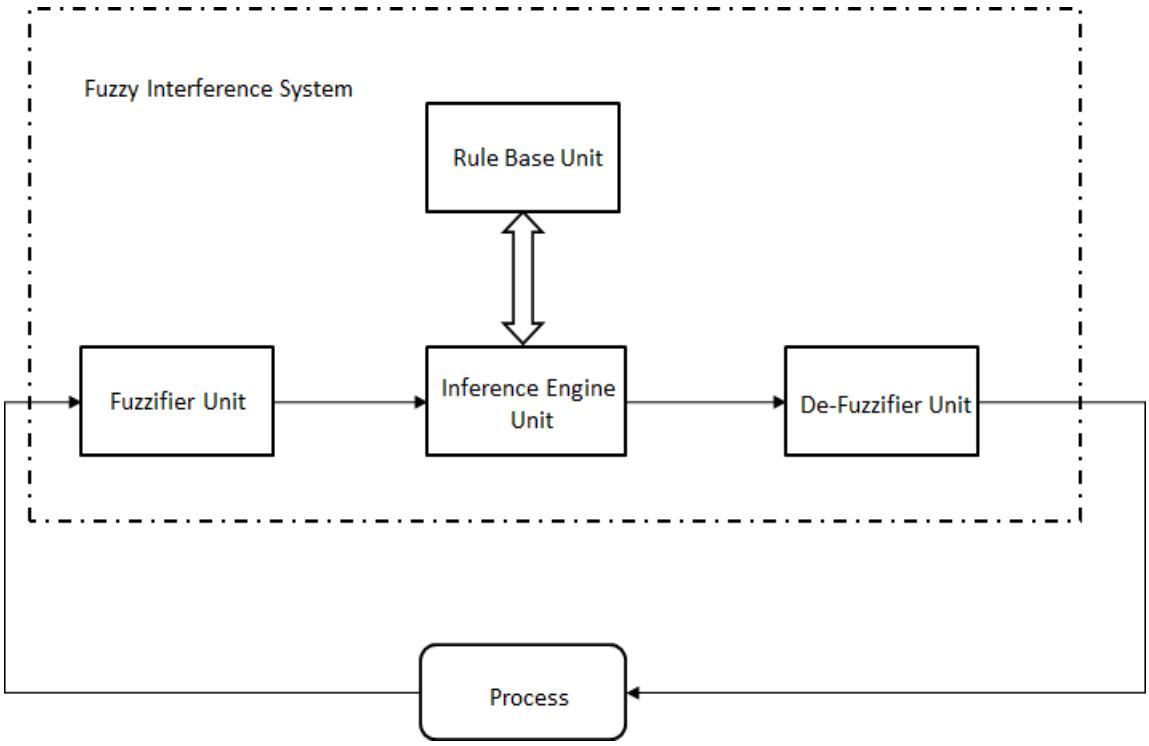

Figure 3.6: Block diagram of fuzzy logic controller

Figure 3.7 illustrates the flow chart for the proposed multimodal biometric authentication system while a user accessing a smartphone. It is described below.

At Block 801: the system determines the access request received from the user performing authentication and determine the external factor and the contextual information.

At Block 802: the contextual confidence score is computed by feeding in the contextual features to the context classification model to get the 'Contextual Confidence Score' for the current user's context.

At Block 803: The confidence score computed at block 802 is compared to the 'First Contextual Confidence Threshold' which is pre-set by the designer. If the score is greater than the threshold, the system moves to block 805 otherwise it moves to block 804.

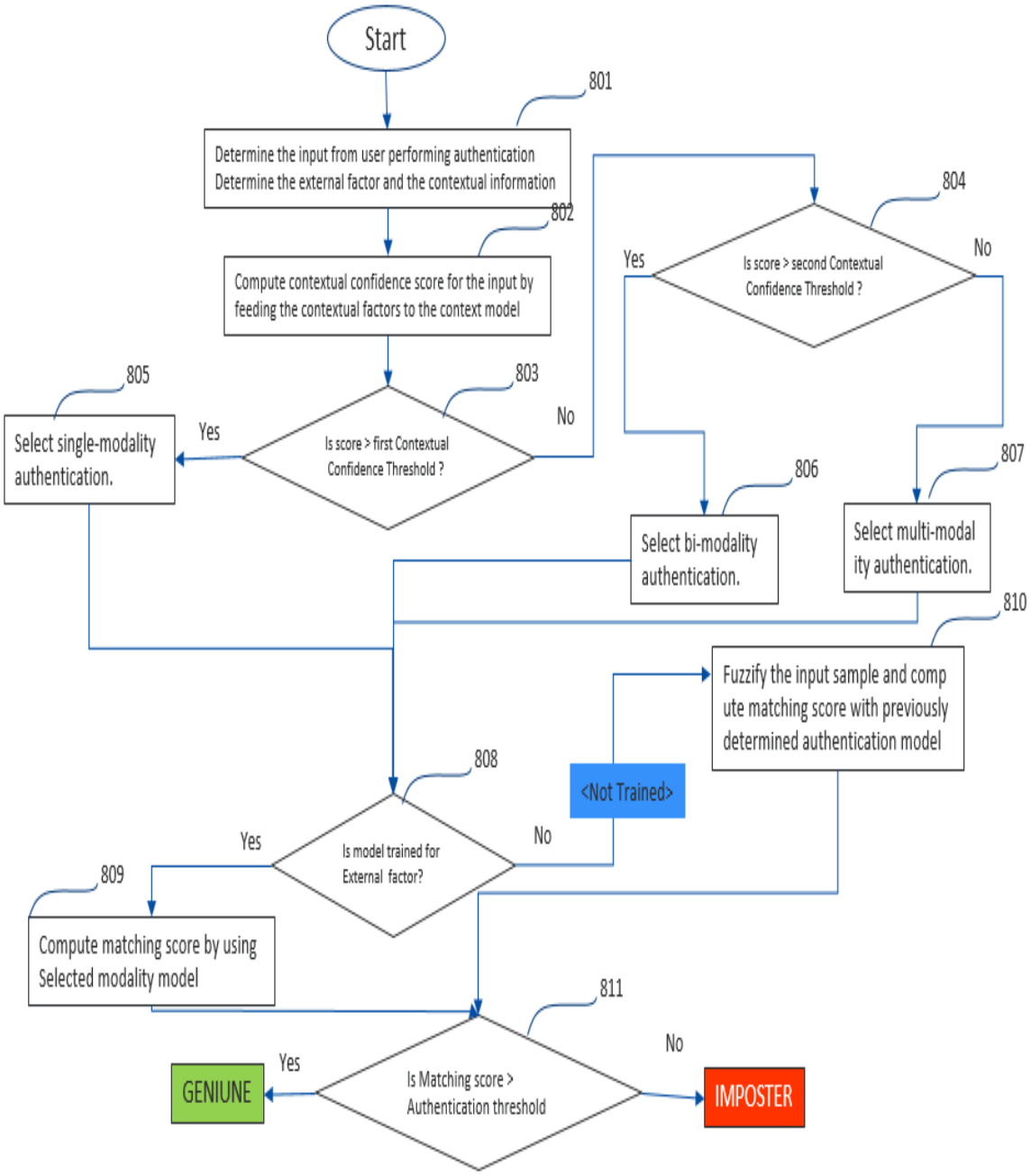

Figure 3.7: Flowchart of proposed biometric authentication system

At Block 804: The confidence score computed at block 802 is compared to the 'Second Contextual Confidence Threshold' which is also pre-set by the designer with constraint

(Second threshold < First threshold). If the score is greater than the second threshold, the system moves to block 806 otherwise, it moves to block 807

At Block 805: the system selects a single-modality recognition model for authenticating the user. The system moves to block 808 with the selected modality information.

At Block 806: the system selects a bi-modality recognition model for authenticating the user. The system moves to block 808 with selected modality information.

At Block 807: the system selects a multi-modality (modality > 2) recognition model for authenticating the user. The system moves to block 808 with the selected modality information.

At Block 808: The system determines whether the authentication model is trained for the external factor. If the determination is yes, it moves to block 809 else, it moves to block 810.

At Block 809: the system computes the matching score by directly using the selected modality model in the previous steps. It then moves to block 811.

At Block 810: If an authentication model is not trained for the determined external factor, then the fuzzy logic unit is utilized. A similar clustered external factor authentication model based on the extracted features is extracted to act as an authentication model during the first authentication process.

At Block 811: the system compares the matching score with the authentication threshold and if the matching score exceeds the threshold, then the user is authenticated as 'Genuine' otherwise 'Imposter'.

3.3. Experiment Results

We collected a dataset of swipe and touch dynamics from 34 users (90 samples from each user) during which we have also extracted features that describe the user's context at the time of authentication for each sample as listed in Table 3.2. Then we partitioned the dataset into the training set and test set with the size ratio of 4:1. Since the total number of samples we collected is 3060, the size of our training set is 2448 samples and the size of our test set is 612 samples.

First, we employ a model for each user to output the contextual confidence score on that user's context by inputting the contextual features, namely parameters denoting familiarity of user's location and network. The network familiarity parameter is a multiplier with the following behavior: A known frequently used network was given the

multiplier of 2, a known intermittently used network was assigned a multiplier of 1, and an unknown network was assigned a multiplier of 0.5. This multiplier multiplies with the location familiarity parameter. The location familiarity parameter is the reciprocal of distance in kilometers from the nearest known location hotspot for the user.

For each user, we consider the self-samples as positive samples and the other users' samples as negative ones. Upon determining the confidence score of the user's context, we determine the modality to be used for authenticating the user by using different contextual confidence thresholds.

Table 3.2: Feature set of the proposed context model and definitions

Features	Description
Nearest Distance	Distance from the user's current location to the nearest hotspot (Most visited places) of the user
Network Status	Whether the device is connected to a home/public/ private network

Table 3.3: Feature Set of the Touch Swipe pattern

Event	Features	Description
Swipe	MajorAxis	Orientation of touch area with axis along x-axis when touched on a screen
	MinorAxis	Orientation of touch area with axis along y-axis when touched on a screen
	SwipeTime	Duration of swipe
	Speed	distance covered by swipe in touch duration

Table 3.4: Feature Set of the Keystroke

Event	Features	Description
KeyStroke	Key1_Latency	Hold Time Key1
	Key2_Latency	Hold Time Key2
	Key3_Latency	Hold Time Key3
	Key4_Latency	Hold Time Key4
	Key5_Latency	Hold Time Key5
	Key6_Latency	Hold Time Key6
	Key1_2_Latency	key switch time K1->K2
	Key2_3_Latency	key switch time K2->K3
	Key3_4_Latency	key switch time K3->K4
	Key4_5_Latency	key switch time K4->K5
	Key5_6_Latency	key switch time K5->K6

In our current experiments, we have limited the number of variations in modalities to one or two, that is, the Uni-modal authentication system and Bi-Modal authentication system. For the unimodal approach, we have trained the authentication system with keystroke features. For bimodal authentication, we have trained the model with combined feature space of touch swipe and keystroke dynamics. The feature set we have used for touch swipe and keystroke dynamics is listed in Table 3.3, and Table 3.4 respectively. For training the network, we have used a k-NN classifier with hyper-parameter k set to 5.

For these two different modalities approaches, we have utilized a single contextual confidence threshold for deciding the target modality. If the contextual confidence score crosses the threshold, we define the target modality as a single modal otherwise, we define it to be bi-modality. To evaluate our approach, we experiment with

three different contextual confidence thresholds and for each threshold, we estimate the equal error rate of the proposed authentication system on the test set of 612 samples. We provide our results in Table 3.5.

Table 3.5: Evaluation Results based on Contextual Factors

First Contextual Confidence Threshold	Authentication Modality	No. of samples assigned	Equal Error Rate (EER %)
0.5	Single Modal	228 (37 %)	3.5
	Bi-Modal	384 (63 %)	3.21
0.7	Single Modal	185 (30 %)	3.51
	Bi-Modal	427 (70 %)	2.68
0.8	Single Modal	172 (28 %)	3.32
	Bi-Modal	440 (72 %)	2.56

From Table 3.5, we observe that by increasing the confidence threshold, the number of samples that are assigned to use bi-modal authentication increases which is as expected. The EER of the system also decreases by increasing the threshold which demonstrates the effectiveness of the bi-modal system in authentication over a single modality. We attribute the increase in accuracy (decrease in EER) to the diverse feature set in the bi-modal system which suggests that the authentication system accuracy improves by increasing the modality of the authentication features. We observe that the EER is about ~ 3% over the entire experiment.

3.4 Conclusion

In this chapter, we have introduced a novel multimodal biometric authentication framework that dynamically defines multi-modality for smartphone user authentication based on contextual and external factors. In our system, the contextual model evaluates the user's context at the time of authentication to provide initial confidence of identity. Based on the obtained confidence, the authentication complexity or modality of the final authentication model is determined dynamically. In our experiments, we have considered two different modalities but this can be set based on the designer's choice. For example, the designer might design Uni-, Bi-, Tri- Modal authentication models and utilize them for three different confidence levels. More details on the applications of the proposed biometric authentication framework are discussed in Chapter 4, where we have utilized the proposed multi-modal behavioral biometric authentication framework for Covid-19 like pandemic situations.

Published Patent:

The work discussed in this chapter is published in patent filed in Indian patent office:

Title: "Method and System of Authenticating a User in an Electronic Device" Authors: Amitabh Thapliyal, Om Prakash Verma and Amioy Kumar Application number: 202011025242, Published Date: 17th December 2021

Chapter 4: Multimodal Behavioral Biometric Authentication System in Smartphones for Covid-19 like Pandemic

4.1 Introduction

Smartphones store and process a large amount of private and financial data, which can cause serious loss when it falls into the wrong hands. Therefore, a strong user authentication system is a critical requirement in smartphones [99]. Traditional authentication approaches in smartphones, such as PIN, password, and pattern, are prone to various attacks such as shoulder surfing, guessing attacks, brute force attacks, and dictionary attacks [9]. Shoulder surfing is a very common attack in which the user's password is compromised by peeping into the password entry screen while the actual user types in the password [8]. Biometrics such as the face, fingerprints, voice, and iris are some of the authentication solutions that are the recent trend in smartphones [100, 101]. Biometrics utilize physiological or behavioural characteristics of the user that need to be presented at the time of authentication. Hence, they cannot be guessed or attacked through brute force. This eliminates the possibility of shoulder surfing.

However, biometrics also have their limitations. Fingerprints or facial recognition-based authentication systems may not provide accurate results due to the use of hand gloves, wet hands or face masks, particularly in healthcare environments and COVID-19 pandemic situations. Additionally, facial recognition-based verification is less accurate in low light [10] and vulnerable to image spoofing. Fingerprints are known to fade away in the working population that uses the palms, especially if they do heavy work. Fingerprint authentication also fails with wet, wrinkled, as well as aging fingers.

Like all authentication techniques, biometrics also suffers from the problem of specificity-sensitivity tension [102]. Authentication requires high sensitivity, but it comes at the cost of reduced specificity, making it prone to focused attacks. Because of these reasons, there is always a need for multimodal biometrics. Multimodal biometrics means that multiple biometric features are used to improve the overall sensitivity and specificity of the authentication system.

Most of the existing work in behavioural biometric authentication uses a single biometric. Thus, the advantages of multimodal biometrics [103, 104] aren't realized, especially in

mobile phones. Furthermore, based on the literature review study we found that none of those behavioural biometric authentication systems for mobile phones, incorporate variations in user behaviour and environmental changes like the use of hand gloves, and wet hands while operating the smartphone.

In this work, a new multimodal behavioural biometric authentication system using uniquely identifiable characteristics of touch swipe, and keystroke dynamics of the user is explained. Keystroke dynamics-based biometric authentication is based on the fact that each user's keystroke pattern is unique and consistent. The proposed system incorporates the user's touchscreen swipe and typing patterns as an additional security layer for authentication to increase the overall security of the system. Our experimental results suggest that the proposed multimodal biometrics system can operate with high accuracy and even wearing hand gloves or wet hands has minimal effect on the accuracy of the authentication system. The proposed multimodal system could improve the sensitivity, specificity, accuracy, and security of biometrics based authentication in smartphones.

In this study, experiments were conducted with a range of classifiers, including the Isolation Forest Classifier, SVM, k-NN Classifier, and fuzzy logic classifier, to find which classifier gives the best authentication accuracy for Samsung Galaxy S20 device users. In the case of a COVID-19 pandemic, the suggested multimodal system intends to be a significant improvement over existing methods for biometrics-based mobile authentication.

4.2 Proposed Multimodal Behavioral Biometric Authentication System for Smartphones

In this research, we propose a new multimodal behavioral biometric system that uses touchscreen swipe and keystroke dynamics patterns to uniquely identify the user and distinguish them from imposters. We propose a multimodal behavioral biometric authentication system with the fusion of the touchscreen swipe and keystroke dynamics. The acquisition of these two biometrics is easy and user-friendly, as both of these modalities can be acquired in one action of the hand. Another important highlight of this work is that it investigates the proposed multimodal system for situations where hand are covered with gloves or wet hands. We propose a Hand Glove mode of authentication for

smartphones where the system will be triggered to authenticate a user based on Touchscreen swipe and Keystroke dynamic patterns.

4.2.1 Hand Glove Mode

This mode will trigger the multimodal behavioural authentication system and allow device access based on user acceptance by the proposed multimodal system using user swipe and keystroke dynamics. A depiction of the Hand Glove mode in mobile devices is shown in Figure 4.1.

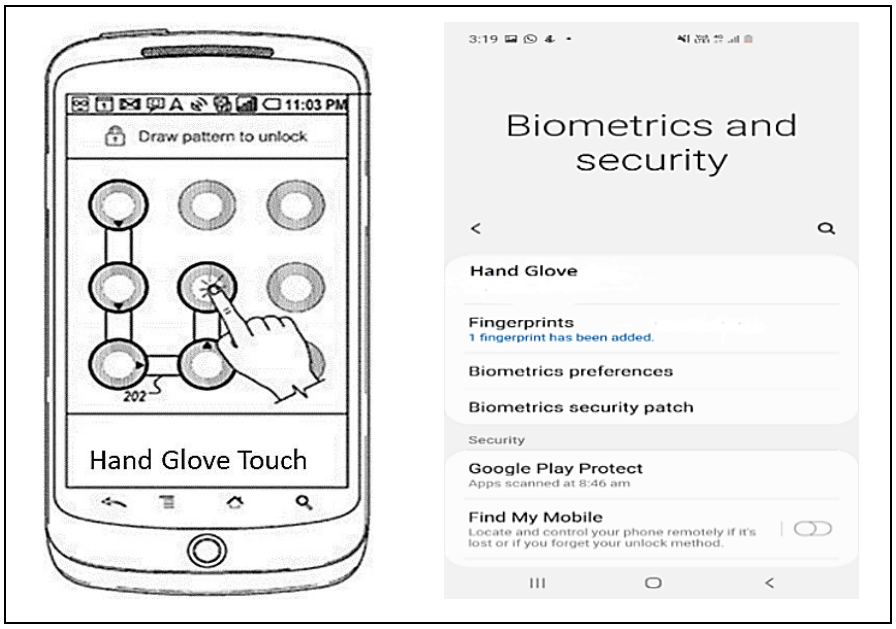

Figure 4.1: Hand Glove Mode - Multimodal Behavioral Biometric

4.2.2 Modules of the Proposed Multimodal Behavioral Biometric Authentication System

In this section the architecture and module details are explained of the proposed Multimodal behavioral biometric authentication system.

A block diagram of the proposed multimodal behavioral biometric authentication system is shown in Figure 4.2.

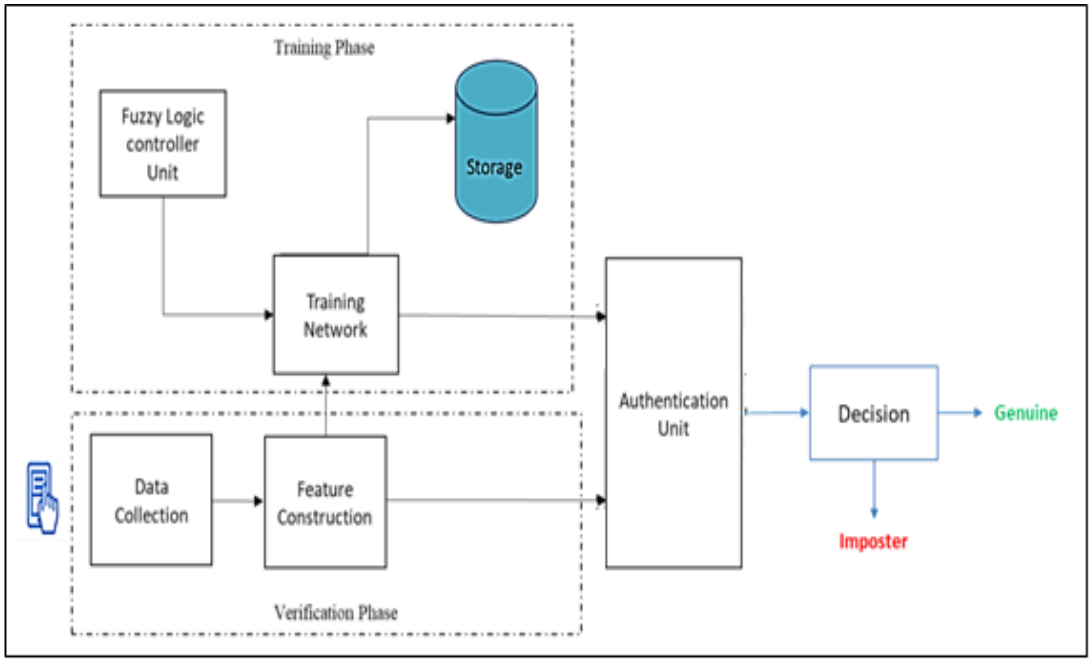

Figure 4.2: Multimodal behavioral biometric authentication system.

