

# USER AUTHENTICATION USING PASSWORD AND HAND GESTURE WITH LEAP MOTION SENSOR

by

Mishkat Haider Chowdhury

17201032

Qazi Shadman

16101194

Sakib Al Hasan

15301035

Md Adib Hassan

16101324

A thesis submitted to the Department of Computer Science and Engineering  
in partial fulfillment of the requirements for the degree of  
B.Sc. in Computer Science and Engineering

Department of Computer Science and Engineering  
BRAC University

© 2020. BRAC University  
All rights reserved.

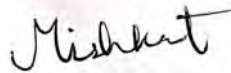
# Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at BRAC University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Type your text

Student's Full Name & Signature:



---

Mishkat Haider Chowdhury  
17201032



---

Qazi Shadman  
16101194



---

Sakib Al Hasan  
15301035



---

Md Adib Hassan  
16101324

# Approval

The thesis/project titled “USER AUTHENTICATION USING PASSWORD AND HAND GESTURE WITH LEAP MOTION SENSOR” submitted by

1. Mishkat Haider Chowdhury (17201032)
2. Qazi Shadman (16101194)
3. Sakib Al Hasan (15301035)
4. Md Adib Hassan (16101324)

Of Spring, 2020 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on April, 2020.

## Examining Committee:

Supervisor:  
(Member)



---

Dr. Jia Uddin  
Assistant Professor (Research Track)  
Technology Studies, Endicott College, Woosong University  
Associate Professor (On leave)  
Department of Computer Science and Engineering  
BRAC University

Thesis Coordinator:  
(Member)

---

Dr. Md. Golam Rabiul Alam  
Associate Professor  
Department of Computer Science and Engineering  
BRAC University

Head of Department:  
(Chair)

---

Dr. Mahbub Alam Majumdar  
Professor  
Department of Computer Science and Engineering  
BRAC University

# Abstract

User Authentication is becoming a significant factor in the field of modern technology. It is a process that permits a device to confirm the recognition of somebody who interfaces with a system asset. In the world of AI, machine learning is currently one of the leading research fields which is looking into practical implementation. In this report, we propose a method where the user will enter the given password while leap motion sensor will compare the behavioural data of the user with an existing dataset. Leap motion controller is a sensor or gadget which can recognize 3D movement of hands, fingers and finger like articles with no contact. Moreover we will be discussing the benefits of using behavioural biometrics instead of physiological biometrics for security, and how behavioural biometrics can solve the faults of physiological biometrics. In addition, we will be discussing the benefits of using leap motion sensor along with password authentication to properly identify an user and how it can improve security. For our project, we chose to use Dynamic Time Warping and Naive Bayes Classifier algorithm. DTW algorithm will be useful by comparing two frames which differ in time or velocity when one user have multiple behavioral entries before identifying user as valid or invalid. Naive Bayes will classify a user as valid or invalid through allowing classifiers to learn user data through features. The proposed system has about 91% accuracy which rises to 93% in the best-case scenario. We believe that because Leap Motion is comparatively low cost at the exchange of an extra layer of security it provides, the proposed system can ensure a secure and efficient environment for user authentication.

**Keywords:** DTW(Dynamic Time Warping); Naive Bayes Classifier; Leap Motion Sensor; Password Authentication; Physiological Biometrics; Behavioral Biometrics; FRR(False Rejection Rate); FAR(False Acceptance Rate)

## **Acknowledgement**

Firstly, all praise to the Great Allah for whom our thesis have been completed without any major interruption.

Secondly, to our supervisor Dr, Jia Uddin sir and co-supervisor Ismail Hossain sir for their kind support and advice in our work. They helped us whenever we needed help and pushed us beyond our limit to bring out the best out of us.

And finally to our parents for always supporting us through the whole period. Without their support it may not be possible. With their benevolent help and support we are now completing our graduation from this prestigious institution.

# Table of Contents

Declaration	i
Approval	ii
Abstract	iii
Acknowledgment	iv
Table of Contents	v
List of Figures	vii
List of Tables	viii
Nomenclature	ix
<b>1 Introduction</b>	<b>1</b>
1.1 Motivation . . . . .	1
1.2 Contribution . . . . .	2
1.2.1 Problem Statement . . . . .	2
1.2.2 Solution . . . . .	2
1.2.3 Methodology . . . . .	3
1.3 Thesis Orientation . . . . .	4
<b>2 User Authentication</b>	<b>6</b>
2.1 Defination of User Authentication . . . . .	6
2.2 User Verification Factors . . . . .	7
2.3 Types of User Authentication . . . . .	7
2.3.1 Single Factor Verification . . . . .	8
2.3.2 Two Factor Verification . . . . .	8
2.3.3 Verification of Multiple Factors . . . . .	9
2.3.4 Physiological Biometrics . . . . .	9
2.3.5 Behavioral Biometrics . . . . .	11
2.4 Physical Biometric Authentication vs Behavioral Biometric Authentication . . . . .	15
2.5 Benefits of Behavioral Authentication . . . . .	16
<b>3 Leap Motion Sensor</b>	<b>18</b>
3.1 Defination of Leap Motion Sensor . . . . .	18
3.2 History . . . . .	19