4.2.2.1 Data Collection

The data collection for the proposed system is done through an android application that triggers the physical sensors to read touchscreen for swipe touch patterns and keystroke password-key input by users. For touchscreen swipe, accelerometer and gyroscope are the sensors used to acquire the user inputs. It captures the touch speed and distance of swipe features corresponding to each enrolled user. For keystroke, we captured the hold-time and inter-key time as a feature for each enrolled user. In contrast to the enrolment module of other biometric systems, the input to the enrolment system in the proposed multimodal system may work in continuous enrolment mode.

The enrolment system works in the background and reads the swipe pattern and keystroke inputs when the user logs into the system. The application was developed on a Samsung Galaxy S20 device using Google Android OS, 11. We collected data from 197 users (124 men, 73 women) aged between 25 and 40 years. The data collection was done in three different postures: standing, sitting, and walking. The users who participated in the data collection process are presented with a mobile application to collect sensor measurements required to calculate feature values encompassing the behavioral patterns in touch-screen

swipe and keystroke dynamics. The users are required to swipe on the application and then type the password (6-digit) appearing on the screen. These steps are to be repeated 30 times for each position and with three different scenarios of external factors namely dry hands, wet hands, and hands with gloves. The schematic of the data collection application is presented in Figure 4.3.

For the experiments, we collected 30 patterns from each individual in each posture. We also asked users to provide inputs with dry hands, wet hands, with gloves as part of data collection, to handle such scenarios to better train the model in Hand Glove mode. In total, we collected 53190 samples from 197 users under the three mentioned postures and three external factor cases. Data collection was performed in two separate sessions for each user. The entire enrolment process took 2 weeks period to collect sample data from all 197 users.

Data collection and all experiments were performed at the **Samsung Research Institute, India R&D**.

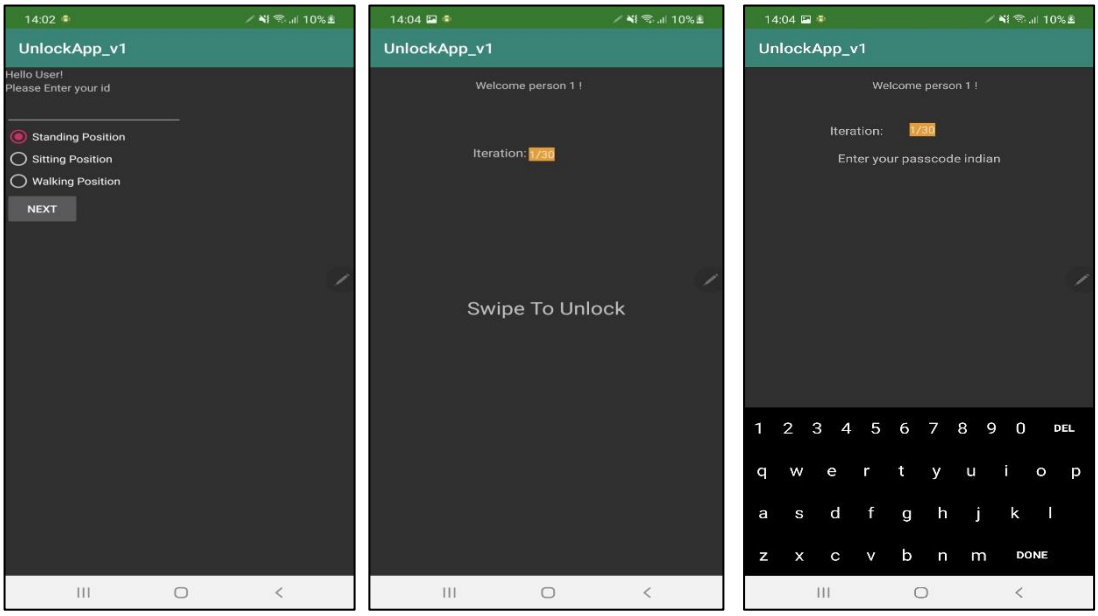

Figure 4.3: Schematic of the keystroke and touch swipe behavioural data collection application from users. (a) Application home-screen where users set their current position. (b) Swipe layout where participants are asked to swipe on the screen to capture touch-swipe related feature values. (c) Password layout where users type the displayed password on the keyboard to capture keystroke dynamics.

4.2.2.2 Feature Extraction

The next step is to extract uniquely identifiable features from the collected data of the user. The features employed by us in our experimental setup are detailed in Table 4.1.

Table 4.1: Feature Set of proposed system and definitions

Feature Category		Features	Description
Swipe	Touch	MajorAxis	Orientation of touch area with axis along x-axis when touched on a screen
		MinorAxis	Orientation of touch area with axis along y-axis when touched on a screen
		SwipeTime	Duration of swipe
		Speed	Distance covered by swipe in touch duration
	Accelerometer	A_Mean	Mean of the set of accelerometer values during the swipe
	Gyroscope	G_Mean	Mean of the set of gyroscope values during the swipe
		G_SD	Standard deviation of the set of gyroscope values during the swipe
Keystroke		Key1_Latency	Hold Time Key1
		Key2_Latency	Hold Time Key2
		Key3_Latency	Hold Time Key3
		Key4_Latency	Hold Time Key4
		Key5_Latency	Hold Time Key5
		Key6_Latency	Hold Time Key6
		Key1_2_Latency	Key switch time K1->K2
		Key2_3_Latency	Key switch time K2->K3
		Key3_4_Latency	Key switch time K3->K4
		Key4_5_Latency	Key switch time K4->K5
		Key5_6_Latency	Key switch time K5->K6

To use these distinct features jointly in multimodal authentication, we need to fuse the information extracted from them. Fusion of this information can occur at various levels, such as feature level [105-106], match score level [107], rank level [108], and decision level [109]. Prior work in biometric authentication has shown that data fusion at the feature level results in the best accuracy. Hence, in our experiments, we employed feature level data fusion of the two behavior modalities, namely keystroke, and swipe dynamics. We combined the feature vectors of the two modalities and generated a combined feature vector with a total of 18 features. However, features extracted from different modalities have different value ranges; therefore, these values are normalized to represent them as a value from 0 to 1. We employ the min-max normalization, which maps the minimum of a feature to zero, the maximum to one, and everything else to a decimal between 0 and 1 [110]. Given a set of N feature vectors x_1, x_2,…x_N for thej^{th} feature, we normalize them as follows:

$$x_{ij,norm} = \frac{x_{ij} - x_{min,j}}{x_{max,j} - x_{min,j}} \tag{4.1}$$

where, x_{min} and x_{max} are calculated as follows:

$$x_{min,j} = \min_{i=1\ to\ N} x_{ij} \quad \text{and} \quad x_{max,j} = \max_{i=1\ to\ N} x_{ij}$$

4.2.2.3 Model Training

After the feature construction step, we experimented with three different classifiers namely 1. Isolation Forest (IF) 2. k-Nearest Neighbors and 3. Radial Support Vector Machine. We partitioned the collected dataset into training and test sets in a ratio of 85:15, and trained these classifiers on the training set. Both the training and the test sets contained all the variations of posture (sitting, standing, and walking). Each model was trained on the combined dataset of the presence of different external factors. The external factors considered in our experiments are dry hands (normal), wet hands (water), and hands with gloves. Each classifier was trained on the combined dataset collected under these three external factors presence from each volunteer. Evaluation of the model

involves computation of the False acceptance rate (FAR), False rejection rate (FRR), and Equal error rate (EER).

- ***Isolation Forest***

Isolation Forest works on the principle of the decision tree algorithm. It is an unsupervised learning technique mostly utilized for anomaly detection. This algorithm recursively generates partitions on the datasets by randomly selecting a feature and then randomly selecting a split value for the feature. Anomalies are patterns that have features that are dissimilar to the usual cases. It exploits the fact that anomalous observations are few and significantly different from normal observations. In other words, it works on the logic that outliers take fewer steps to isolate compared to the normal point in any data set.

Let *s*: anomaly score at instance *t*.

p(t): length of a point *t* is computed by the number of edges *t* covered in the tree until the traversal is terminated.

k(m): average of *p(t)* for a specified *m* (see Equation 4.3 below).

E(p(t)): mean of *p(t)* from a group of isolation trees.

Then,

$$s(t,m) = 2^{-\frac{E(p(t))}{k(m)}} \tag{4.2}$$

where,

$$k(m) = 2p(m-1) - \frac{2(m-1)}{m} \tag{4.3}$$

Using the anomaly score, we can make the following assessments:

a) Values close to 1 are considered an anomaly
b) Values smaller than 0.5 are considered normal

In training, Isolation Forest creates binary search trees for different features. They are called Isolation Trees. The test phase entails the following steps:

- Find the path length of the data point under test from all the trained Isolation Trees and find the average path length. The higher the path length, the more normal the point, and vice-versa.
- Based on the average path length, calculate the anomaly score.
- Based on the anomaly score, we decide whether the given sample is anomalous or not by choosing a value of contamination. The contamination was tuned to arrive at the Equal Error Rate.

- ***k-Nearest Neighbors***

k–Nearest Neighbor (k-NN) is a simple supervised classification algorithm that can be applied to both classification and regression problems. For each query sample, it finds the k number of nearest samples from the train set in the feature space according to a distance metric. We train a k-NN classifier model on our dataset as a multi-class classification model assigning a label of target identity for the test sample. We divide the entire dataset into training and test sets randomly at 85:15 proportion and classify the test samples and record the FAR, FRR, and EER of the model for evaluation. By tuning the hyper-parameters using the validation set, we used k=5 in all our experiments with k-NN. For the distance metric, we used the Minkowski distance metric which is computed as follows.

Let $X = (x_1, x_2, \dots, x_n)$ and $Y = (y_1, y_2, \dots, y_n)$ be the two points in the feature space. Then the Minkowski distance of order p between those two points is given by:

$$D(X,Y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p\right)^{\frac{1}{p}} \tag{4.4}$$

A suitable order (p) is chosen by experiment which gives the lowest Equal Error Rate.

- ***Radial Support Vector Machine***

Support Vector Machines are primarily used for binary classification problems. They generate the hyperplanes to separate/classify data in some n-dimensional feature space into different regions. The non-linearity in the data are accommodated into SVM to work well on high dimensional and linearly inseparable data using a mechanism called the kernel trick.

The kernel trick is based on the idea that the SVM need not compute the exact form of the non-linear transformations applied to each data point to increase its dimensionality, as long as we have a way to compute the transformed inner products directly from the original inner products and utilize them in the SVM. The kernel function is the function which computes the transformed inner products of the factors from the original inner products.

In our experiments, we used the radial kernel function, which is of the form,

$$K(X,Y) = exp\left(-\gamma \sum_{j=1}^{p}\left(x_j - y_j\right)^2\right) \tag{4.6}$$

where, γ is the hyper-parameter that controls the smoothness of the decision boundary and in turn regularizes the model. The regularization strength of the model is inversely proportional to γ. We choose a suitable value for γ which gave the lowest Equal Error Rate in our experiments.

Generally, SVM don't support multi-class classification in its normal form. For multi-class classification, the basic SVM principle is utilized after breaking down the multi-class classification problem into smaller sub-problems, all of which are binary classification problems.

We train the *N* number of SVM classifiers, where *N* is the number of identities/classes in the dataset. In our case, it is the number of individuals to be authenticated. Each classifier learns the decision boundary between its specific class and the rest of the classes. For a new test sample, we compute the score on each classifier and decide the target class by combining all the scores.

- ***Fuzzification***

Behavioral biometrics, by their very nature, are subject to variations. One of the primary sources of the variations is the inexactness of human behavior itself. Other sources of variations could be external and environmental factors. For example, the user's hand could be affected by sanitizer, dust, oil or grease, different kinds of gloves, and so on. This can add variations to the input presented from the user during the training phase resulting in high false-positive cases. In such scenarios, the conventional machine learning based classifiers may not be decisive and fail to handle the test input because their network is not trained for all variable factors. To handle such a situation, we fuzzify the input to minimize the effect of variable factors on authentication accuracy.

A membership function for a fuzzy set A on the universe of discourse X is defined as $\mu_A: X \rightarrow [0,1]$, where each element of X is mapped to a value between 0 and 1. This value, called membership value or degree of membership, quantifies the grade of the membership of the element in X to the fuzzy set A.

In our case, we are doing authentication, so each class is an individual. We introduce an additional variable quantifying the degree of membership of a candidate to a class representing an individual. In our case, the primary external variables we considered were wet, dry, and gloved hands. During the training phase, the degree of membership of a candidate was taken as input based on the distance of the candidate feature vector from the mean feature vector of the individual. This is done by first recording all the training candidate feature vectors for every individual, and then calculating the degree of membership of each candidate feature vector based on its distance from the mean feature vector. The degree of membership becomes an additional dimension of the vector. The enhanced feature vectors along with the degree of membership dimension are then passed to the SVM for finding hyper-planes of optimal separation.

During testing, we first measure the distance of the test feature vector from the mean feature vector of the nearest individual. From this, we calculate the degree of membership of the test feature vector. The modified test feature vector including the degree of membership is then passed to the classifier authentication module. The training and test algorithm is shown in Figure 4.4.

Let a_i represent the i^{th} feature vector for an individual and n_{train} represent the number of training data samples. Then the mean feature vector $\overline{a}$ is:

$$\overline{a} = \frac{\sum_i a_i}{n_{train}} \tag{4.7}$$

Let D be the distance of the furthest feature vector from the mean feature vector $\overline{a}$.

$$D = Max_i(\overline{a} - a_i) \tag{4.8}$$

Let d_i be the distance of the i^{th} feature vector for an individual from the mean feature vector $\overline{a}$.

$$d_i = \overline{a} - a_i \tag{4.9}$$

Then the membership m_i of that feature vector was calculated from the following expression.

$$m_i = 1 - \frac{d_i}{2D} \tag{4.10}$$

The range of d_i/D is $[0, 1]$. The range of m_i is $[0.5, 1]$. The minimum membership value of the training feature vectors is 50% which happens for the feature vector with the largest distance from the mean feature vector $\overline{a}$. All the other feature vectors have higher membership values with reducing distance from the mean feature vector$\overline{a}$. The highest membership value will be for the feature vector nearest to the mean feature vector $\overline{a}$.

The membership value m_i is then added to the feature vector a_i. The SVM classifier is trained using the enhanced feature vectors.

During testing, the membership value is calculated for the test feature vector from its distance to the mean feature vector $\overline{a}$ and the test vector is enhanced by adding the membership value. Then, the enhanced test feature vector is passed to the SVM for classification.

The authentication module makes the authentication decision that the claimant sample matches with the owner of the device. In this case, the claimant user fuzzified features are matched against the stored model, and the degree of membership for each class is

computed. In the matching process, the degree of membership is compared to the threshold value; if the membership degree is higher than the threshold value, the sample is classified as genuine, otherwise, it is classified as an imposter. The threshold value is tuned to give high accuracy and a low error rate. We found that this proposed Fuzzification with SVM classifier helps to significantly reduce the equal error rate for the authentication system.

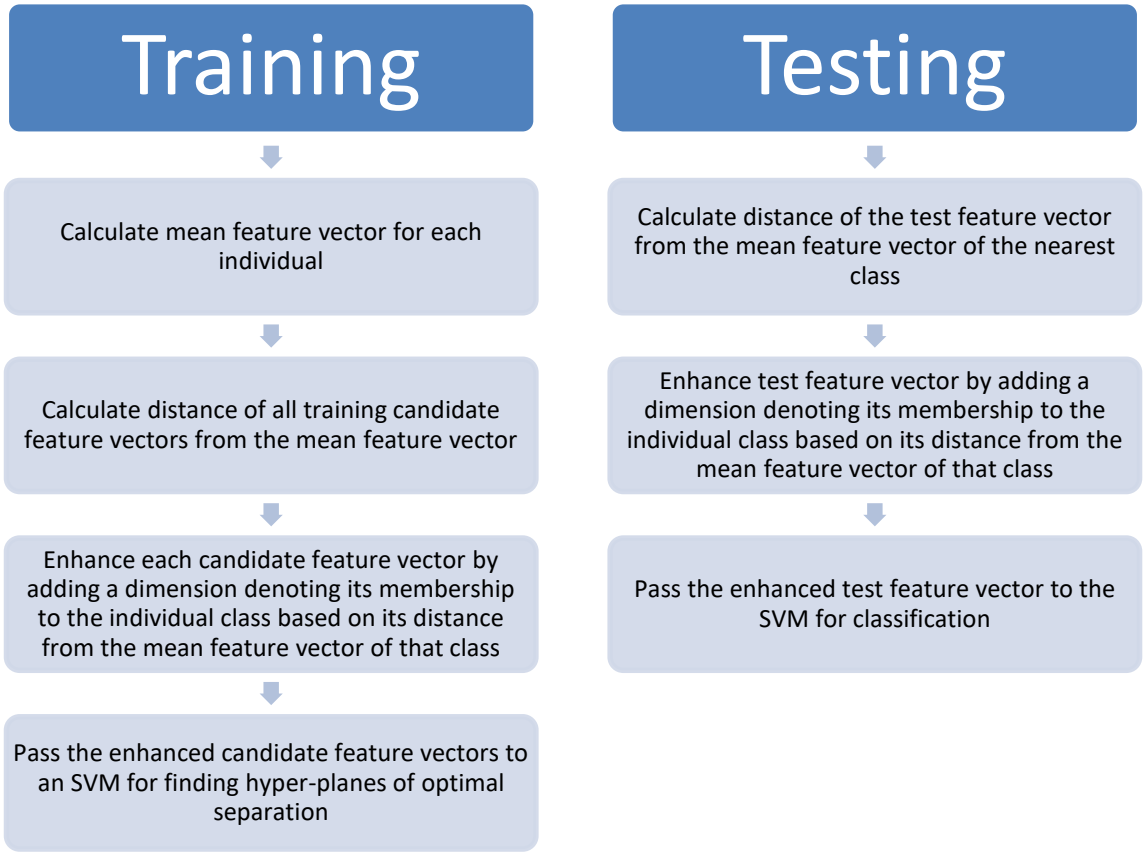

Figure 4.4 Training and test algorithm used in our fuzzy SVM based authentication system.

4.3 Evaluation Methodology

We evaluate the accuracy of the proposed multimodal behavioral biometric system based on touchscreen Swipe and keystroke dynamics. We employ different binary classifiers such as Isolation Forest, k-NN, SVM, and fuzzy logic based SVM Classifier.

First, we divided the subjects into two parts: one was treated as the genuine subject and the other as the imposter subject. In our experiment, a total of 197 users participated; for every mobile device, one user is the owner of the device, and his/her samples are labeled as genuine and the remaining 196 users are labeled as imposters. We partitioned the collected dataset into training and test sets in a ratio of 85:15 and trained these classifiers on the training set. We generated four models using four different training sets for different postures: sitting, standing, walking, and all postures. Both the training and the test sets contained all the variations in the external factors (dry hands, wet hands, and hands with gloves). Finally, based on the decision, the evaluation metric values were computed on the test data.

We have four sets of data samples: a genuine training set, a genuine testing set, an imposter training set, and an imposter testing set. Once we have acquired the sample sets, they are used to evaluate the above metrics of the proposed multimodal behavioral biometric system. In the experiments with fuzzy classifier with SVM, users presented the inputs with non-trained / unseen external inputs such as hands with a sanitizer.

The accuracy of the proposed multimodal behavioral biometric system was measured using the following metrics:

a) The false rejection rate (FRR) is defined as the probability of a genuine user being rejected as an impostor. It is measured as the fraction of the genuine user's score below the predefined threshold.
b) The false acceptance rate (FAR) is defined as the probability of an impostor being accepted as a genuine user. It is measured as the fraction of the impostor score (a matching score that involves comparing two biometric samples originating from different users) exceeding the predefined threshold.

The equal error rate (EER) is used to determine the accuracy of the biometric system. When both FAR and FRR rates are equal, the intersection point is the EER. The lower the value of EER, the higher is the precision of the biometric system.

4.4 Experimental Results

In experimental results, the EER value was computed for the Isolation Forest Classifier from the graph for FAR and FRR values while controlling the 'ease of acceptance' of the isolation forest by varying the contamination factor, and the intersection point in the graph between FAR and FRR lines gives us the EER value as shown in Figure 4.5.

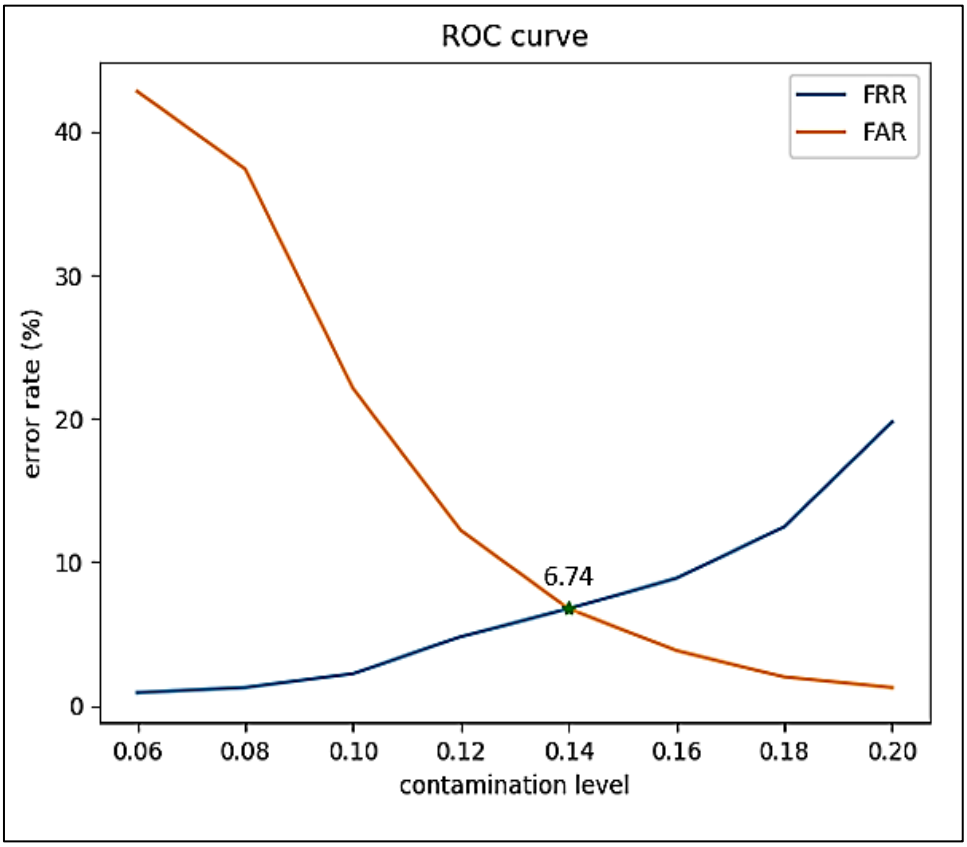

Figure 4.5: ROC curve plot of suggested system

From Figure 4.5 the equal error rate with isolation forest is obtained at around 6.74% for authentication. These results are obtained on the combined dataset with and without the presence of external factors such as hand gloves, wet hands, etc. for both training and validation. We conducted experiments by including individual positions in the dataset separately as well as the complete dataset with all three positions.

We also experiment with other classifiers such as k-NN and SVM and summarize our results in Table 4.2.

Table 4.2: Results of proposed Multimodal Behavioral Biometric system with Isolation Forest, k-NN, and SVM classifiers

Classifier	Posture	Average EER (%)
Isolation Forest	Standing	8.65
	Sitting	6.55
	Walking	8.92
	All	6.74
k-NN	Standing	4.05
	Sitting	4.08
	Walking	4.76
	All	1.58
SVM	Standing	2.04
	Sitting	0.68
	Walking	2.70
	All	0.45

As per the results mentioned in Table 4.2, we observed that SVM gave the best result of 0.45% equal error rate when including all the positions (Sitting, walking, and standing). SVM is closely followed by k-NN at 1.58% and then isolation forest at 6.74% EER. The error rates are shown for each posture setting as shown in Figure 4.6. Classifiers gave the best results when all the positions are included except for the isolation forest which gave the best result with the 'Sitting' position. This shows that the presence of samples of each identity in diverse positions helps to form precise decision boundaries for that identity which further increases the identification accuracy. We note that both touch swipe and keystroke dynamics for all the subjects were considered in the dataset to achieve the results. Further, we observe that the results obtained in the 'Sitting' position are better than other positions for all the classifiers as expected because the users are generally more stable while in the sitting position and the variance among the different samples obtained will be minimum.

On contrary, the users will be most unstable while walking and so the variance of the samples would be considerably high, and thus walking position accuracy is the lowest.

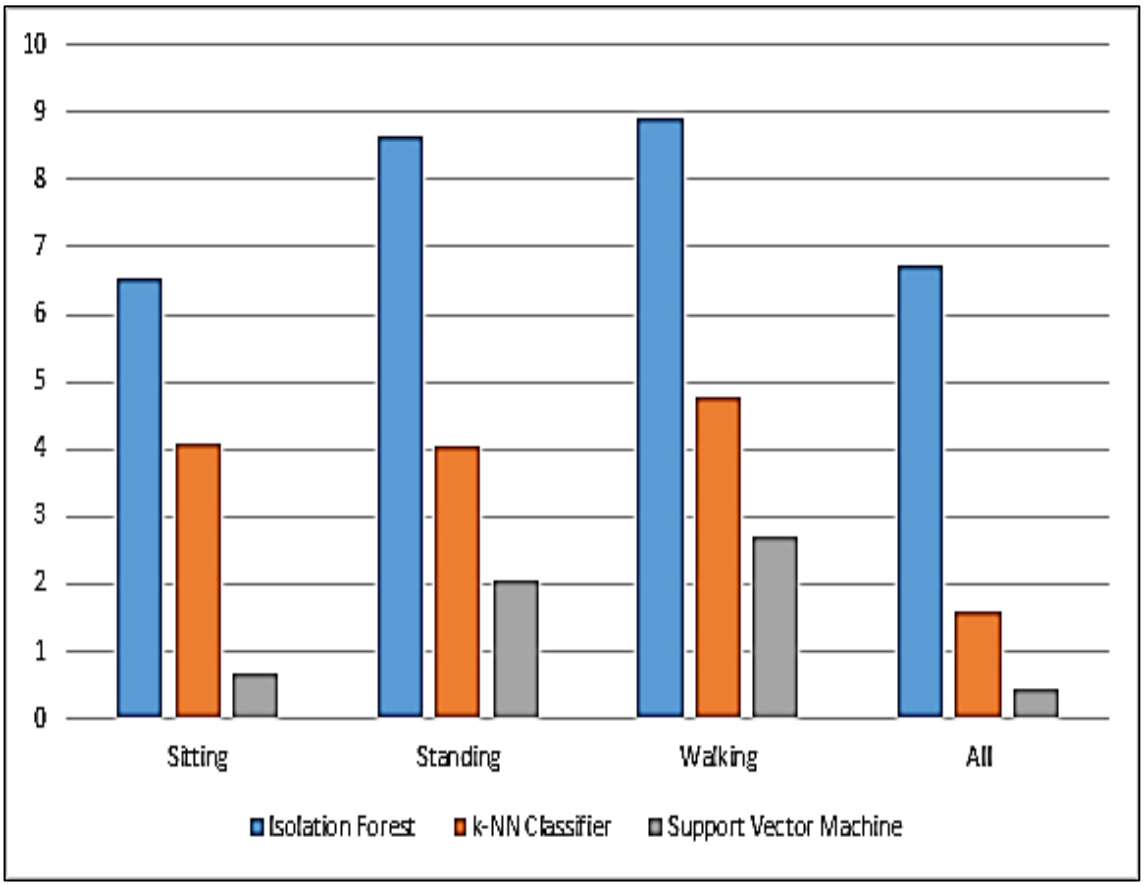

Figure 4.6: Performance of classifiers for each position (Sitting, Standing, Walking and All combined)

We also quantitatively compared our work with the recent existing methods utilizing touch-swipe and keystroke dynamics behavioral patterns for authentication/verification in Table 4.3.

Table 4.3: Comparison with existing work

Study	Work Description	Modality	Average ERR
N. L. Clarke *et al.* [67]	Authentication using keystroke dynamics	keystroke	9% to 16%
Hwang *et. al* [70]	Arthematics rhythms with Cues	keystroke	13%
Nan Zheng [69]	Tapping patterns	Touch	3.65%
Wang Y. *et al.* [111]	Support Vector Machine	keystroke	8.70%
Meng *et al.* [83]	Neural Network with PSO	Touch gestures	2.92%
Pin Shen Teh *et al.* [77]	Gaussian, Z-Score, Standard deviation	Touch	8.50%
Ka-Wing Tse *et al.* [78]	RNN	Touch, keystroke	Accuracy 83.9%
Proposed work	SVM	Touch, Keystroke	0.45%
	k-Nearest Neighbor		1.58%
	Isolation Forest		6.74%

However, in a real case scenario, users can try to access the authentication system in presence of varied types of external factors. For example, in the current situation of the COVID19 pandemic, the user may likely try to authenticate his mobile by swiping/typing a passcode with hands containing sanitizer, dirt or dust, etc. In such cases, the typing or swiping behavioral characteristics may vary slightly due to the presence of such external factors. So, there is a need for a system that can recognize the true owner/ imposter even when the behavioral patterns are slightly varied because of external factors. Since training the model on the dataset under the influence of all possible external factors is infeasible and impractical, we aim to explore the neighborhood similarities in feature space to solve this problem. We argue that the behavioral features influenced by an unknown external factor 'a', will be in near neighborhood space to the behavioral features of 'closely related' external factor 'b'. For example, the behavioral patterns influenced by sanitized hands will be in the near neighborhood to the patterns influenced by wet hands (from water) in the feature space because of the closely related physical properties of sanitizer and water. We utilize this contextual neighborhood to train the model to classify into fuzzy sets instead of sharp binary sets such that it incorporates relations between the 'closely related' external factors. For this reason, we train a fuzzy logic classifier on the collected dataset with samples affected by only two external factors namely wet hands and gloves.

We then utilized the trained fuzzy logic classifier to classify samples of the same individuals affected by an untrained external factor like hands with sanitizer as positive/negative. The results on the untrained external factor are summarized in Table 4.4. We observe that the error rates of the traditional machine learning based classifiers increased when trying to evaluate an untrained external factor case. The fuzzy with SVM classifier gave the best evaluation results on untrained cases with a 6.46% error rate. This shows that our approach can minimize the effect of external factors like sanitizer, gloves, etc. which are common during the pandemic times like COVID-19 by making use of fuzzy logic.

Table 4.4: Validation results of the authentication system in the presence of untrained external factors: Hands with sanitizer

Classifier	Average EER (%)
Isolation Forest	22.4
k-NN Classifier	18.25
SVM	16.5
Fuzzy Membership with SVM Classifier	6.46

4.5 Conclusion

This research work investigates the situations in which fingerprints cannot be utilized due to hand gloves and hence presents an alternative biometric system using the multimodal touchscreen swipe and keystroke dynamics pattern. We propose a Hand Glove mode of authentication where the system will automatically be triggered to authenticate a user based on touchscreen swipe and keystroke dynamics patterns. The proposed system incorporates touchscreen swipe and typing patterns as a security layer for authentication to increase the total security of the system. We demonstrate use of a fuzzy classification with SVM to incorporate fuzziness in the authentication system, thereby reducing the effects of unknown external factors such as dust or sanitized hands in user authentication. Our experimental results suggest that the proposed multimodal biometrics system can operate with high accuracy and that the Hand Glove mode of authentication has a very limited of hand gloves on the accuracy of the authentication system. We experimented with multiple commonly used machine learning based classification algorithms to obtain the best authentication accuracy of 99.55% with 197 users on the Samsung Galaxy S20. This proposed work provides a framework for the implementation of a multimodal approach for user authentication in smartphones using touch swipe and keystroke patterns of users. It also provides extensive experimentation on a dataset created using a smartphone (Samsung Galaxy S20). The experimental results established the usability and importance of the presented work for smartphones.

We use a fuzzy network to learn the patterns in this multimodal system to reduce the effects of hands with sanitizer in user authentication and achieved 93.5% accuracy. The

results are achieved with 197 users; however, it is sufficient to conclude the potential of the presented work for user authentication in smartphones. More extensive experiments on large smartphone datasets with more variations in acquisition could be a future scope. To further increase the scope of this work, other modalities such as application usage patterns, battery charging patterns, and walking patterns of an individual can be explored as future research work for smartphone security under a multimodal behavioral biometric system.

We are able to demonstrate that a multimodal behavioural biometric classifier based on touch swipe, and keystroke dynamics can be suitable for authentication in low security applications. We are also able to demonstrate that a multimodal biometric classifier performs better than a single mode biometric classifier.

One of the key takeaways from our experiments is the power of fuzzification of features to deal with variations in the external factors and the environment. We find that fuzzification reduces the error rate of touch swipe and keystroke dynamics authentication with wet hands or hands with gloves from 16.5% for a non-fuzzified SVM model, to 6.46% for a fuzzified SVM model.

Publication:

The work discussed in this chapter is published in:
Amitabh Thapliyal, Om Prakash Verma, Amioy Kumar, “Multimodal Behavioral Biometric Authentication in Smartphones for COVID-19 Pandemic”, *International Journal of Electrical and Computer Engineering Systems*, ISSN: 1847-7003, Vol 13, Issue 9, 2022.

Chapter 5: Behavioral Biometric Authentication System for Mobile Phones Based on Keystroke Dynamics

5.1 Introduction

In the last decade, the use of mobile phones has increased tremendously. The growth of mobile phones has increased over time with rapid changes in technology like network growth from 2G to 5G and handset evolution from feature phones to powerful smartphones. As per a report from GSMA [112], there are 5.2 billion subscribers globally. The growth of mobile phones has also increased mobile related thefts with 183 smartphones stolen every day between March 2015 and March 2016 in the UK itself [113]. Mobile phones have become high risk defrauding targets as most of the transactions nowadays take place through them, right from the management of bank accounts to the buying and selling of stocks. This raises potential questions regarding the security of mobile phones [114], [115].

Nowadays, different authentication approaches have been used on handheld devices to ensure the security of content [116], [117]. Some of them are password, fingerprint, iris, face, and pattern. These approaches are now the mainstream authentication techniques used across all handheld and portable devices. The demerit of the existing approaches is that they are prone to attacks like shoulder surfing, guessing attacks, brute force attacks, and dictionary attacks. A relatively newer authentication method, that is pattern based authentication in touchscreen devices, is also prone to finger marks and smudges which can be used to lift the pattern sequence. As per a recent report from counterpoint research, there is going to be a huge demand for the feature phone market as mentioned in [118]. Globally, the feature phone segment is forecast to generate around $16 billion US dollars cumulatively in wholesale hardware revenues over the next three years. The affordability of feature phones is one of the major reasons why feature phones are the preferred mobile phone in many segments of the population in developing countries like India, Pakistan, , and Bangladesh. The market reports from counterpoint and shipment opportunity for feature phones there is a strong need to have a robust security system [119], [120] without any additional hardware cost. Deploying the fingerprint scanner or iris to the feature phone requires additional cost, memory, and high computing power in the device which

tends to increase the cost of the phone, therefore, such a system is not a feasible option for a feature phone.

It has been observed that existing security authentication mechanisms in feature phones are based on the personal identification number (PIN) or password characters. Current security authentication provided in feature phones is prone to security attacks from imposters and fraudulent attackers.

In this work, we have developed an authentication solution based on behavioral keystroke dynamics from the user's learned machine learning model for feature phones that does not require any additional hardware support. The basic concept with keystroke dynamics is the capacity of the method to understand the patterns like typing patterns during keyboard usage from the individual and then use this as a parameter to verify the user. In the proposed work, the typing pattern (keystroke modality) of the user is learned with the k-nearest neighbors (k-NN) and fuzzy logic. The experimental data was collected on Samsung On7 Pro C3590 and the model was trained on the desktop PC Windows 10, by dividing user data into training and validation sets.

5.2 Keystroke Dynamics for Feature Phones

The behavioral biometric [121], [122] technology proposed in this research work by analyzing the typing pattern of the user which is also known as keystroke dynamics.

The block diagram of the proposed keystroke dynamics authentication system is shown in Figure 5.1. The whole process of keystroke dynamics is divided into the following three steps: 1) data collection, 2) model training, and 3) authentication.

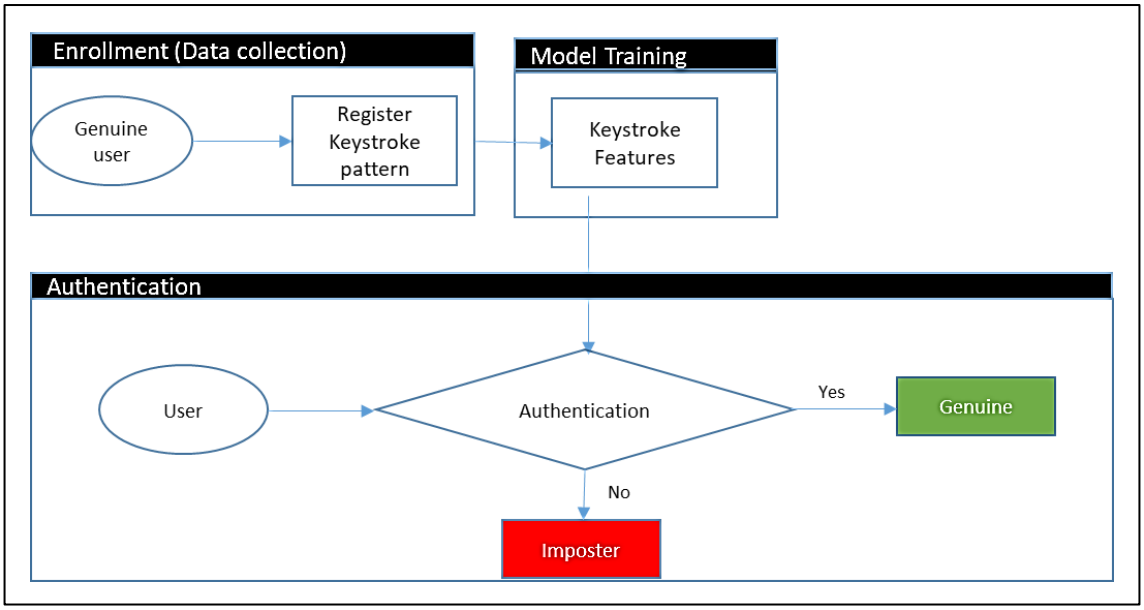

Figure 5.1: Keystroke dynamics based authentication system

5.2.1 Data Collection

In the proposed study, a total of 25 users aged between 22 to 42 years, have participated in the experiment. To capture the keystroke data input from the users, we have developed a mobile application for Samsung On7 Pro C3590. In our experiments, the 4-digit password "1976" was used and users were asked to enter the password 60-times during the enrolment phase at the Samsung India Noida R&D center. The data collection was done in two separate sessions for each user. The entire enrolment process took one week to collect the sample data from all the users. The keystroke data acquisition step comprises building character transition lists for the particular chosen keyword. The duration of key-presses between every two characters is stored. This proposed work was designed to classify the users in feature phones based on the typing patterns while entering the 4-digit PIN key, which is based on the hold-time of key press, flight time, and the total time entering the PIN. Our work utilizes the following mentioned parameters while capturing the data from the user: 1) keystroke latency (flight time): time taken between two consecutive keystrokes, 2) hold-time: time to press and release a key, and 3) total time: time to press first key press and last key release. The components of features that are utilized in this work are shown in Figure 5.2.

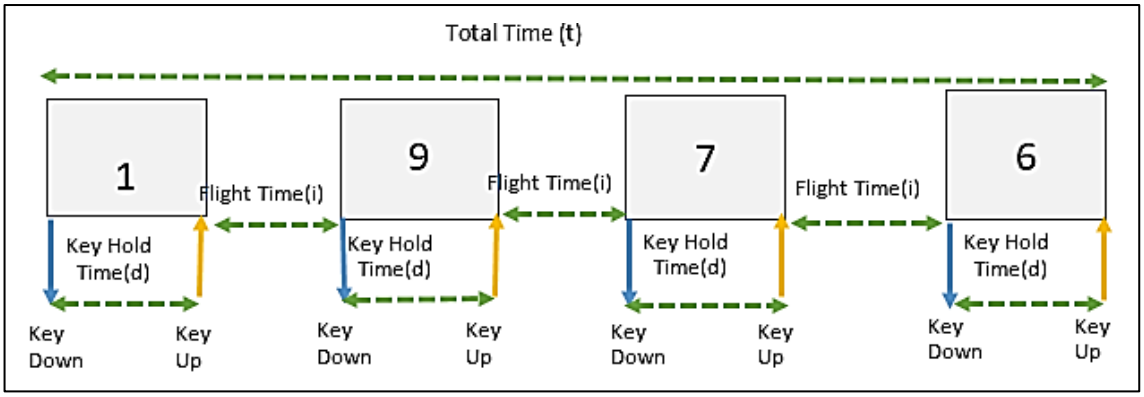

Figure 5.2: Keystroke dynamics features

For the keyword "1976," the input captured during enrolment is in the following format, with 8 features $[i_1, i_2, i_3, d_1, d_2, d_3, d_4, t]$. Where,

d_k : *Time of press for key (in milliseconds)*

i_k : *Time between first key release and next key press(in milliseconds)*

t : *Total time from first key press to last key release (in milliseconds)*

5.2.2 Model Training

With the help of data collected during the enrolment phase typing pattern is recorded for a particular password, after which the model is trained using k-NN and fuzzy logic. Overall, 8 features are collected as shown in Figure 5.2 including hold time, flight time, and total time from the first key to the last key release for the keyword "1976". The input features obtained are then passed through the k-NN model and the fuzzy logic based training model separately and both the models are then trained using the given input features.

Figure 5.3 shows how the authentication values are obtained separately from both models and combined to get the final authentication value.

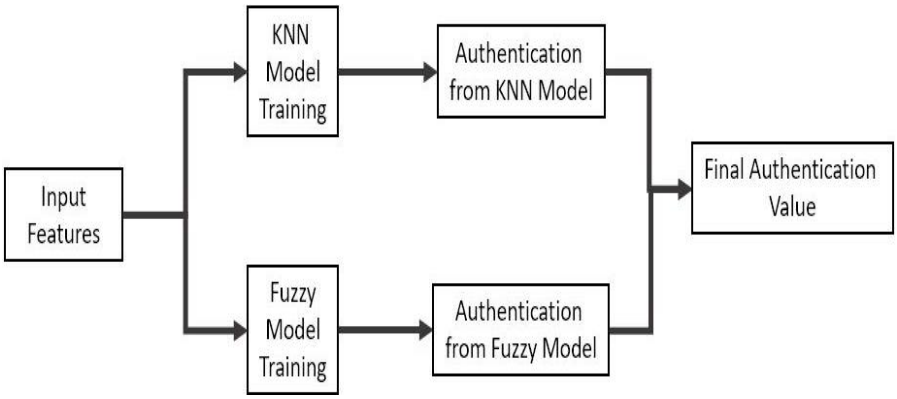

Figure 5.3: Proposed Keystroke Model Architecture based on k-NN and Fuzzy Logic

5.2.2.1 k-NN

The Nearest Neighbours (NN) algorithm is widely used for conventional classification problems: namely, where the model predicts a class from the trained classes for the each of the test candidates. We used k-Nearest Neighbors (k-NN) algorithm as a classification method because of its wide applicability in pattern recognition and classification.

k-NN searches for the feature value's k nearest neighbors. We have used 5-NN to find the five closest neighbors of the user's typing patterns. The difference between the claimed user typing pattern and the primary user features is determined in this algorithm using Euclidean distance. The Euclidean disstance is the straight-line segment between two locations in space. It assists in discovering the shortest path between two input feature vectors along the line segment connecting them. Euclidean distances between all points are determined, and the points with the smallest space are chosen as the nearest. Figure 5.4 shows how Euclidean distance is used in k-NN in a pictorial representation.

$$d(z, z') = \sqrt{(z_1 - z'_1)^2 + (z_2 - z'_2)^2 + \cdots + (z_n - z'_n)^2} \quad (5.1)$$

where,

$z : Training\ Sample\ Value$

$z' : Test\ Sample\ Value$

$d(z, z') : Computes\ the\ Euclidean\ distance$

In the Nearest-Neighbor algorithm, the number of degrees of freedom determines the number of dimensions in hyper-dimensional space. Each set of identifying features of typing pattern is one point in that hyper-dimensional space.

We collected multiple inputs to train the model from each person to train the model. We have multiple points plotted for each class (every class is a person in our case because our problem is of person identification and authentication) once the classifier training is complete.

Our features include hold time, flight time, and total time, and the model is trained for a 4-digit keyword like “1976”. As shown in Figure 5.5, the model is trained using a data set that includes training samples, genuine or true cases, and imposter cases.

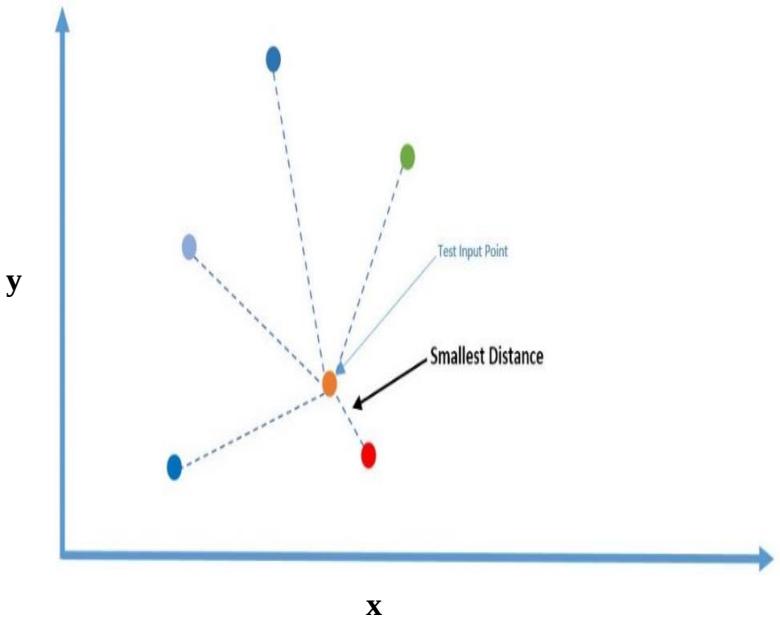

Figure 5.4: k-NN using Euclidean Distance

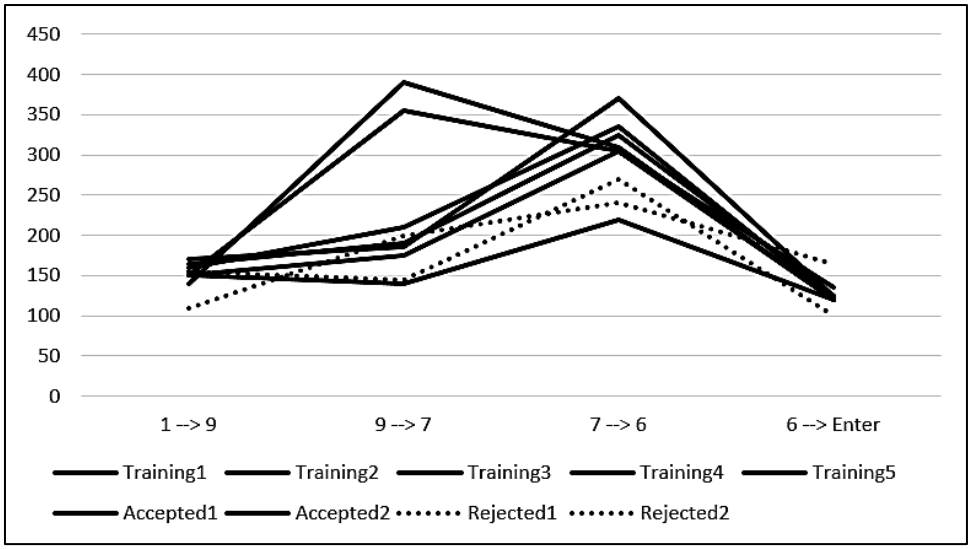

Figure 5.5: Training - keystroke dynamics

5.2.2.2 Fuzzy Logic

Fuzzy means something that does not have crisp values. Fuzzy logic is used in the cases where a crisp definition cannot be provided for a quantity. As an example, a user when typing can have variable typing speeds, classified as fast, slow, or normal. A crisp definition of the quantity where the value changes from fast to normal or normal to slow cannot be defined in this case. Figure 5.6 shows the frequency of typing speed timings for a typical user, the normal typing speed has a maximum frequency that occurs in day-to-day life while typing, while the frequency decreases as moving towards timings that are categorized as fast or slow. The actual values of timing will vary from person to person and a crisp range cannot be defined between these three classes. Such classes introduce a degree of fuzziness and using methods such as the k-NN algorithm fails to reliably classify two users with similar typing speeds. Such impreciseness can be solved by employing the ideas of fuzzy Logic. Fuzzy logic is used in authentication systems based on behavioral biometrics to provide enhanced security. This is because, in the case of biometrics, a lot of data from different users can be similar to one another. In the case of a keystroke dynamics-based authentication system, the input features are keystroke timings which can vary for a single user and may or may not overlap with another user's timings. From Figure 5.6 we can see that it is not possible to define a single value as fast or slow based on typing speed of a given user. As explained in Figure 5.7 in the fuzzy logic model, the input properties of the keystroke timings that are initially transformed into the

fuzzified input that are then used by the inference engine, which is in charge of calculating the output for a given input based on learned data. Using the input keystroke timings, the rule base is generated which is used to determine the timing similarities for a test input. Similarity gives a degree of closeness between one typing speed timing against the timings from learned users and is calculated by fuzzifying the test input. Finally, the fuzzy output can be converted to the crisp authentication value using the available de-fuzzification functions such as the centroid method, or the normal max value.

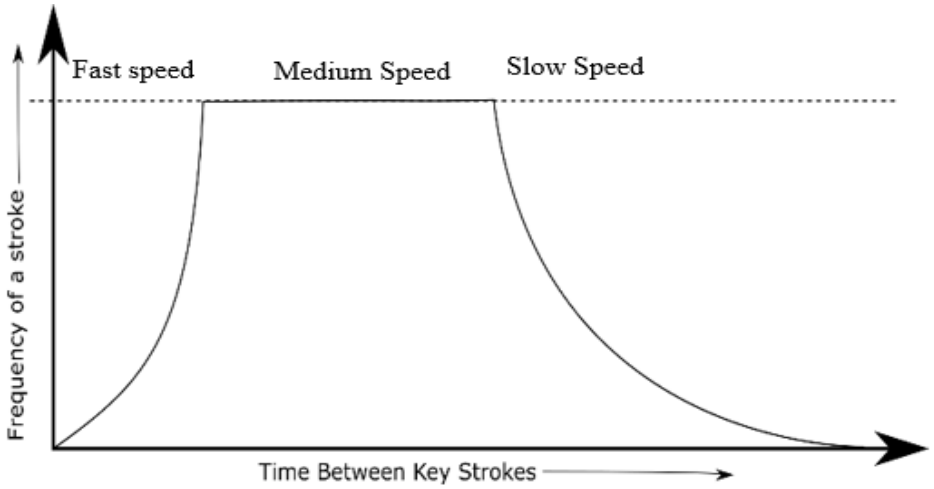

Figure 5.6: Timings of a participant's keystrokes

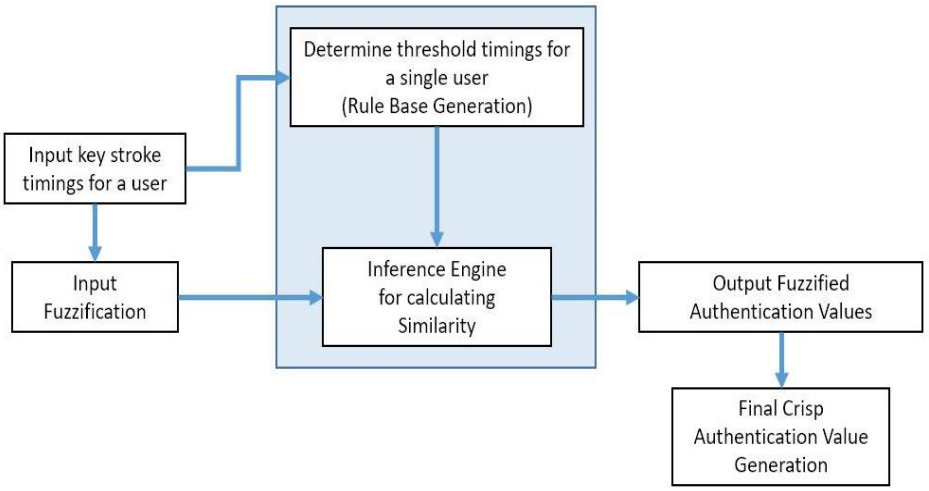

Figure 5.7: Function of the proposed keystroke dynamics fuzzy logic model

- **Rule Base for User Classification**

  The input to the fuzzy system are the keystroke timings from a user collected over time; these inputs need to be converted to their fuzzified forms before they are passed through the inference engine for further processing.

  The following timings are taken into consideration when calculating the fuzzification function input:

  - Time of press for key (hold time: d_k)
  - Time between first key release and next keypress (flight time: i_k)
  - Total time from the first keypress to the last key release (t)

  The feature set for the four-character keyword "1976" is as follows: $[i_1, i_2, i_3, d_1, d_2, d_3, d_4, t]$. As the number of characters utilized in learning expands, this feature set, which is currently restricted to four-character keywords, may change. In this case, i_1, i_2, and i_3 denote the time interval between releasing a key and stroking the following key (in milliseconds). Likewise, the values d_1, d_2, d_3, and d_4 indicate the duration of pressing the key. Finally, the final number represents the time interval between pressing the first key and releasing the last key (in milliseconds).

  Multiple feature sets, say n, are obtained for a given user during the learning phase. The values were averaged to obtain an average typing time for a single user for each of the three types of timings. We get the following 3 values for each input tuple for a single user.

$$(d, i, t) = (\sum_{x=1}^{\text{Number of key press (4)}} d_x, \sum_{y=1}^{\text{Intervals between key press (3)}} i_y, t) \quad (5.2)$$

$$d_{avg} = \frac{\sum_{k=0}^{n} d_k}{n} \quad (5.3)$$

$$i_{avg} = \frac{\sum_{k=0}^{n} i_k}{n} \quad (5.4)$$

$$t_{avg} = \frac{\sum_{k=0}^{n} t_k}{n} \quad (5.5)$$

where,

n : total number of input timing feature sets for a single user obtained while training

Finally, we calculate an upper and lower limit of the typing speeds that can be used as a rough estimate of the typing timing of a single user in day-to-day life. Threshold t_l and t_u are defined for every three inputs which give a rough estimate of the minimum and maximum value of timing for a single user and is calculated as a multiple of the standard deviation from the average value. This methodology helps to discard any outliers that may have occurred during data collection:

The upper limit (u) and lower limit (l),

For *d*:

$$t_{ld} = d_{avg} - m * \sigma(d) \quad (5.6)$$

$$t_{ud} = d_{avg} + m * \sigma(d) \quad (5.7)$$

For *i*:

$$t_{li} = i_{avg} - m * \sigma(i) \quad (5.8)$$

$$t_{ui} = i_{avg} + m * \sigma(i) \quad (5.9)$$

For *t*:

$$t_{lt} = t_{avg} - m * \sigma(t) \quad (5.10)$$

$$t_{ut} = t_{avg} + m * \sigma(t) \quad (5.11)$$

Here, $m * \sigma(d)$ defines the m^{th} standard deviation around the average value. t_{lk} and t_{uk} represents the lower and upper learned threshold timings for the user, where k is d,i,t. These values of the threshold are used during the input fuzzification phase to generate an input membership function for user input.

m is commonly taken to be 3. However, for our purposes, we have taken the value of m to be 1. This is because we found that in the case of typing, it is possible that multiple users may have a high degree of overlap in their timings and may lead to false acceptance.

- **Input Fuzzification**

The obtained threshold values in the previous step (Equation 5.6 to 5.11) are then used to generate an input membership function. The input membership function for the classes fast, normal, and slow based on the password input speed is defined as:

$$\mu_k = \begin{cases} \frac{0}{fast} + \frac{1}{normal} + \frac{0}{slow}, if\ t_{lk} \leq\ t_k \leq t_{uk} \\ \frac{\left(1-\frac{1}{|t_k - t_{lk}|}\right)}{fast} + \frac{\frac{1}{|t_k - t_{lk}|}}{normal} + \frac{0}{slow}, if\ t_k < t_{lk} \\ \frac{0}{fast} + \frac{\frac{1}{|t_k - t_{uk}|}}{normal} + \frac{1-\frac{1}{|t_k - t_{uk}|}}{slow}, if\ t_k > t_{uk} \end{cases} \quad (5.12)$$

where, k= d, i, and t and the membership function is calculated for d, i, and t respectively. The membership function calculations are partitioned based on the thresholds. The membership function will have value 1 for normal class when the timings are between the upper and lower threshold value and zero for fast and slow classes. Similarly for cases when the timing is less than or greater than the threshold the degree of membership is calculated as shown in (5.12).

For any incoming test input $[t_{i1}, t_{i2}, t_{i3}, t_{d1}, t_{d2}, t_{d3}, t_{d4}, t_t]$, (d, i, t) is calculated as shown previously in (5.2). The membership values are calculated for three values d, i, and t, using the membership function as mentioned in (5.12). For an incoming test input, we have obtained three membership functions μ_d, μ_i and μ_t.

- **Inference Engine**

After converting the input to fuzzified values the inference engine uses the rule base to determine the similarity of the input to the learned user timings. Based on the closeness of the features to the limits of the authentication values, the similarity function can be defined as mentioned in (5.13).

$$s = \left(\frac{(\sum(\mu_k))}{3}\right) \tag{5.13}$$

where,

μ_k=input membership function with k=d, i, t

s =represents the similarity, 0<s<1

- **Fuzzy Output**

Finally, after applying keystroke dynamics timings and calculating the score, the inference engine will calculate the possible authentication value based on the current learned preferences, and based on a threshold of similarity 's_l', 's_u' the authentication values are generated, where s_l is the lower limit and s_u is the upper limit for similarity thresholds. A similarity value below 0.9 times s_l of means no authentication, while if the similarity is greater than 1.1 times of s_u the user is fully authenticated. Using a range instead of strict values of s_l and s_u helps to achieve the desired fuzziness by removing any strict crispiness in the threshold values. For in-between values of similarity, authentication values are defined using the output membership function as shown in (5.14). Values for the s_l and s_u can be set based on the learning from the previous data. Typical values for s_l are 0.3 to 0.5 and for s_u are 0.6 to 0.8. Similar, to the input function an output function for the classes NoAuth, ∂Auth, and FullAuth based on the fuzzy degree of authentication can be defined as shown in (5.14):

$$\mu_{op} = \begin{cases} \frac{0}{NoAuth} + \frac{1}{\partial Auth} + \frac{0}{FullAuth}, if(1.1 * s_l) < s \leq (0.9 * s_u) \\ \frac{1}{NoAuth} + \frac{0}{\partial Auth} + \frac{0}{FullAuth}, if s < s_l \\ \frac{0}{NoAuth} + \frac{0}{\partial Auth} + \frac{1}{FullAuth}, if s > s_u \\ \frac{1-\frac{s-s_l}{0.1*sl}}{NoAuth} + \frac{\frac{s-s_l}{0.1s_l}}{\partial Auth} + \frac{0}{FullAuth}, if s_l \leq s \leq 1.1 s_u \\ \frac{0}{NoAuth} + \frac{\frac{s_u-s}{0.1s_u}}{\partial Auth} + \frac{1-\frac{s_u-s}{0.1*s_u}}{FullAuth}, if 0.9 s_u \leq s \leq s_u \end{cases} \quad (5.14)$$

Based on the similarity value s, the membership function for the output $\mu_{op,}$ is calculated as shown in (5.14). Three classes have been defined for the authentication membership function: 1) no authentication, 2) partial/strict authentication, and 3) full authentication.

Instead of using crisp similarity thresholds for s_l and s_u the authentication membership values are generated by varying over a range which helps to achieve the desired fuzziness in the output membership function. The partial authentication decreases as the reliability/similarity increases while at the same time partial authentication membership increases, similarly in the case of partial and full authentication the membership values change gradually over a range of similarity values.

- **Crisp Output**

  From this approach, finally, the output can be converted into de-fuzzified output by taking the max of the three outputs as defined in (5.15).

$$Output = max\ (a, b, c) \quad (5.15)$$

  where,

  a : membership value for no authentication

  b : membership value for partial authentication

  c : membership value for full authentication

5.2.3 Authentication

There are two phases in the authentication system-enrolment and login phase. In the enrolment phase, the user keystroke dynamics are learned by the classifier. The final step after model training is authentication. Both the trained classifiers separately generate the authentication results which are then combined to generate the final authentication value. For authentication using k-NN classification, the trained classifier is used to calculate the nearest distance of the test sample from all of the training samples in that hyper-dimensional space. Once the nearest distance of the testing sample is calculated, it is checked with the permissible threshold value for that keyword and if the value is outside the limits of the threshold, the test sample is marked as an unrecognized typing pattern and the user is classified as an imposter.

For the fuzzy model, the similarity is calculated for the user and output authentication values are generated for the user. The user is considered to be authenticated if the authentication value is obtained as full authentication. A value of no or partial authentication is considered as no authentication in this case. Figure 5.8 shows a basic flow chart when an unknown user tries to access the mobile app or log in to the device. Even when the unknown user knows the password, the proposed system checks the behavioral characteristics of the keystroke input pattern and disallows access to the imposters. In this way it provides an additional layer of enhanced security.

When setting a 4-digit PIN, the timings for the user are captured feature vector is created with it. This feature vector is then passed through the k-NN classifier for training. The fuzzy classifier also learns threshold values for the lower and upper typing timings for the user. During the login phase when a similar timing feature vector is obtained for the candidate user and passed through the learned classifier to obtain the authentication output. Similarly, the input is converted to a fuzzified input, and then using the fuzzy inference converted to fuzzified output to finally obtain the crisp output result.

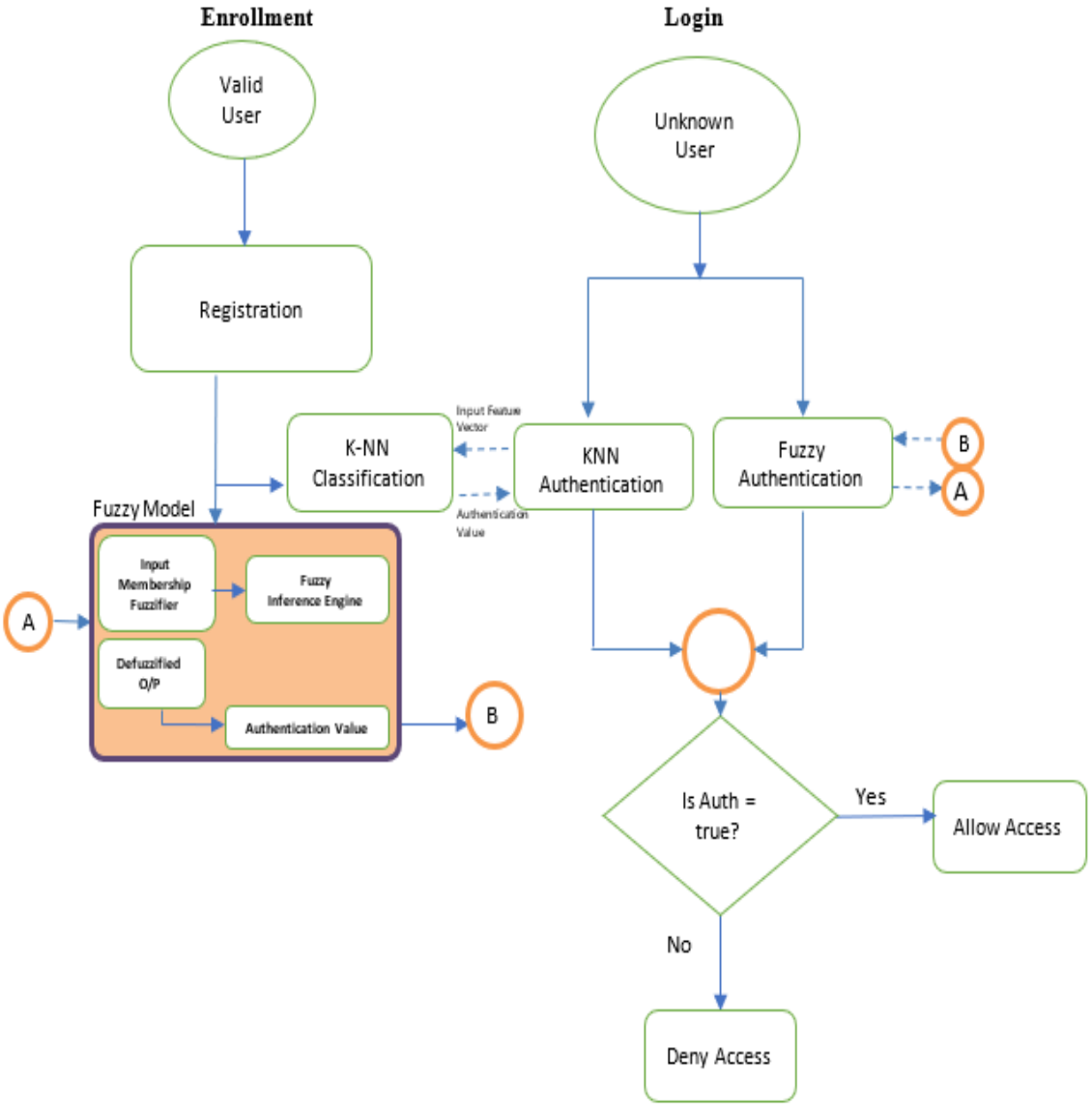

Figure 5.8: Schematic of proposed keystroke dynamics

5.3 Experiment Results

Experiments were performed for 25 different users with different acceptance thresholds. The authorized user keyed in a 4-digit PIN as input. We recorded 60 patterns from each user.

Table 5.1 represents a comparative evaluation of accuracy parameters performed between our proposed k-NN model and the improved version of our model when fuzzy logic is added alongside the k-NN classifier to find the final authentication value.

Table 5.1: Comparison of results k-NN Vs k-NN with Fuzzy Logic

User	Age	Gender	k-NN	k-NN with Fuzzy Logic
			EER	EER
User1	27	Male	1.45%	1.6%
User2	32	Male	3.65%	1.45%
User3	27	Female	9.25%	1.5%
User4	24	Female	2.25%	1.95%
User5	28	Female	9.25%	1.05%
User6	31	Male	2.20%	1.5%
User7	42	Male	3.00%	1.39%
User8	25	Male	1.45%	1.00%
User9	29	Male	5.25%	1.44%
User10	22	Male	5.90%	1.35%
User11	22	Female	2.9%	1.95%
User12	23	Female	2.1%	1.1%
User13	24	Female	1.6%	1.20%
User14	25	Male	2.6%	1.90%
User15	22	Male	1.46%	1.1%
User16	23	Female	2.19%	1.6%
User17	24	Female	2.0%	1.95%
User18	23	Male	2.3%	2.0%

User	Age	Gender	k-NN	k-NN with Fuzzy Logic
			EER	EER
User19	22	Male	2.04%	4.2%
User20	23	Female	0.8%	3.45%
User21	22	Male	2.9%	3.5%
User22	22	Male	1.4%	2.3%
User23	27	Female	1.75%	1.5%
User24	25	Male	3.0%	2.75%
User25	27	Male	3.0%	2.35%

In this performance evaluation, we find that using only the k-NN model over the biometric input features had a limitation in that the model does not take into account the variance in the keystroke latencies among the multiple attempts of the same user. From the tabulated experimental results, we can observe that the k-NN classifier has an average EER of 3.03%. This is the best result we found with our experiments when the value of k was set to 5.

We can observe that the EER has shown improvement and it decreased from 3.03% to 1.88% when fuzzy logic was applied along with k-NN. Out of 25 users, we observed that EER results for 12 of the users were less than 1.5%. Best results were observed for user8 with EER 1% with k-NN classifier combined with fuzzy logic.

In Figure 5.9 we have the ERR for 25 users with k-NN, as well as k-NN combined with fuzzy logic methods. It can be observed from our experiments that the k-NN classifier combined with fuzzy logic have performed better for most users and their results are superior to k-NN classifier alone.

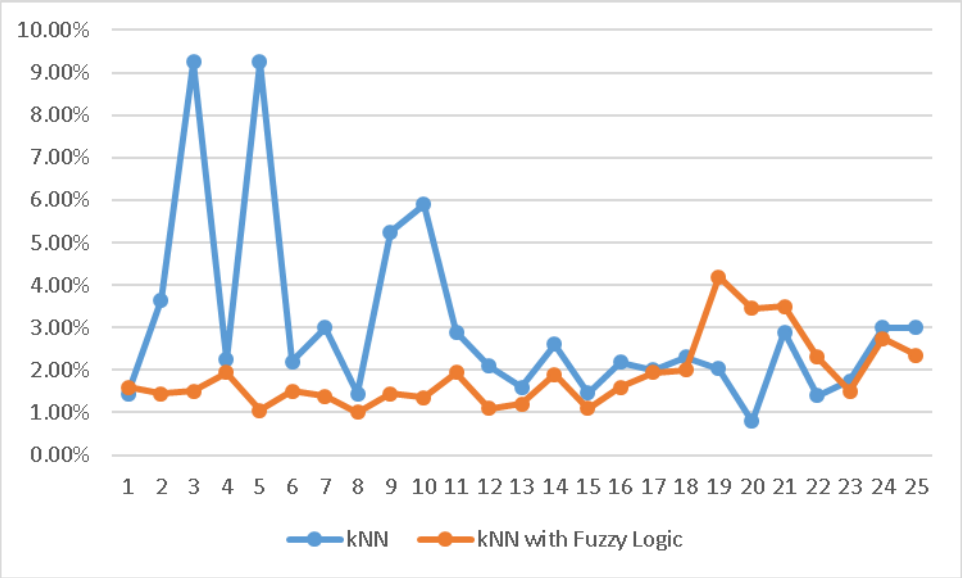

Figure 5.9: EER Results of proposed system (25 Users)

In Table 5.2 we summarize a comparison of our work with the existing work in keystroke dynamics literature. Our results are encouraging when viewed in comparison to previous work.

Table 5.2: Comparison with Existing Work

Study	Input Data	# Of Participants	# of Inputs in Training	Classifier	EER (%)
Clarke and Furnell [67]	4-digit PIN	32	30	Neural networks	12.8%
Hwang *et al.* [70]	4-digit PIN	10	5	Artificial rhythm with Cues	4% to 13%
Wang *et al*. [111]	4-digit PIN	104	20	Support vector machine (SVM)	8.70%
Chang *et al.* [123]	200 words	114	3	Statistical classifier	7.89%
Mondal *et al.* [124]	All keys of keyboard	53	$7*10^5$	ANN and CPANN	2.35%
Lee *et al*. [125]	6-digit PIN	22	100	Manhattan and Euclidean Distance	7.89%
Kim *et al*. [126]	6-digit PIN	6	100	Statistical classifier	13.44 %
Frolova *et al*. [127]	alphanumeric	15	30	LOF, Manhattan, and Euclidean ensemble	8.00%
Proposed Work	4-digit PIN	25	60	k-NN	3.07%
Proposed Work	4-digit PIN	25	60	k-NN with Fuzzy Logic	1.88%

We have been able to demonstrate improved authentication performance by employing a k-NN classifier with a fuzzy logic model to provide enhanced security when keystroke behavior data from different users can be overlapping.

5.4 Conclusion

Behavioral biometrics is set to play a crucial role in the future of authentication, and using keystroke modality can be one of the simplest ways to achieve this efficiently and precisely. With the current study, EER of 1.88% is achieved by a classification model with 25 users having 60 samples each.We find that the EER rate improves by using a combination of k-NN classifier with fuzzy logic.

Building multiple models for different keywords that are frequent in usage can help us to monitor the user while typing in a general scenarios like a chatting platform, and

suspicious operations over the handheld device can be tracked and prevented. To increase the scope of this security, other behavioral modalities such as screen touch analytics and walking patterns of an individual can be explored as a potential future research avenue for enhanced mobile phone security.

Publication:

The work discussed in this chapter is published in:
Amitabh Thapliyal, Om Prakash Verma, Amioy Kumar, "Behavioral biometric based personal authentication in feature phones", *International Journal of Electrical and Computer Engineering*, ISSN: 2088-8708, Vol 12, Issue 1,February 2022.

Chapter 6: Face Mask Recognition System Based on HAAR Cascade Classifier and Fuzzy Logic

6.1 Introduction

Face recognition market size is anticipated to grow from USD 3.8 billion in 2020 to USD 8.5 billion by 2025 [128]. The face recognition process can be categorized into 4 steps: face detection, image pre-processing, feature extraction, and matching. Principal component analysis [38], fisher Discriminant analysis, along with support vector machine [46] are examples of algorithms for face recognition.

The problem of masked face recognition is addressed in this study via Haar-feature cascade classifier, a Local Binary Pattern Histogram (LBPH) feature extractor, and a fuzzy logic-based decision maker.

Face detection has been improved by the contribution of the Viola-Jones object detection framework [129] with the application of a Haar-feature-based cascade classifier. Haar features are specific types of rectangular regions and the difference between the regions is used to classify the subsections of an image, separating the non-objects from objects [130]. The modular flow diagram for face detection is given in Figure 6.1.

Figure 6.1: Flow diagram of the proposed method for face detection.

Users wear masks in different ways which change the shape and the regions covered with the mask, as well as the regions exposed. This has a significant impact on the accuracy of results as the similarity between the trained image of the user and the presented image to the system for authentication varies considerably. To address this limitation, we introduced a fuzzy logic based system that is implemented to reduce this inaccuracy. Fuzzy logic is an approach for computing centred on "degrees of truth" instead of the usual "true or false" (1 or 0) [6].

In summary, this work is composed of three steps:

- Face detection using a Haar-feature cascade classifier.
- Feature extraction based on Local Binary Pattern Histogram (LBPH).
- Recognition decision based on Fuzzy logic.

6.2 Proposed System

Our primary idea comprises of two improvements over most of the existing work:

1. Modifying traditional face recognition algorithms to consider only the unmasked features in the top half of the face. This increased the accuracy of face recognition from 50% to 86%.

2. Fuzzy logic based decision maker to reduce false negative for variations introduced due to masking. This increased the accuracy of face recognition from 86% to 97%.

We trained our system from publicly available face recognition datasets containing both masked and unmasked images.

As mentioned before, our methodology consists of three distinct subsystems that work together to complete the masked face recognition process. The first subsystem is Haar cascade classifier to detect human faces in the presented image. The second subsystem is LBPH recognizer which does the recognition and finds out the percentage similarity between the presented (or test) image of the user and the registered image of the same user. The third subsystem used in our work is based on fuzzy logic that boosts the accuracy of our Face recognition system by predicting the best threshold confidence score (or percentage similarity) so that we have minimized false positives and false negatives.

Mask covers a considerable portion of the face but there are other exposed portions such as the eyes and eyebrows. These exposed features are given more weightage for recognition. These different weight allocations to the different exposed regions of faces help to capture the fact that there are a lot of distinctive features unevenly distributed in a face. This helped in enhancing the accuracy of recognition of masked faces from the

initial 50% to 86% as we kept tuning our Haar cascade and LBPH-based system. The proposed methodology for these sub-systems is explained in sections 6.2.1 and 6.2.2.

6.2.1 Haar feature cascade classifier with LBPH recognizer subsystem

The proposed methodology to develop the Haar feature cascade classifier with the LBPH recognizer subsystem is elucidated with the help of the block diagram in Figure 6.2.

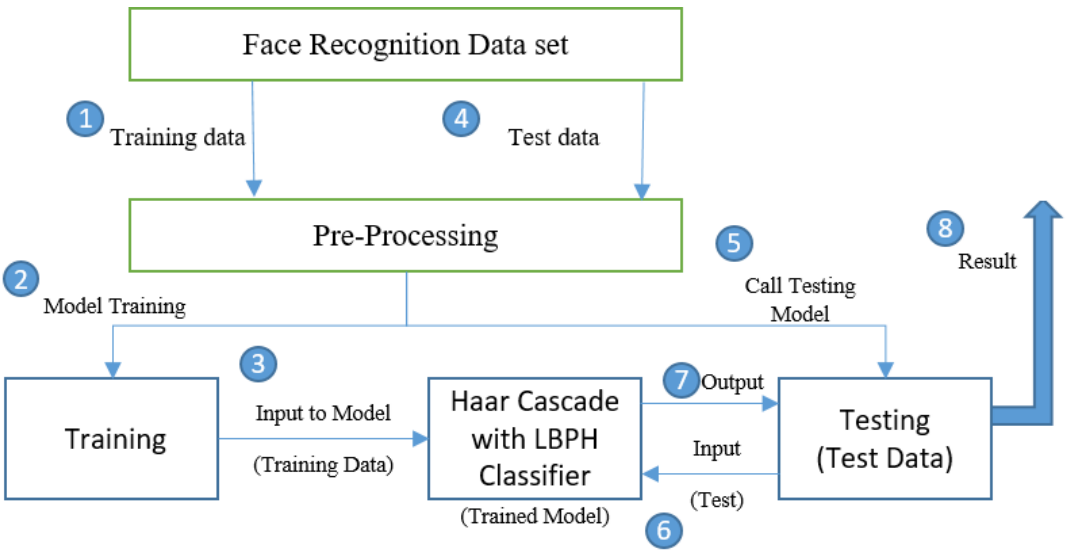

Figure 6.2: Block diagram of face recognition classification system

The Haar feature cascade with LBPH recognizer sub-system is developed as a standalone system and can independently be applied to recognize whether the presented image belongs to an authentic user or not.

Working steps:

1) **Face Recognition Dataset:** For training, we used publicly available masked face datasets. These datasets are namely:
    a. Masked Face Detection Dataset (MFDD): 24,771 Masked Face Images.
    b. Real-World Masked Face Recognition Dataset (RMFRD): 90,000 images of 525 subjects without masks and 5,000 images of the same 525 subjects wearing masks.
    c. Simulated Masked Face Recognition Dataset (SMFRD): 500,000 face images of 10,000 Subjects.
2) **Building the face recognition classifier with Haar cascade and LBPH recognizer:** Haar features involve calculations that are performed by summing the pixel intensities in each region and computing the differences between the sums as shown in Figure 6.3. These are executed on adjacent rectangular regions at a particular location in a detection window. However, this task can be very performance intensive, therefore each pixel is replaced by the sum of pixels above it and to the left of it. The image thus formed is called an integral image.

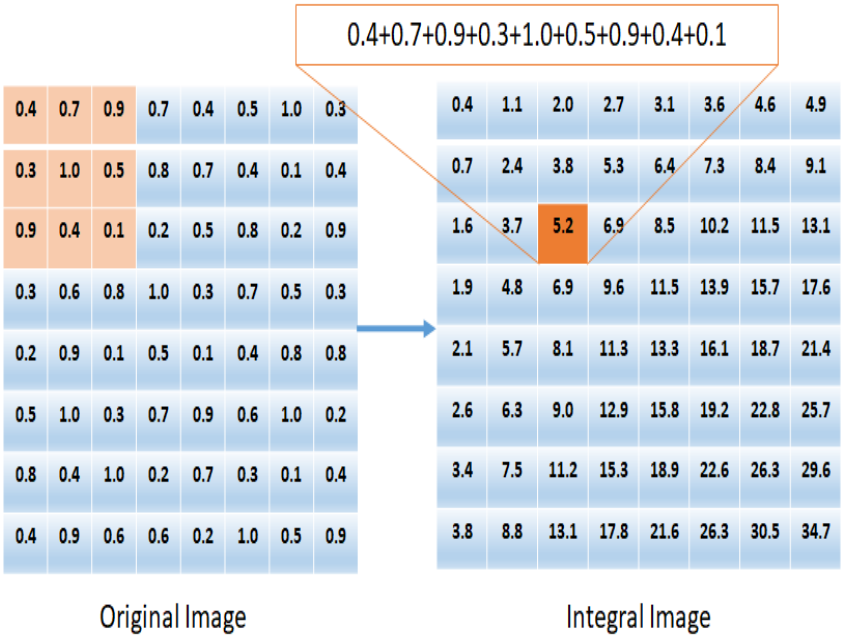

Figure 6.3: Integral Image

The sum of every pixel above and to the left is the value of the integral image at point (x, y). The following equation is deemed:

$$I_i(x,y) = \sum_{x' \le x, y' \le y} i(x', y') \quad (6.1)$$

In Equation 6.1, $I_i(x,y)$ implies the integral image and $i(x,y)$ denotes the original image.

Being a cascaded classifier, we shall be using many weak classifiers to build a strong classifier. These weak learners are trained to utilize boosting which makes for a high accuracy classifier based on the mean prediction of all less accurate ones.

For masked face detection, Haar features are a set of two rectangles that are adjacent to each other. These rectangles lie above the region of the cheeks. Sliding these adjacent rectangles over the image, we attempt to regions where one of the rectangles is dark and the other one is light. This is because the region near the eyes is somewhat darker than that of the cheeks. The positioning of these rectangles is done relative to that of a detection window.

Most of such detected Haar features are irrelevant. Hence, Adaboost is used to select the best ones. Several weak classifiers are utilized by Adaboost. Each of them is centered on disparate features. These disparate weak classifiers are merged into a single powerful classifier. The features that successfully propagate through all stages are detected as a face region.

There are several classifiers for face, eyes, etc. as xml files in OpenCV, these xml files are stored in Haar cascades. In our implementation, we have used Haar cascade frontal face default xml.

Training the system: For training the system, the dataset is organized in a form of a tuple consisting of a face image and a label. The pre-processed training data prepared from the publicly available dataset already contains the label as discussed above.

Testing the system: For testing the system, we used multiple combinations of the registered image of the user and presented the image of the same user. Also, we used random combinations of images of different users to measure the false positivity rate of our system. When each of the pairs of the registered and tested images is used to test the system, we get the confidence score for the similarity between the images. The decision is taken by two separate systems: one a combination of Haar cascade face detector and LBPH based face recognizer, and the other by using a separate fuzzy decision-making

module to take the final decision based on fuzzy logic. This is done to evaluate the impact of fuzzy decision-making on the error rate of the system.

6.2.2 Fuzzy logic based threshold confidence level selection subsystem

We found that using a system based only on the Haar cascade classifier and LBPH recognizer cannot yield the high accuracy when it comes to the recognition of faces covered with masks.

Generalized training for masked faces isn't feasible because there is a very high degree of variability in the masks themselves as well as their ways of wearing. More importantly, this variability is huge, not only among different people but also in each individual at different times. Users may wear the mask in different ways and styles. In addition to that, the user might be wearing a mask that only covers the mouth while the nose left visible to the phone camera whereas in other instances mask is even worn below the lips covering only the chin with the rest of the face exposed. Also, face masks come in varieties of sizes and shapes. Hence, certain mask sizes and shapes will allow coverage of 70 ~ 75% of the face starting from the top of the nose till the neck whereas certain other masks may only be covering essential parts of the face i.e., nose and mouth extending to only around 40 ~ 45% of the face. All these factors reduce the accuracy of face recognition. This leads to the occurrence of some false negatives. This issue can be solved by decreasing the threshold confidence score of similarity by setting it lesser than the preceding value in the algorithm needed for asserting the given user's image as an authentic user. But the problem with this technique is choosing such a strategy will lead to an increase in the number of false positives which will again reduce the accuracy of the system. Therefore, we conclude that there is a need to decide the threshold confidence level dynamically so that our system chooses the best threshold confidence value to get the most accurate overall results.

We found that a fuzzy logic-based subsystem is an appropriate and optimized approach to determine the threshold Confidence Score for the above-discussed problems. The fuzzy logic can be conveniently applied at this stage when the percentage similarity between the presented (or test) image compared with a registered (or trained) set of images has been determined and we need to dynamically decide the threshold percent (or confidence level) that would be most appropriate to maximize the accuracy of the overall system.

Our fuzzy logic based subsystem depends upon the percentage coverage of face with a mask in the registered (or trained) set of images, the percentage coverage of face in the presented (or tested) image, and the range of confidence levels (or percentage similarity) possible for different ranges of variations between the former two in a trained Haar cascade face detector with LBPH recognizer system.

The step-by-step methodology for the working of this subsystem is depicted in Figure 6.4.

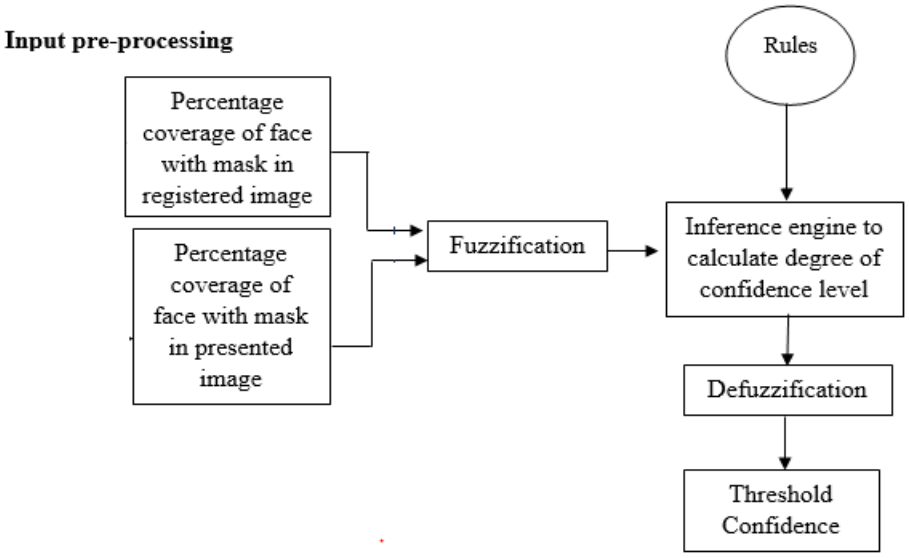

Figure 6.4: Flow diagram for Fuzzy logic based confidence level prediction system

This subsystem takes two inputs which are percentage coverage of the area of the face which is covered by the mask of the presented and registered image. These inputs will go through fuzzification and inference engine to get the aggregated conclusion which is passed through the defuzzification process to get the crisp results of which threshold confidence score to be picked to determine if the presented image qualifies to be recognized as authenticated image against the registered image of user covering its face with a typical mask.

The details of each step are mentioned below:

1) **Input pre-processing:** The fuzzy system takes the input in the form of percentages for coverage of mask in the training images and tested images. These

values are simple arithmetic values that need to be calculated from the provided image. The percentage coverage of a face with the mask is estimated from the Haar object classifier that finds out the area of the complete face and the area of the object lying inside the face area which can be asserted as the mask. Based on the above two parameters, the percentage coverage of the face by the mask is calculated. It may be noted that the module doesn't take into account whether the user is wearing a mask properly or not (i.e. completely covering the mouth and nose together) as this is out of the scope of this study.

2) **Fuzzification:** The initial step in the fuzzy inference mechanism is Fuzzification. It is defined as the process of mapping the crisp value into the degrees to which the inputs belong to the respective fuzzy sets. Several sorts of curves could be utilized. However, the most common are triangular or trapezoidal-shaped membership functions. Here, the triangular membership function is utilized. It is specified by '3' parameters $\{a, b, c\}$ in which for each value, the membership function is denoted as $\mu_A(X)$. For fuzzifying the crisp value, if-then rules are utilized by fuzzification. The first module of our system obtains the membership values for the below two crisp inputs gathered from two input sources namely the registered image and presented image. The actual inputs from these sources are defined as below:

Variation between percentage coverage of face between registered image and presented image (σ): This value is simply the absolute difference between the percentage coverage of face with a mask in registered (ρ_{r}) and presented image (ρ_{p}). Mathematically, this is defined as below:

$$\sigma = |\rho_{\mathrm{r}} - \rho_{\mathrm{p}}| \tag{6.2}$$

We are going to introduce three variables for σ viz. HIGH ($\mu_{\sigma\mathrm{H}}$), MEDIUM ($\mu_{\sigma\mathrm{M}}$), and LOW ($\mu_{\sigma\mathrm{L}}$). The graphical representation of membership functions for these variables is depicted in Figure 6.5.

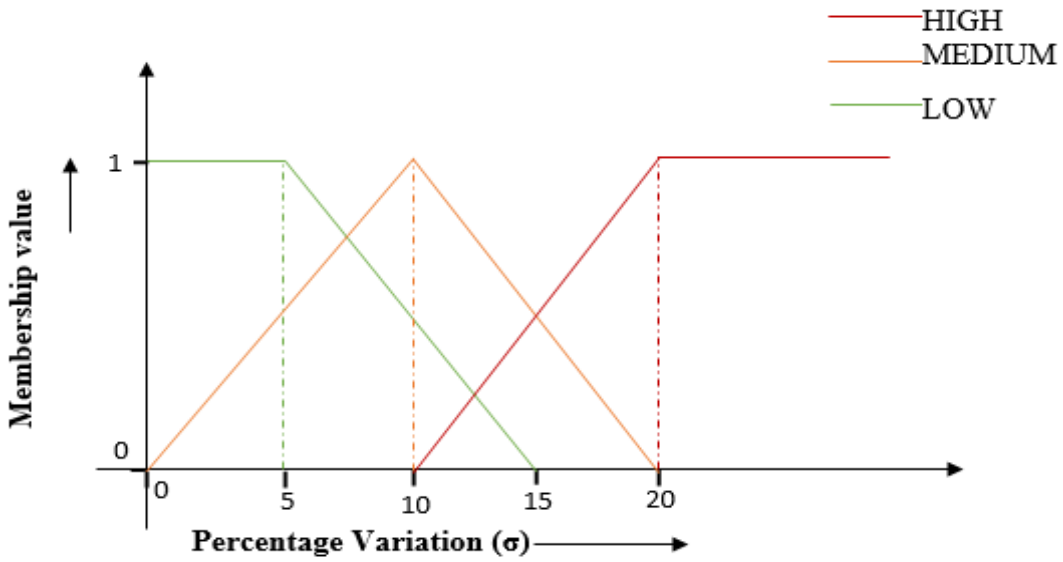

Figure 6.5: Membership function for percentage variation

Mathematically, the membership functions for the three variables are represented as below in Equations 6.3 to 6.5:

$$\mu_{\sigma H} = \begin{cases} 0\,, & if\ \sigma \leq 10 \\ \frac{\sigma - 10}{10}, & if\ 10 < \sigma \leq 20 \\ 1\,, & if\ \sigma > 20 \end{cases} \tag{6.3}$$

$$\mu_{\sigma M} = \begin{cases} 0, & if\ \sigma \leq 0 \\ \frac{\sigma}{10}, & if\ 0 < \sigma \leq 10 \\ \frac{20 - \sigma}{10}, & if\ 10 < \sigma \leq 20 \\ 0\,, & if\ \sigma > 20 \end{cases} \tag{6.4}$$

$$\mu_{\sigma L} = \begin{cases} 1\,, & if\ \sigma \leq 5 \\ \frac{15 - \sigma}{10}, & if\ 5 < \sigma \leq 15 \\ 0\,, & if\ \sigma > 15 \end{cases} \tag{6.5}$$

Percentage coverage of face (ρ): This is the percentage of the area of the face which is covered with a mask and used for identification of the image by the Haar cascade classifier. Similar to the previous input, we are going to use the same

variables viz. HIGH ($\mu_{\rho H}$), MEDIUM ($\mu_{\rho M}$), along with LOW ($\mu_{\rho L}$). The membership functions for them are defined as below in Figure 6.6:

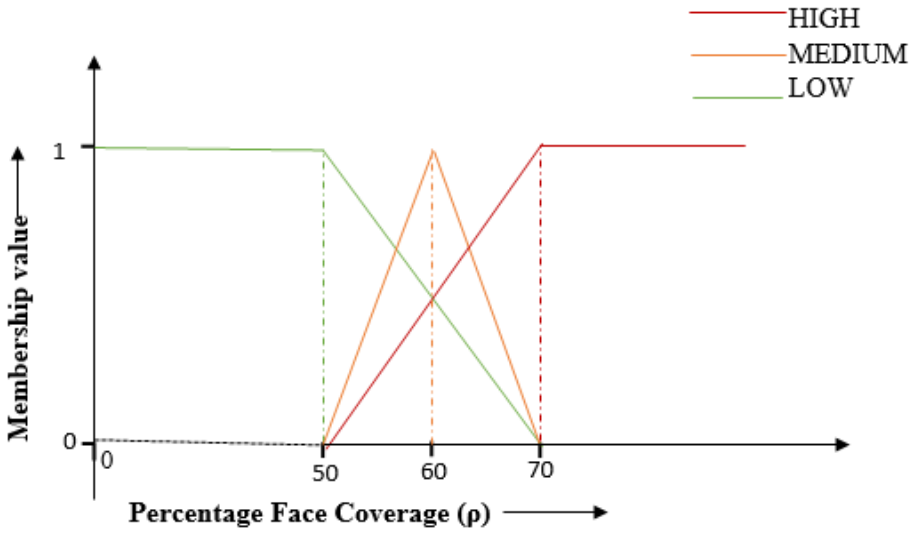

Figure 6.6: Membership function for percentage face coverage

Mathematically, the membership functions for the above three variables are represented below in Equations from 6.6 to 6.8:

$$\mu_{\rho H} = \begin{cases} 0\,, & if\ \rho \leq 50 \\ \frac{\rho - 50}{20}, & if\ 50 < \rho < 70 \\ 1\,, & if\ \rho \geq 70 \end{cases} \tag{6.6}$$

$$\mu_{\rho M} = \begin{cases} 0, & if\ \rho \leq 50 \\ \frac{\rho - 50}{10}, & if\ 50 < \rho < 60 \\ \frac{70 - \rho}{10}, & if\ 60 \leq \rho < 70 \\ 0\,, & if\ \rho \geq 70 \end{cases} \tag{6.7}$$

$$\mu_{\rho L} = \begin{cases} 1\,, & if\ \rho \leq 50 \\ \frac{70 - \rho}{20}, & if\ 50 < \rho \leq 70 \\ 0\,, & if\ \rho > 70 \end{cases} \tag{6.8}$$

3. **Rule Base:** The rule base to be used for the inference engine is represented in Table 6.1 for various combinations of the two input fuzzy sets:

Table 6.1. Rule Base representation

Percentage Variation (σ)	HIGH	MEDIUM	LOW
HIGH	LOW	LOW	MEDIUM
MEDIUM	LOW	MEDIUM	HIGH
LOW	MEDIUM	MEDIUM	HIGH

Percentage Face Coverage (ρ)

4. **Inference engine:** Based on the rule base defined above in Table 6.1, the conclusions for each of the members viz. HIGH (μ_{rH}), MEDIUM (μ_{rM}), and LOW (μ_{rL}) in the output set is done using the below equations:

$$\mathrm{T} = Min(\mu_{\sigma\mathrm{H}}, \mu_{\rho\mathrm{H}}) + Min(\mu_{\sigma\mathrm{H}}, \mu_{\rho\mathrm{M}}) + Min(\mu_{\sigma\mathrm{H}}, \mu_{\rho\mathrm{L}}) + Min(\mu_{\sigma\mathrm{M}}, \mu_{\rho\mathrm{H}}) + Min(\mu_{\sigma\mathrm{M}}, \mu_{\rho\mathrm{M}}) + Min(\mu_{\sigma\mathrm{M}}, \mu_{\rho\mathrm{L}}) + Min(\mu_{\sigma\mathrm{L}}, \mu_{\rho\mathrm{H}}) + Min(\mu_{\sigma\mathrm{L}}, \mu_{\rho\mathrm{M}}) + Min(\mu_{\sigma\mathrm{L}}, \mu_{\rho\mathrm{L}}) \quad (6.8)$$

$$\mu_{\mathrm{rH}} = \frac{Min(\mu_{\sigma\mathrm{M}}, \mu_{\rho\mathrm{L}}) + Min(\mu_{\sigma\mathrm{L}}, \mu_{\rho\mathrm{L}})}{2T} \quad (6.9)$$

$$\mu_{\mathrm{rM}} = \frac{Min(\mu_{\sigma\mathrm{M}}, \mu_{\rho\mathrm{M}}) + Min(\mu_{\sigma\mathrm{L}}, \mu_{\rho\mathrm{M}}) + Min(\mu_{\sigma\mathrm{H}}, \mu_{\rho\mathrm{L}}) + Min(\mu_{\sigma\mathrm{L}}, \mu_{\rho\mathrm{H}})}{4T} \quad (6.10)$$

$$\mu_{\mathrm{rL}} = \frac{Min(\mu_{\sigma\mathrm{M}}, \mu_{\rho\mathrm{H}}) + Min(\mu_{\sigma\mathrm{H}}, \mu_{\rho\mathrm{H}}) + Min(\mu_{\sigma\mathrm{H}}, \mu_{\rho\mathrm{M}})}{3T} \quad (6.11)$$

5. **Defuzzification -** Defuzzification will be done to get the final crisp output. For this, we are going to simply use the max function in the way that member which has the highest value in the output fuzzy set is selected. Below is the simple equation for doing this:

$$Output = Max(\mu_{\mathrm{rH}}, \mu_{\mathrm{rM}}, \mu_{\mathrm{rL}}) \quad (6.12)$$

With equation 6.12 and the following inference rule base, we will determine which level of "threshold confidence score" we need to keep out of HIGH, MEDIUM, and LOW for the most optimized results. For our implementation, we took HIGH as 90%, MEDIUM as 85% whereas LOW as 80%. This value is returned to the comparator for further evaluation.

- If μ_{rH} is maximum, then we keep the threshold score HIGH
- If μ_{rM} is maximum, then we keep the threshold score MEDIUM
- If μ_{rL} is maximum, then we keep the threshold score LOW

6.3 Implementation Details

The implementation of the system based on the methodology described in section 6.2 requires certain technical aspects that include processing the image, developing a Face recognition module, creating a training tuple, perform the training followed by testing and results. The implementation process is explained in Figure 6.7.

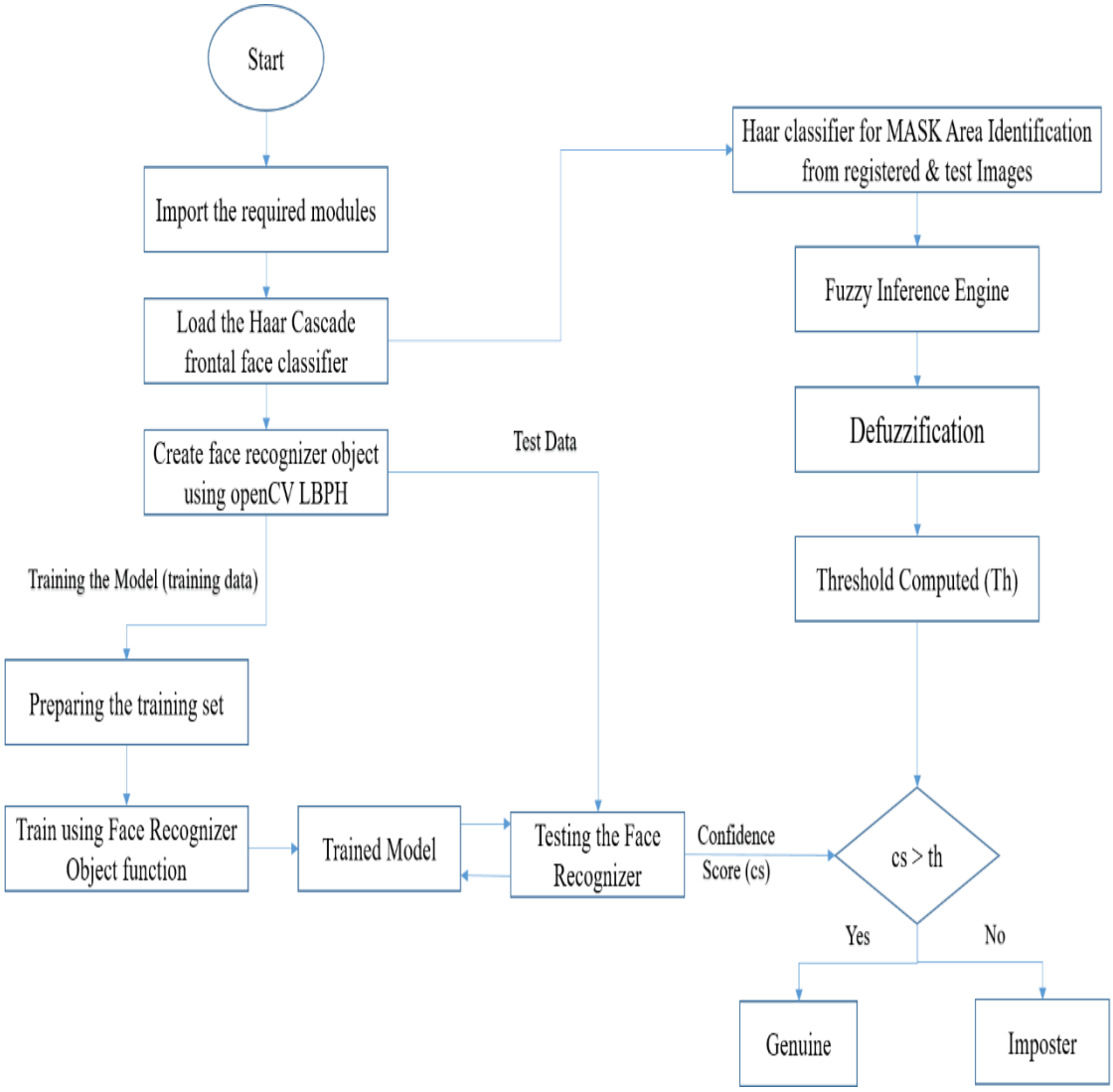

Figure 6.7: Flow chart for implementation steps

The implementation process could be broadly divided into five major stages. These include import of required modules, loading face detection Haar cascade, creating face recognizer objects, preparing and executing training along with the prior steps to prepare training data, and finally testing with the data at the end of which the confidence score (or percentage similarity) determines whether the presented (or tested) image belongs to the same user as that of the registered (or trained) user. Each of these stages is described in detail below. There are several steps involved with our implementation design for the proposed technique.

A. Import of the required modules

The available modules in the OpenCV library are used to perform basic processing to convert the images into three dimensional arrays.

The implementation of Haar cascade classifier and LBPH face recognizer are implemented using the OpenCV library. Facial recognition modules that are required are cv2, numPy, OS, and Image module. cv2 is the name that is chosen by OpenCV developers when they generated the binding generators. A module for Python is the numPy which is an acronym for "Numeric Python" or "Numerical Python". Moreover, the programming language Python is enriched by numPy with powerful data structures, applying multi-dimensional arrays along with matrices. System software that handles computer hardware, and software resources, along with that it offers common services for computer programs is the OS. A class with the same name is offered by the image module which is utilized for representing a Python Imaging Library (PIL) image. Many factory functions are also offered by the module, comprising functions to load images as files and create new images. OpenCV contains module name cv2 which includes functions useful in detecting faces as well as their recognition. OS library is used to deal with the image as well as the names of the directory as it provides many utility methods to interact with the operating system. Modules are initially used to perform basic processing.

These modules are used necessarily for the following important steps:

- Modules are initially used to draw out the names of the image from the database. A separate number from the names of each image is taken out. The respective numbers extracted are assigned to each image respectively. The number assigned is utilized as a label for the face present in that image.

- Images in the dataset are present in gif format by default. Since OpenCV does not support the gif format, it is converted into a grayscale format using the image module of PIL. This module is used for reading the image in grayscale format and the images are stored in NumPy arrays.

B. Loading face detection cascade

We use Haar cascade by OpenCV to grab and segment the face in the image which will be used to train the recognizer. Haar cascade classifiers are very efficient in object detection. OpenCV has algorithms that use Haar features which are the input to basic classifiers. Pre-trained Haar cascade algorithms are offered by OpenCV, which are arranged into categories (faces, eyes, etc.), relying upon the images they have been trained on. These features are edge features, line features, and center-surround features. These features when grouped into different stages of classifiers are applied accordingly on a window. In case the window fails at any stage, the processing stops, and the remaining features are not considered. But if the window passes, then the second set of features is implemented and the process is continued. The window that successfully propagates through all stages is termed as face region. There are several classifiers for face, eyes, etc as xml files in OpenCV.

C. Creating face recognizer object

The next step involves creating the face recognizer object. It possesses functions like Face Recognizer train for training the recognizer and Face Recognizer predict for recognizing a face. We used the Local Binary Patterns Histograms (LBPH) Face Recognizer. The LBPH algorithm is a face recognition algorithm centered on a local binary operator. Using LBPH, it is possible to comprehend the texture along with the shape of a digital image. This image is split into numerous small regions from where the features are drawn out. This is then used to find the similarity between the images. In our implementation, we used only the top half portion of the face to draw out the features. This improved the accuracy of face recognition from 50% to 86%.

D. Prepare and execute the training

Images of faces are used to train the recognizer. For preparing the training set we need to define a function. This function takes input from the absolute path of images of database (DB). It outputs the tuple containing two lists. One of the lists of tuples contains the detected faces and the other contains the corresponding label for that face. For instance, in the case in the list containing the detected faces, the i^{th} location represents the third individual in the database then in the list of labels we have value 3 at i^{th} index. This output

tuple constitutes the training set. Now the training is performed utilizing the Face Recognizer Train function. This function requires two parameters, the features, and the label.

We used three data sets for masked face recognition. Some information about the datasets provided is explained below:

- **MFDD:** This dataset comprises images that are a sample from related research. Also, the other source is from the internet. These face images from the internet are labeled by adding some more metadata such as whether the mask is there on the face or not and the coordinates positioning the masked face. This formed dataset has 24771 masked faces. This dataset finds application in training a face detection model for face recognition. Besides this, it can also determine if the person is wearing a mask or not.

- **RMFRD:** This dataset is composed by using a python crawler tool. This tool crawls the face image of the subject. Also, from the internet sources, it crawls the corresponding masked image. Then the unreasonable portions emerging post wrong correspondence is removed. Semi-automatic annotation tools namely LabelImg along with LabelMe is used to segment accurate face areas. The 90,000 images of 525 subjects without masks along with 5,000 images of the same 525 subjects wearing masks.

- **SMFRD:** This dataset is developed with the help of a mask wearing software on Dlib-ML for performing mask wearing automatically. Popular datasets LFW and Webface dataset is using this software to apply the mask on the faces. Thus, a simulated masked face dataset is generated that has 500000 face images of 10000 subjects.

E. Testing

At this stage, a new set of images for some of the registered (or trained) users is selected and compared with the registered (or trained) images of the same users. A confidence score representing the similarity percentage is determined. Testing is done only with masked images.

After the confidence of percentage similarity of the presented image is determined, the decision to whether that presented image belongs to one of the users whose image is registered in the system. This is being done using a comparator which simply checks whether the determined confidence level is above a determined "threshold". The value of this "threshold" is determined using another intelligent subsystem that is based on fuzzy logic. The purpose of this subsystem is to determine which category of confidence level is appropriate to get accurate results. The comparator passes the value obtained from the testing module to the fuzzy subsystem and gets the result back from that after which a simple comparison gets to the final result to be displayed.

Fuzzy logic based subsystem:

The fuzzy logic based subsystem to determine the optimized "threshold" confidence score, gets the input from the registered (or training) image of the user. The input mainly comprises percentage coverage of the face by mask. This value from multiple images is used to calculate the parameters such as mean and variance. Again, the same values are determined from the input of the presented (or test) image. The fuzzy inference engine based on the pre-determined rule base infers the association of test input image with a category of "threshold" confidence level which can be HIGH, MEDIUM, or LOW as per our rule base. After this, we take a simple mapping of the determined "threshold" confidence category with a percentage number. For our implementation, we took HIGH as 90%, MEDIUM as 85% whereas LOW as 80%. This value is returned to the comparator for further evaluation.

The above steps are quite exhaustive and start right from importing modules to yielding results after comparison. To demonstrate a practical application of the proposed methodology and implementation details along with determining the accuracy results, we developed a camera-based security system. Security systems are one of the important concerns for time being. We witness advancements in technologies to boost security

systems. Face recognition also comprises the security system. But due to the COVID-19 pandemic, we witness the necessity of masks and also take into consideration the security breach that can happen due to this. Hence, we essentially proposed a technique of face mask recognition that could authenticate a person. So, we propose to further deploy it into a security system that could identify a person in a mask and also serves as a provision of contactless authentication for security aspects. This security system can be deployed at door. Once the person enters, his image is taken by the system and compared with the existing image data. The snapped image and the authorization details will be sent to Google drive. Also, information such as time and entry date will be sent to Google drive. The system already has the mechanism to ensure that the image is taken only when a person comes to the door. This is done by deploying infrared sensors which sense and detects the person. Raspberry pi post receiving the signal from Infrared sensors activates the camera and the LCD screen that displays the message to stop. The camera on getting activated takes the picture of the person. This picture is saved in a new folder which would be later used for comparison. Raspberry pi gets enabled using Ethernet wire. Once the image is snapped based on our proposed approach the face is segmented and detected. Internally the algorithm works firstly the segmented face is given to the model. Using the database records the saved image is extracted, once extracted saved image and snapped image are compared and the confidence score is evaluated as per our methodology. Based on this authentication is done and correspondingly the LCD screen displays the confidence score and claims on this basis whether the person is authorized or not.

The confidence about how much a person is an authorized person is also displayed as shown in Figure 6.8.

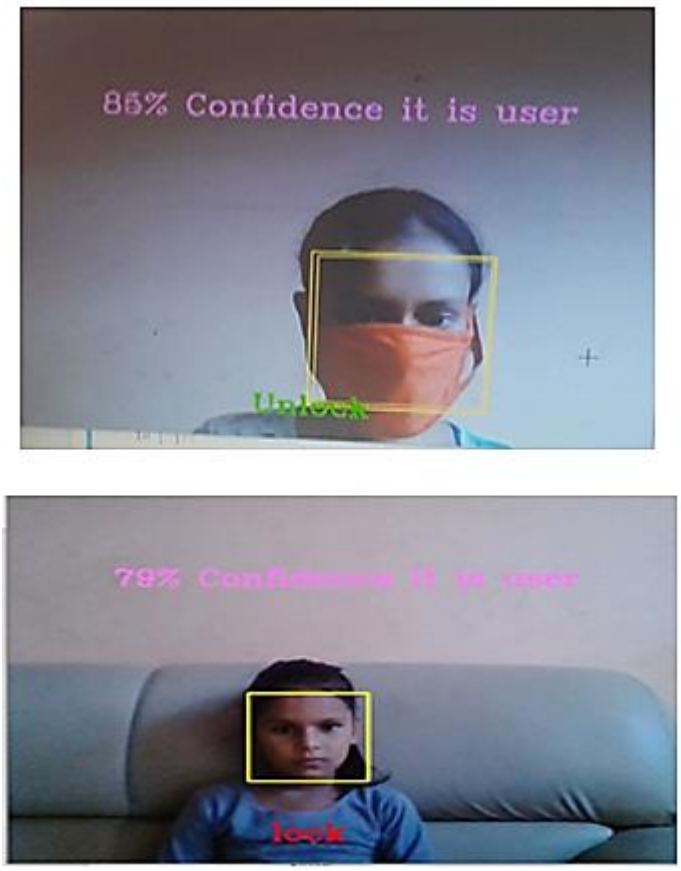

Figure 6.8: Detection of faces with and without the mask

It takes about five seconds to give the result of face detection and recognition with a face mask on the system which is developed on the LINUX system on a computer with 8GB RAM, Intel i7 CPU specs. The decision for lock or unlock is taken based on our methodology which has determined the optimized "threshold" confidence score to authenticate a user.

6.4 Experimental Results

Post training, we tested our proposed system for 236 combinations of registered and tested images of 89 users spread across different demographical and ethnic backgrounds. We classified our results under the heads of 1) "valid authentications", 2) "false negative" authentications, and 3) "false positive" authentications. The "false negatives" are such combinations of registered images and tested images wherein the combination was expected to be recognized as valid authentication but found as unauthenticated by our

system whereas “false positives” are those wherein such combination that should not have been recognized as authenticated was wrongly identified to be authentic. The lab experiments were performed in Samsung India R&D, Noida. The results are summarized in Table 6.2.

Table 6.2: Results Summary

	Valid	**False Negative**	**False Positive**
Only Haar cascade classifier	203	27	6
Haar cascade classifier combined with Fuzzy Logic	229	2	5

The proposed Haar-cascade classifier model achieved the recognition accuracy of almost 86% when used standalone with a fixed “threshold” confidence score. Here, the term “accuracy” implies the number of valid authentications. This was the highest accuracy result possible achieved by tuning the “threshold” confidence score exhaustively several times but keeping that fixed for testing all combinations. However, the accuracy reached almost 97% when we applied the fuzzy logic based decision making module to determine the “threshold confidence score” dynamically when the test image is presented. Moreover, it would be worth mentioning that the number of false negatives fell drastically whereas there was relatively less impact on the number of false positives.

Comparison with prior work

Sense Time Technology [131] reported 85% accuracy when the images showed 50% of the covered nose. Hanvon Technology [132] reported that their success rate of masked Face recognition was 85%. Another study by MINIVISION Technology [133] showed a success rate of over 90%. However, the best available results are the outcomes of Wang *et. al* [19] which achieved an accuracy of 95%.

This comparison of our results with from different works is summarized in Table 6.3 and Figure 6.9.

Table 6.3: Comparisons of results with prior works

Name	**Accuracy of masked face recognition**
Sense Time [131]	85%
Hanvon [132]	85%
MINIVISION [133]	90%
Face and eye based multi-granularity model [19]	95%
HAAR cascade detector + LBPH recognizer (our work)	86%
HAAR cascade detector + LBPH feature extractor + Fuzzy decision maker (our work)	97%

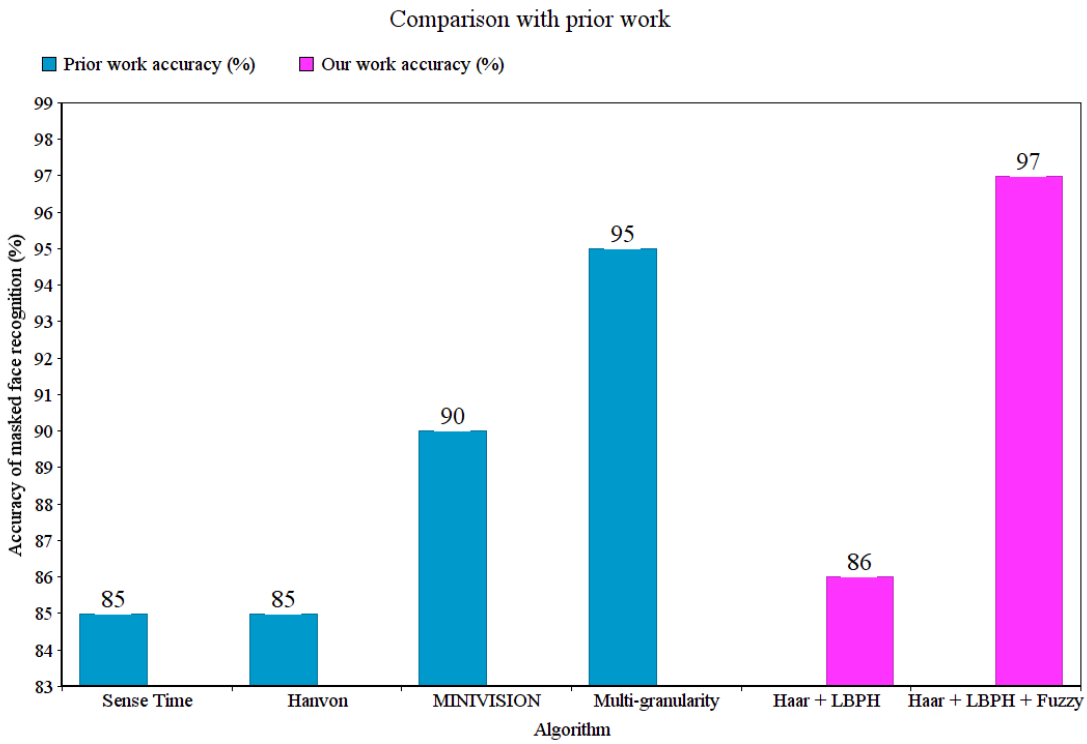

Figure 6.9: Performance analysis of different methods: prior work versus our work.

6.5 Conclusion

Overall, this work proposes a highly accurate recognition system that can recognize faces that are even covered with masks. Not only is accurate, but the system is also overall highly efficient as well. The two-component subsystems involved in this work can work independently to perform their respective roles of determining similarity between two images with faces covered with masks and determining an optimum confidence score above which such similarity can qualify the tested image to be authenticated version of the same user in the registered image. The Haar cascade classifier and LBPH recognizer are evaluated for the masked face and also fuzzy logic is used for the first time to resolve such uncertainty when it comes to the problem of recognizing faces with masks. We determined the accuracy results of 86% for a standalone Haar cascade classifier with LBPH face recognizer and demonstrated how it can be improved to 97% if the fuzzy logic based system is applied. Our proposed fuzzy subsystem can be used in conjunction with other deep learning models as well. The applications that can be made out of this work don't only include masked Face recognition but also in scenarios when the user's face is

only partially exposed to a Face recognition system. This may include scenarios like wearing up spectacles, growing a beard, etc. Future applications of this work are not only limited to the ongoing COVID-19 pandemic but also to when the pandemic hopefully ends in the future. This includes deployment on handheld devices for a smooth and safe user experience, a face recognition-based attendance system at workplaces where the mask is mandatory, and so on.

Publication:

The work discussed in this chapter is published in:

Amitabh Thapliyal, Om Prakash Verma and Amioy Kumar, "Mask Covered Face Recognition Using Haar Cascade Classifier and Fuzzy Logic", *International Journal of Emerging Technology & Advanced Engineering*, Vol. 12, Issue 8, 2022.

Chapter 7: Conclusion and Future Work

Biometrics-based authentication systems, such as fingerprint or facial recognition, are considered more reliable both by security experts and public at large as compared to PIN, password, or pattern-based traditional authentication systems on smartphones. Since biometrics need to be presented at the time of power-on, hence, they cannot be guessed or attacked through brute force, eliminating the possibility of shoulder surfing. However, fingerprints or facial recognition-based systems in smartphones may not be applicable in a pandemic situation like COVID-19, where hand gloves or face masks are mandatory to protect against unwanted exposure of the body parts.

To tide over these and other similar challenges, our work investigates some potential advances in the field of biometrics. The contributions of our work to the existing body of literature can be enumerated in the following points:

- A biometric authentication system is influenced by external and contextual factors. A novel multimodal biometric authentication framework was introduced that dynamically invokes multi-modality for smartphone user authentication based on contextual factors and external variables. In the proposed system, the contextual model evaluates a user's context at the time of authentication to provide initial identity confidence. Based on the obtained confidence, the authentication complexity or modality of the final authentication model is determined dynamically. We designed a multimodal biometric authentication framework to meet the changing security needs considering external variables while leveraging the contextual factors. The designed system was tested on behavioural biometrics. We were able to demonstrate improved results in terms of accuracy with a reduction in the equal error rate with proposed framework.

- A novel bimodal system is developed based on the proposed biometric authentication framework. A hand glove mode of authentication is proposed for smartphones considering the COVID-19 pandemic when the user's input samples may be impacted by external variables like water, sanitizer, and gloves. In such situations, it is difficult for legitimate users to authenticate using conventional biometric authentication methods like fingerprint recognition. We developed a

bimodal behavioural biometric authentication system based on keystroke and touch swipe that can also handle situations when the user samples are impacted by external variables like hands with gloves, water, and sanitizer. The data collection was performed with 197 users using an Android application developed on Android OS 11.0 and a Samsung Galaxy S20 device. The experimental results shown good authentication accuracy.

- We have been able to make the application of keystroke dynamics to mobile phones as a biometric authentication system fast, efficient, and adaptable. Our study proposed a method for learning the user's typing patterns on a feature phone and employing it for authentication. We applied k-Nearest Neighbours algorithm with Fuzzy Logic and attained an equal error rate of 1.88 percent. The experiments were carried out using a Samsung On7 Pro C3590 with 25 users.

- Numerous precautions must be taken to combat COVID-19 pandemic, one of the most significant of which is the widespread use of a face mask. Though research to improve face recognition has advanced significantly over the last two decades, recognizing faces hidden behind masks has become a new concern due to the developing situation. Unfortunately, abundant work has not been done in this area. Innovative solutions to these problems were proposed and investigated in our work.

Our work investigates the situations in which fingerprints cannot be utilized due to hand gloves and presents an alternative biometric system using the multimodal touchscreen swipe and keystroke dynamics pattern. A hand glove mode of authentication was proposed, where the system would automatically be triggered to authenticate a user based on touchscreen swipe and keystroke dynamics patterns. The proposed method incorporates the touchscreen's swipe and typing patterns as a security layer for authentication to increase the total security of the system. A fuzzy classification network was also proposed to incorporate fuzziness into the authentication system, thereby reducing the effects of unknown external variables, such as dust or sanitized hands, on user authentication. Our experimental results suggest that the proposed multimodal behavioural biometrics system can operate with a high accuracy. We were able to obtain an authentication accuracy of 99.55% with 197 users on the Samsung Galaxy S20 device and Android 11 OS. The importance of this work is mainly due to the reason that most of

the biometrics utilized in smartphones are physiological, such as fingerprints, iris, face, etc. Some attempts have been made to use behavioural biometrics such as voice, signature, gait, and keystroke. However, these attempts are very few and are currently not commercialized on smartphones. The fuzzy logic based decision system was used to reduce the effects of hand gloves or sanitized hands on user authentication and achieved 93.5% accuracy in such cases. Our experimental results suggest that the proposed multimodal biometrics system can operate with high accuracy even in the presence of gloved, sanitized, and wet hands. It is sufficient to conclude that the presented work for user authentication in smartphones has a promising potential for further development and investigation.

We also developed a masked face recognition system based on a Haar cascade classifier, which demonstrated better performance than the state of the art. We use a Haar-feature-based cascade classifier to identify the extent to which a given face and the registered face resemble each other. Additionally, this study attempts to address problems in face recognition that occur when the user wears a mask that covers a different portion of the face in different instances, resulting in visible errors when various tests return false negatives or false positives on multiple instances. This problem is addressed by using a fuzzy logic based system that decides the "threshold confidence score" needed to pass the authentication dynamically. The proposed model for masked face recognition achieves an accuracy of 86% when a Haar-feature-based cascade classifier is used standalone, which further reaches to around 97% when used in conjunction with a fuzzy logic based decision making module. The result is better than reported in the existing literature surveyed by us. Therefore, our work provides an accurate identification system that can distinguish faces covered with masks. The procedure is not only quite accurate but also efficient in general. This work involves two component subsystems that can work independently and perform their respective roles for authentication with mask covered faces.

Future applications of our work are limited not just to the COVID-19 pandemic, but also applicable to the time when the pandemic is expected to end. This includes mobile device authentication system for a convenient and secure user experience, face recognition based attendance systems in organizations where masks are required, authentication in healthcare settings where gloved hands and masked faces are common,

and so on. Various modalities like touch analytics, patterns of battery charging, and walking patterns of a person can be investigated as behavioural biometric modalities for a future study for mobile phone security.

References

1. A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, Jan. 2004.

2. J. Nelson CPP, "Biometrics Characteristics," in *Effective Physical Security (Fourth Edition)*, L. J. Fennelly, Ed. Oxford, England: Elsevier, pp. 255–256, 2013.

3. Azal Habeeb, "Comparison between physiological and behavioral characteristics of biometric system," *Journal of Southwest Jiaotong University*, vol. 54, no. 6, 2019.

4. Foudil Belhadj, "Biometric system for identification and authentication," *Computer Vision and Pattern Recognition*, Ecole nationale Supérieure en Informatique Alger, 2017.

5. S. Ramakrishnan, Ed. "Face Recognition: Semisupervised Classification, Subspace Projection and Evaluation Methods," London, United Kingdom, IntechOpen, 2016. Available at: https://www.intechopen.com/books/5183 doi: 10.5772/61471 [accessed: 05-Oct-2021].

6. Krishna Dharavath, Fazal A. Talukdar, and Rabul H. Laskar, "Study on biometric authentication systems, challenges and future trends: A review," *2013 IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-7, IEEE, 2013.

7. Statcounter (2021), "Mobile Operating System Market Share Worldwide," StatCounter Global Stats. Available at: https://gs.statcounter.com/os-market-share/mobile/worldwide [accessed: 10-Dec-2021].

8. Ting Zhao, Gang Zhang, and Lei Zhang. "An overview of mobile devices security issues and countermeasures." *2014 International Conference on Wireless Communication and Sensor Network*. pp. 439-443, IEEE, 2014.

9. Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider, "A survey of password attacks and comparative analysis on methods for secure authentication," *World applied sciences journal,* vol. 19, no. 4, pp. 439-444, 2012.

10. Sonia Ohlyan, Sunita Sangwan, and Tarun Ahuja "A survey on various problems & challenges in face recognition," *International Journal of Engineering Research & Technology (IJERT),* vol. 2, no. 6, pp. 2533-2538, 2013.

11. L. A. Zadeh, "Fuzzy sets," *Information and control*, vol. 8, no. 3, pp. 338-353, 1965.

12. Fabian Maul, and Naser Damer, "Fuzzy Logic and Multi-biometric Fusion," *Proceedings of the International Conference on Pattern Recognition Applications and Methods*, vol. 1, pp. 218-222, 2015

13. Ravi Sandhu, Jennifer Hadley, Steven Lovaas, and Nicholas Takacs, "Identification and authentication," *Computer Security Handbook* , vol. 4, pp. 28-1, 2012.

14. Karthik Nandakumar, "Integration of multiple cues in biometric systems," *Michigan State University*, 2005.

15. Stuart Carlaw, "Impact on biometrics of Covid-19," *Biometric Technology Today* 2020, no. 4, pp. 8-9, 2020.

16. "Assessing the impact of COVID-19 on the biometrics market," Abiresearch*.com*. Available at: https://www.abiresearch.com/market-research/product/7778287-assessing-the-impact-of-covid-19-on-the-bi/. [accessed: 06-Dec-2021].

17. China Smartphone Market Posts Largest Decline Ever as Shipments Drop by 20.3% YoY in Q1 2020, IDC Reports. (2020), Available at: https://www.displaydaily.com/article/press-releases/china-smartphone-market-posts-largest-decline-ever-as-shipments-drop-by-20-3-yoy-in-q1-2020-idc-reports. [accessed: 10-Nov-2022]

18. Worldwide Smartphone Market Suffers Its Largest Year-Over-Year Decline in Q1 2020 Due to COVID-19, According to IDC. (2020). Available at: https://www.businesswire.com/news/home/20200430006052/en/Worldwide-Smartphone-Market-Suffers-Its-Largest-Year-Over-Year-Decline-in-Q1-2020-Due-to-COVID-19-According-to-IDC. [accessed: 15-June-2022]

19. Zhongyuan Wang, Guangcheng Wang, Baojin Huang, Zhangyang Xiong, Qi Hong, Hao Wu, Peng Yi, Kui Jiang, Nanxi Wang, Yingjiao Pei, Heling Chen, Yu Miao, Zhibing Huang, Jinbi Liang, "Masked face recognition dataset and application," *arXiv preprint arXiv:2003.09093, 2020.*

20. Statisca Research Department (2022), *Number of smartphone subscriptions worldwide from 2016 to 2021,* Statista, Available at: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide. [accessed: 15-Nov-2022]

21. Josh Howarth (2022), *How Many People Own Smartphones (2022-2027)?*, Available at: https://explodingtopics.com/blog/smartphone-stats [accessed: 25-Nov-2022]

22. Shah Faisal Darwaish, Esmiralda Moradian, Tirdad Rahmani, and Martin Knauer, “Biometric identification on android smartphones,” *Procedia Computer Science,* vol. 35, pp. 832-841, 2014.

23. Farzaneh Karegar, John Sören Pettersson, and Simone Fischer-Hübner, “Fingerprint recognition on mobile devices: widely deployed, rarely understood, ” *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1-9, 2018.

24. Mohamed Amine Ferrag, Leandros Maglaras, Abdelouahid Derhab, and Helge Janicke, "Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues," *Telecommunication Systems,* vol. 73, no. 2, pp. 317-348, 2020.

25. Kavita Rathi, and Sudhir Sawarkar, "Finger print matching algorithm for android," *International Journal of Engineering Research and Technology*, vol. 2, no. 10, pp. 3819-3823, 2013.

26. V. Wilson Tracy, "How Biometrics Works," 2017, Available at: https://science.howstuffworks.com/biometrics.htm.

27. Anil K. Jain, Patrick Flynn, and Arun A. Ross, eds. Handbook of biometrics. *Springer Science & Business Media*, 2007.

28. staff, S.X. (2005), World's First Face Recognition Biometric for Mobile Phones. [online] Phys.org, available at: https://phys.org/news/2005-03-world-recognition-biometric-mobile.html.

29. Alreja, K. (2019). *Face Unlock in Phones – From 2011 to 2019 !*, Available at: http://kirat.in/tech/face-unlock-in-phones-2019/

30. J. A. Popoola, and C. O. Yinka-Banjo, "Comparative analysis of selected facial recognition algorithms," *Nigerian Journal of Technology*, vol. 39, no. 3, pp. 896-904, 2020.

31. Fujitsu Limited (2015), *Fujitsu Releases ARROWS NX F-04G*, Available at: https://www.fujitsu.com/global/about/resources/news/press-releases/2015/0525-01.html [accessed: 15-May-2022]

32. Samsung Introduces Galaxy Tab Iris Equipped with Iris Recognition Technology for Government and Enterprises in India. (2016). Samsung News, Available at: https://news.samsung.com/global/samsung-introduces-galaxy-tab-iris-equipped-with-iris-recognition-technology-for-government-and-enterprises-in-india

33. Markov (2020), "*Fingerprint Scanner On Phones: History & Evolution, But Do We Really Need That?*," Available at: https://www.igadgetsworld.com/fingerprint-scanner-history-evolution-but-do-we-really-need-that [accessed: 20-June-2022]

34. Ashraf El-Sisi, "Design and implementation biometric access control system using fingerprint for restricted area based on gabor filter," *The International Arab Journal of Information Technology*, vol. 8, no. 4, pp. 355-363, 2011.

35. Walid Hariri, "Efficient masked face recognition method during the covid-19 pandemic," *Signal, image and video processing*, vol. 16, no. 3, pp. 605-612, 2022.

36. Shiming Ge, Jia Li, Qiting Ye, and Zhao Luo. "Detecting masked faces in the wild with lle-cnns," *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 2682-2690, 2017.

37. Takeo Kanade, "*Computer recognition of human faces*," Vol. 47, Basel: Birkhäuser, 1977.

38. Lawrence Sirovich, and Michael Kirby, "Low-dimensional procedure for the characterization of human faces," *Josa a*, vol. 4, no. 3, pp. 519-524, 1987.

39. Matthew Turk and Alex Pentland. "Eigenfaces for recognition," *Journal of cognitive neuroscience*, vol. 3, no. 1, pp. 71-86, 1991.

40. Dong-Chen He, and Li Wang. "Texture unit, texture spectrum, and texture analysis," *IEEE transactions on Geoscience and Remote Sensing*, vol. 28, no. 4, pp. 509-512, 1990.

41. Xiaoyu Wang, Tony X. Han, and Shuicheng Yan, "An HOG-LBP human detector with partial occlusion handling," *2009 IEEE 12th international conference on computer vision*, pp. 32-39, IEEE, 2009.

42. Keun-Chang Kwak, and Witold Pedrycz, "Face recognition using fuzzy integral and wavelet decomposition method," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 34, no. 4, pp. 1666-1675, 2004.

43. Norma Latif Fitriyani, Chuan-Kai Yang, and Muhammad Syafrudin, "Real-time eye state detection system using haar cascade classifier and circular hough transform," *2016 IEEE 5th Global conference on consumer electronics*, pp. 1-3, IEEE, 2016.

44. Debotosh Bhattacharjee, Dipak K. Basu, Mita Nasipuri, and Mohantapash Kundu, "Human face recognition using fuzzy multilayer perceptron," *Soft Computing*, vol. 14, no. 6, pp. 559-570, 2010.

45. Dong Yi, Zhen Lei, and Stan Z. Li, “Shared representation learning for heterogenous face recognition,” *2015 11th IEEE international conference and workshops on automatic face and gesture recognition (FG)*, vol. 1, pp. 1-7, IEEE, 2015.

46. Bhaskar Anand, and Prashant K. Shah, “Face recognition using SURF features and SVM classifier,” *International Journal of Electronics Engineering Research*, vol. 8, no. 1, pp. 1-8, 2016.

47. Haitham Farooq Ibrahim, "Human Face Recognition by Using Image Coding," *Journal of American Science,* vol. 10, no. 5, 2014.

48. Suchitra Basak, Ruting Jia, and Chengwei Lei, "Face Recognition using Fuzzy Logic," *2018 IEEE International Conference on Information and Automation (ICIA)*, pp. 1317-1322, IEEE, 2018.

49. Guanhao Yang, Wei Feng, Jintao Jin, Qujiang Lei, Xiuhao Li, Guangchao Gui, and Weijun Wang, "Face mask recognition system with YOLOV5 based on image recognition," *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, pp. 1398-1404, IEEE, 2020.

50. Jean-Marie Henckaerts, ed. “The international status of Taiwan in the new world order: legal and political considerations,” *Martinus Nijhoff Publishers*, 1996.

51. Renliang Weng, Jiwen Lu, and Yap-Peng Tan, "Robust point set matching for partial face recognition," *IEEE transactions on image processing,* vol. 25, no. 3, pp. 1163-1176, 2016.

52. Dong Yi, Zhen Lei, Shengcai Liao, and Stan Z. Li, "Learning face representation from scratch," *arXiv preprint* arXiv:1411.7923, 2014.

53. Ramachandra Raghavendra, Kiran B. Raja, Bian Yang, and Christoph Busch, "Comparative evaluation of super-resolution techniques for multi-face recognition using light-field camera," *2013 18th International Conference on Digital Signal Processing (DSP)*, pp. 1-6, IEEE, 2013.

54. Kiran B. Raja, Ramachandra Raghavendra, Vinay Krishna Vemuri, and Christoph Busch, "Smartphone based visible iris recognition using deep sparse filtering," *Pattern Recognition Letters*, vol. 57, pp. 33-42, 2015.

55. Kiran B. Raja, R. Raghavendra, and Christoph Busch, "Smartphone based robust iris recognition in visible spectrum using clustered k-means features," *2014 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS)* Proceedings, pp. 15-21, IEEE, 2014.

56. Kiran B. Raja, Ramachandra Raghavendra, and Christoph Busch, "Iris imaging in visible spectrum using white LED," *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1-8, IEEE, 2015.

57. Mateusz Trokielewicz, Ewelina Bartuzi, Katarzyna Michowska, Antonina Andrzejewska, and Monika Selegrat, "Exploring the feasibility of iris recognition for visible spectrum iris images obtained using smartphone camera," *Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2015*, vol. 9662, pp. 641-648, SPIE, 2015.

58. Ajita Rattani, and Reza Derakhshani, "A survey of mobile face biometrics," *Computers & Electrical Engineering*, vol. 72, pp. 39-52, 2018.

59. Masao Yamazaki, Dongju Li, Tsuyoshi Isshiki, and Hiroaki Kunieda, "SIFT-based algorithm for fingerprint authentication on smartphone," *2015 6th International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES)*, pp. 1-5, IEEE, 2015.

60. Vincenzo Conti, Mario Collotta, Giovanni Pau, and Salvatore Vitabile, "Usability analysis of a novel biometric authentication approach for android-based mobile devicesm," *Journal of Telecommunications and Information Technology*, no. 4, pp. 34-43, 2014.

61. Shaveta Dargan, and Munish Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Systems with Applications*, vol. 143, pp. 113114, 2020.

62. Jiawei Hu, Liangrui Peng, and Li Zheng, "XFace: a face recognition system for android mobile phones," *2015 IEEE 3rd International Conference on Cyber-Physical Systems, Networks, and Applications*, pp. 13-18, IEEE, 2015.

63. Kiran B. Raja, Ramachandra Raghavendra, Martin Stokkenes, and Christoph Busch, "Multi-modal authentication system for smartphones using face, iris and periocular," *2015 International Conference on Biometrics (ICB)*, pp. 143-150, IEEE, 2015.

64. Farzana Rahman, Md Osman Gani, Golam Mushih Tanimul Ahsan, and Sheikh Iqbal Ahamed, "Seeing beyond visibility: A four way fusion of user authentication for efficient usable security on mobile devices," *2014 IEEE Eighth International Conference on Software Security and Reliability-Companion*, pp. 121-129, IEEE, 2014.

65. Swati K. Choudhary, and Ameya K. Naik, "Multimodal Biometric Authentication with Secured Templates—A Review," *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, pp. 1062-1069, IEEE, 2019.

66. Lorenzo Gomez, Iulian Neamtiu, Tanzirul Azim, and Todd Millstein, "Reran: Timing-and touch-sensitive record and replay for android," *2013 35th International Conference on Software Engineering (ICSE)*, pp. 72-81, IEEE, 2013.

67. Nathan L. Clarke, and Steven M. Furnell, "Authenticating mobile phone users using keystroke analysis," *International journal of information security*, vol. 6, no. 1, pp. 1-14, 2007.

68. Patrizio Campisi, Emanuele Maiorana, M. Lo Bosco, and Alessandro Neri, "User authentication using keystroke dynamics for cellular phones." *IET Signal Processing*, vol. 3, no. 4 pp. 333-341, 2009.

69. Nan Zheng, Kun Bai, Hai Huang, and Haining Wang, "You are how you touch: User verification on smartphones via tapping behaviors," *2014 IEEE 22nd International Conference on Network Protocols*, pp. 221-232, IEEE, 2014.

70. Seong-seob Hwang, Sungzoon Cho, and Sunghoon Park, "Keystroke dynamics-based authentication for mobile devices," *Computers & Security*, vol. 28, no. 1-2, pp. 85-93, 2009.

71. Anand Motwani, Raina Jain, and Jyoti Sondhi, "A multimodal behavioral biometric technique for user identification using mouse and keystroke dynamics," *International Journal of Computer Applications*, vol. 111, no. 8, pp. 15-20, 2015.

72. Valeriu-Daniel Stanciu, Riccardo Spolaor, Mauro Conti, and Cristiano Giuffrida, "On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks," *proceedings of the sixth ACM conference on data and application security and privacy*, pp. 105-112. 2016.

73. Xuan Huang, Geoffrey Lund, and Andrew Sapeluk, "Development of a typing behaviour recognition mechanism on android," *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 1342-1347, IEEE, 2012.

74. Sowndarya Krishnamoorthy, Luis Rueda, Sherif Saad, and Haytham Elmiligi, "Identification of user behavioral biometrics for authentication using keystroke dynamics and machine learning," *Poceedings of the 2018 2nd International Conference on Biometric Engineering and Applications*, pp. 50-57, 2018.

75. Junhong Kim, and Pilsung Kang, "Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features," *Pattern Recognition*, vol. 108, pp. 107556, 2020.

76. Nataasha Raul, Radha Shankarmani, and Padmaja Joshi, "A comprehensive review of keystroke dynamics-based authentication mechanism," *International Conference on Innovative Computing and Communications*, pp. 149-162, Springer, Singapore, 2020.

77. Pin Shen Teh, Ning Zhang, Andrew Beng Jin Teoh, and Ke Chen, "Recognizing your touch: Towards strengthening mobile device authentication via touch

dynamics integration," *Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia*, pp. 108-116, 2015.

78. Ka-Wing Tse, and Kevin Hung, "User behavioral biometrics identification on mobile platform using multimodal fusion of keystroke and swipe dynamics and recurrent neural network," *2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, pp. 262-267, IEEE, 2020.

79. Saira Zahid, Muhammad Shahzad, Syed Ali Khayam, and Muddassar Farooq, "Keystroke-based user identification on smart phones," *International Workshop on Recent advances in intrusion detection*, pp. 224-243, Springer, Berlin, Heidelberg, 2009.

80. Jatin Yadav and S Gupta, "Keystroke dynamics based authentication using fuzzy logic," *The tenth International Conference on Contemporary Computing (IC3)*, pp. 1-6, 2017.

81. Y. Zhong, Y. Deng and A.K. Jain, "Keystroke dynamics for user authentication", *IEEE Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 117-123, 2012.

82. Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE transactions on information forensics and security*, vol. 8, no. 1 pp. 136-148, 2012.

83. Yuxin Meng, Duncan S. Wong, and Roman Schlegel, "Touch gestures based biometric authentication scheme for touchscreen mobile phones," *International conference on information security and cryptology*, pp. 331-350. Springer, Berlin, Heidelberg, 2013.

84. Elakkiya Ellavarason, Richard Guest, and Farzin Deravi, "A framework for assessing factors influencing user interaction for touch-based biometrics," *2018 26th European Signal Processing Conference (EUSIPCO)*, pp. 553-557, IEEE, 2018.

85. Yuxin Meng, Duncan S. Wong, and Lam-For Kwok, "Design of touch dynamics based user authentication with an adaptive mechanism on mobile phones," *Proceedings of the 29th annual ACM symposium on applied computing*, pp. 1680-1687, 2014.

86. Minori Inoue, and Takefumi Ogawa, “TapOnce: a novel authentication method on smartphones,” *International Journal of Pervasive Computing and Communications*, vol. 14, no. 1, 2018.

87. Jin Su Kim, Gen Li, Byungjun Son, and Jaihie Kim, "An empirical study of palmprint recognition for mobile phones," *IEEE Transactions on Consumer Electronics*, vol. 61, no. 3, pp. 311-319, 2015.

88. Ahmad Zairi Zaidi, Chun Yong Chong, Zhe Jin, Rajendran Parthiban, and Ali Safaa Sadiq, "Touch-based continuous mobile device authentication: State-of-the-art, challenges and opportunities," *Journal of Network and Computer Applications*, vol. 191, pp. 103162, 2021.

89. Muhammad Irwan Padli Nasution, Nurbaiti Nurbaiti, Nurlaila Nurlaila, Tri Inda Fadhila Rahma, and Kamilah Kamilah, "Face Recognition Login Authentication for Digital Payment Solution at COVID-19 Pandemic," *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)*, pp. 48-51. IEEE, 2020.

90. Jonathan Talahua, S., Jorge Buele, P. Calvopiña, and José Varela-Aldás, "Facial recognition system for people with and without face mask in times of the covid-19 pandemic," *Sustainability*, vol. 13, no. 12, pp. 6900, 2021.

91. Jackson G. Lu, Peter Jin, and Alexander S. English, "Collectivism predicts mask use during COVID-19," *Proceedings of the National Academy of Sciences*, vol. 118, no. 23, 2021.

92. Ernestine Atangana, and Abdon Atangana, "Facemasks simple but powerful weapons to protect against COVID-19 spread: Can they have sides effects?," *Results in physics*, vol. 19 pp. 103425, 2020.

93. Meiling Fang, Naser Damer, Florian Kirchbuchner, and Arjan Kuijper, "Real masks and spoof faces: On the masked face presentation attack detection," *Pattern recognition,* vol. 123, pp. 108398, 2022.

94. Adnane Cabani, Karim Hammoudi, Halim Benhabiles, and Mahmoud Melkemi, "MaskedFace-Net–A dataset of correctly/incorrectly masked face images in the context of COVID-19," *Smart Health,* vol. 19, pp. 100144, 2021.

95. Mingjie Jiang, Xinqi Fan, and Hong Yan, "Retinamask: A face mask detector," *arXiv preprint* arXiv:2005.03950, 2020.

96. Soad Almabdy, and Lamiaa Elrefaei, "Deep convolutional neural network-based approaches for face recognition," *Applied Sciences,* vol. 9, no. 20, pp. 4397, 2019.

97. Hazar Mliki, Sahar Dammak, and Emna Fendri, "An improved multi-scale face detection using convolutional neural network," *Signal, Image and Video Processing,* vol. 14, no. 7, pp. 1345-1353, 2020.

98. Enrique David Martí Muñoz, "A framework for context-aware sensor fusion," *PhD diss., Universidad Carlos III de Madrid*, 2015.

99. Max Landman, "Managing smart phone security risks," *2010 Information Security Curriculum Development Conference,* pp. 145-155, 2010.

100. T. Sabhanayagam, V. Prasanna Venkatesan, and K. Senthamaraikannan, "A comprehensive survey on various biometric systems," *International Journal of Applied Engineering Research,* vol. 13, no.5, pp. 2276-2297, 2018.

101. Atul N. Kataria, Dipak M. Adhyaru, Ankit K. Sharma, and Tanish H. Zaveri, "A survey of automated biometric authentication techniques," *2013 Nirma university international conference on engineering (NUiCONE)*, pp. 1-6, IEEE, 2013.

102. Nicolas Ortiz, Ruben Dario Hernández, Robinson Jimenez, Mauricio Mauledeoux, and Oscar Avilés, "Survey of biometric pattern recognition via machine learning techniques," *Contemporary Engineering Sciences,* vol. 11, no. 34, pp. 1677-1694, 2018.

103. S. Prabu, M. Lakshmanan, and V. Noor Mohammed, "A multimodal authentication for biometric recognition system using intelligent hybrid fusion techniques," *Journal of medical systems,* vol. 43, no. 8, pp. 1-9, 2019.

104. Soyuj Kumar Sahoo, Tarun Choubisa, and SR Mahadeva Prasanna, "Multimodal biometric person authentication: A review," *IETE Technical Review*, vol. 29, no. 1, pp. 54-75, 2012.

105. Arun A. Ross, and Rohin Govindarajan, "Feature level fusion of hand and face biometrics," *Biometric technology for human identification II*, vol. 5779, pp. 196-204, SPIE, 2005.

106. Kyong Chang, Kevin W. Bowyer, Sudeep Sarkar, and Barnabas Victor, "Comparison and combination of ear and face images in appearance-based biometrics," *IEEE Transactions on pattern analysis and machine intelligence,* vol. 25, no. 9, pp. 1160-1165, 2003.

107. Arun Ross, and Anil Jain, "Information fusion in biometrics," *Pattern recognition letters,* vol. 24, no. 13, pp. 2115-2125, 2003.

108. Arun A. Ross, Karthik Nandakumar, and Anil K. Jain, "Handbook of multibiometrics," vol. 6, Springer Science & Business Media, 2006.

109. Tomi Kinnunen, Ville Hautamäki, and Pasi Fränti, "Fusion of spectral feature sets for accurate speaker identification," *Proceedings of the 9th conference speech and computer,* pp. 361–365, 2004.

110. S. Gopal Krishna Patro, Kishore Kumar Sahu, "Normalization: A Preprocessing Stage," arXiv preprint arXiv:1503.06462, 2015

111. Yuhua Wang, Chunhua Wu, Kangfeng Zheng, and Xiujuan Wang, "Improving reliability: User authentication on smartphones using keystroke biometrics," *IEEE Access*, vol. 7, pp. 26218-26228, 2019.

112. "The Mobile Economy," GSMA.com, https://www.gsma.com/mobileeconomy (accessed Mar. 2, 2021).

113. Claire Jarrett and Olivia Shalofsky, “Apple products too a-peeling for thieves,” [online] DLG Corporate Corporate Website, available at: https://www.directlinegroup.co.uk/en/news/brand-news/2017/apple-products-too-a-peeling-for-thieves.html, [accessed 7 Mar. 2022].

114. Lukas Aron, and Petr Hanacek, "Overview of security on mobile devices," *2015 2nd World Symposium on Web Applications and Networking (WSWAN)*, pp. 1-11, IEEE, 2015.

115. Anselmo Lacerda, Ruy de Queiroz, and Márcio Barbosa, "A systematic mapping on security threats in mobile devices," *2015 Internet Technologies and Applications (ITA)*, pp. 286-291, IEEE, 2015.

116. Mohammed E. Fathy, Vishal M. Patel, and Rama Chellappa, "Face-based active authentication on mobile devices," *2015 IEEE international conference on acoustics, speech and signal processing (ICASSP)*, pp. 1687-1691, IEEE, 2015.

117. Qian Tao, and Raymond Veldhuis, “Biometric authentication system on mobile personal devices,” *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, pp. 763-773, 2010.

118. Varun Mishra, “More than a billion feature phones to be sold over next three years,” Counterpointresearch.com, available at: https://www.counterpointresearch.com/more-than-a-billion-feature-phones-to-be-sold-over-next-three-years, 2019. [accessed Mar. 10, 2021]

119. H. Abdul Shabeer, and P. Suganthi, "Mobile phones security using biometrics," *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, vol. 4, pp. 270-274, IEEE, 2007.

120. Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra, "A survey on security for mobile devices," *IEEE communications surveys & tutorials*, vol. 15, no. 1, pp. 446-471, 2012.

121. Roman V. Yampolskiy, and Venu Govindaraju, “Behavioural biometrics: a survey and classification,” *International Journal of Biometrics*, vol. 1, no. 1, pp. 81-113, 2008.

122. Ala. EL MASRI, “Active authentication using behavioral biometrics and machine learning,” *PhD diss.*, 2016.

123. Ting-Yi Chang, Cheng-Jung Tsai, Jen-Yuan Yeh, Chun-Cheng Peng, and Pei-Hsuan Chen, "New soft biometrics for limited resource in keystroke dynamics authentication," *Multimedia Tools and Applications*, vol. 79, no. 31, pp. 23295-23324, 2020.

124. Soumik Mondal and Patrick Bours, "A study on continuous authentication using a combination of keystroke and mouse biometrics," *Neurocomputing*, vol. 230, pp. 1-22, 2017.

125. Hyungu Lee, Jung Yeon Hwang, Dong In Kim, Shincheol Lee, Sung-Hoon Lee, and Ji Sun Shin, "Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors," *Security and Communication Networks*, 2018, pp. 1-10, 2018.

126. Dong In Kim, Shincheol Lee, and Ji Sun Shin, "A new feature scoring method in keystroke dynamics-based user authentications," *IEEE Access*, vol. 8 pp. 27901-27914, 2020.

127. Daria Frolova, Anna Epishkina, and Konstantin Kogos, "Mobile user authentication using keystroke dynamics," 2*019 European Intelligence and Security Informatics Conference (EISIC)*, pp. 140-140. IEEE, 2019.

128. Aashish Mehra, Facial Recognition Market worth $8.5 billion by 2025. Available at: https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp.

129. Modesto Castrillón, Oscar Déniz, Daniel Hernández, and Javier Lorenzo, "A comparison of face and facial feature detectors based on the Viola–Jones general object detection framework," *Machine Vision and Applications*, vol. 22, no. 3, pp. 481-494, 2011.

130. Athena, What is a Haar classifier, Available at: http://athenanichol.com/blog/?p=127.

131. Sensetime, Available at: https://www.sensetime.com/en

132. Hanvon, Available at: https://www.hanvon.com

133. Minivision, Available at: https://www.crunchbase.com/organization/minivision