3.3	Mechanism . . . . .	19
3.3.1	Hardware . . . . .	19
3.3.2	Software . . . . .	19
3.4	Developers . . . . .	20
<b>4</b>	<b>Literature Reviews</b>	<b>21</b>
<b>5</b>	<b>Proposed Model</b>	<b>24</b>
5.1	Dynamic Time Warping (DTW) . . . . .	24
5.2	Naive Bayes . . . . .	25
5.3	Mechanism of the Proposed Model . . . . .	26
<b>6</b>	<b>Collecting and Processing The Dataset</b>	<b>28</b>
6.1	Dataset Collection . . . . .	28
6.1.1	Frame Data . . . . .	28
6.1.2	Hand Data . . . . .	28
6.1.3	Finger Data . . . . .	29
6.2	Processing the Dataset . . . . .	30
<b>7</b>	<b>Result Analysis</b>	<b>32</b>
7.1	Applying DTW Algorithm . . . . .	32
7.2	Results of applying DTW Algorithm . . . . .	33
7.3	Applying Naïve Bayes Algorithm . . . . .	34
7.4	Results of applying Naïve Bayes Algorithm . . . . .	34
7.5	Comparison of Results . . . . .	36
<b>8</b>	<b>Conclusion</b>	<b>38</b>
8.1	Future Uses . . . . .	38
	<b>Bibliography</b>	<b>42</b>

# List of Figures

1.1	Methodology of our proposed method . . . . .	3
2.1	User Authentication System . . . . .	6
2.2	One factor Verification System . . . . .	8
2.3	Two factor Verification System . . . . .	8
2.4	Multi Factor Verification System . . . . .	9
2.5	Physiological Biometrics System . . . . .	10
2.6	Retina scan technology . . . . .	10
2.7	Iris identification mechanics . . . . .	11
2.8	Finger vein identification . . . . .	11
2.9	Behavioral Biometrics System . . . . .	12
2.10	Keystroke biometrics authentication . . . . .	13
2.11	Gait Analysis . . . . .	14
2.12	Cognitive Biometrics of Human Brain . . . . .	14
3.1	Leap Motion Sensor . . . . .	18
3.2	Hand Illuminated by Leap Motion Controller's LEDs . . . . .	20
5.1	Two analytical series adjusted by DTW . . . . .	24
5.2	Graphical representation of DTW . . . . .	25
5.3	Normal distribution for Gaussian Naive Bayes . . . . .	26
5.4	Block Diagram of Registering User in the System . . . . .	26
5.5	First Layer of User Authentication . . . . .	27
5.6	Second Layer of User Authentication . . . . .	27
6.1	Code for determining hand type . . . . .	28
6.2	Code for calculating pitch, roll and yaw . . . . .	29
6.3	Code for determining finger type . . . . .	29
6.4	Code for serializing frame data . . . . .	30
6.5	Code for deserializing frame data . . . . .	31
7.1	Relationship between number of inputs and number of false rejections	33
7.2	Relationship between number of inputs and number of false rejections	35
7.3	Relationship between number of inputs and number of false rejections	36
7.4	Comparison chart between DTW and Naïve Bayes . . . . .	36
7.5	Comparison chart between DTW and Naïve Bayes(without behav- ioral features) . . . . .	37



# List of Tables

7.1	Experimental result for DTW algorithm authentication . . . . .	33
7.2	Features used for Naive Bayes authentication . . . . .	34
7.3	Experimental result for Naive Bayes algorithm authentication . . . .	34
7.4	Experimental result for Naive Bayes algorithm authentication(without behavioral features) . . . . .	35

# Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

*2FV* Two Factor Verification

*AC* Alternating Current

*AI* Artificial Intelligence

*AR* Augmented Reality

*DTW* Dynamic Time Warping

*ECG* Electrocardiogram

*EEG* Electroencephalogram

*FAR* False Acceptance Rate

*FRR* False Rejection Rate

*IoT* Internet of Things

*LED* Light Emiting Diode

*MFV* Multi Factor Verification

*PC* Personal Computer

*RFID* Radio Frequency Identification

*VR* Virtual Reality

# Chapter 1

## Introduction

Authentication plays a vital role in securing various corporate offices or electronic resources. In order to keep an organization's system secure authentication plays a very important role. In this current world among Artificial Intelligence, machine learning is one of the leading research fields which is also applicable for practical implementations. While it has greatly flourished in other sectors, it is still being thoroughly researched in security. Various types of authentication mechanisms have been proposed in the past. Recently there has been a great need to enhance security to various electronic resources. These days various types of authentications processes has been performed. By using this method the main focus part is confirming the character of the user by utilizing behavioral biometrics such as keystroke dynamics, voice recognition, mouse dynamics etc. Among them authentication using leap motion sensor is a more reliable way of securing resources. The Leap Motion Sensor is a customer gesture sensor which intends to increase a user's interactive involvement to their computer. The Leap Motion Sensor is basically a camera based device which captures hand gestures from a user to give an input. In this paper we are proposing a new and more efficient method of authentication using password and leap motion sensor. The method that we are proposing in this paper, there is a very minimum chance for any sort of token theft as it is quite impossible to copy someone's hand gesture.

### 1.1 Motivation

With the advancement of technology the uses of digital devices including computer has increased immensely. Due to this increase a large number of important documents of various organizations are stored in the computer. As a result computer security is a very important factor now. User authentication mainly focuses on 3 types which includes information based, biometric based and token based. [11] Information based which can also be said as knowledge based mainly includes use of text password but this has a lot of demerits as the electronic medium cannot recognize the person with just text passwords. Token based authentication such as RFID keys, smart card, smartphones are also vulnerable to token theft. However the biometric based such as voice recognition, fingerprints, iris patterns has minimum chances of identity theft. Among the biometric based authentication we believe that the behavioral scanners such as leap motion sensors are now on the way to be used for more reliable and secured medium for user authentication. [28] If we look at the

current world we all can see the various types of cybercrime that is happening. In 2016 an amount of \$81M had been stolen from Bangladesh Bank through hacking [16]. Other than that there have been found cases of blackmailing people by hacking their social media accounts. Many large industries are getting spied by hacking their websites. Different unauthorized accesses happened to different institutions through which important datas has been changed, stolen, erased etc. Moreover there is a group of people who logs in to different networks through unauthorized ways and spreads malware. Some malwares are very deadly that it destroys the entire network. Years of hardwork of people are getting destroyed through hacking. Therefore above all we can see the necessary of increasing computer security. That is why we came with the idea of user authentication using password and hand gesture with leap motion sensor.

## **1.2 Contribution**

### **1.2.1 Problem Statement**

Due to the immense advancement of technology in this era the use of digital devices has increased to a great extent. Many big organizations keep their organizational data online through cloud or their own websites. So as a result security is a very important factor here. There are various types of security which includes information based, biometric based and token based. [11] Information based consist of mainly text passwords. But it cannot ensure complete security as the password can be hacked easily. Anyone knowing the password can access the data of that specific person. Token based authentication consist of authentication through RFID keys, smart card, smartphones etc. These authentications are highly vulnerable to token theft as now a days everything can be copied starting from fingerprint to Iris Scan. So we can see that complete security cannot be established through knowledge based and token based. With the advancement of technology experts started to believe that two-factor authentication would be the answer. But even in this it is still dependent on text passwords. Few study shows that many people uses the same characters repeatedly for passwords in order to remember the password. They mainly rely on common terms like birthday date, phone number, name etc. Two-factor authentication is not only a slow process but also if the thief can steal the token then the thief can get access to all the information. Thus it can be stated that the security given in two factor authentication is not much efficient. Cmarsden[13] suggested that due to the IoT landscape being more complex, biometric security is the way forward.

### **1.2.2 Solution**

We have seen so far the demerits of knowledge based and token based authentication system on how they can easily be hacked. Therefor the solution is to focus more on biometric based authentication system. Anyone who knows the password can go through in token based authentication but in biometric authentication that specific individual is needed to go through. Biometric security cannot be forged at all without the specific individual. By any chance if any unfortunate event occurs such as if someone forcefully forged into then that can be easily identified as there will

be proof of confirmation which is backed by data. Every big organizations expects better security system. This biometric authentication system enhances security of the device or system and also at the same time make it simpler and increasingly productive to manage key functions. One of the major factor of using this biometric is convenience. The passwords does not need to be reset timely as once the biometric test is activated all finger prints, iris etc are done. Once the biometric authentication system is activated no more costing or investment is needed for security. These systems are additionally basic to preventing loss due to illegal entries. This authentication system is very easy to operate and there is a very negligible chances for failures. Manan[29] suggested to move forward with biometric authentication system as it is on the way to become a key to various factors authentication and it is used for a vast number of purposes. Now a days the giant institutions are embracing biometric authentication system instead of knowledge based or token based. They rely more on biometric based because of this efficiency in the security system. More over there is a very less chance of theft in this system. Overall it can be said that with the immense advancement of science and technology we have to move forward with biometric based authentication system.

### 1.2.3 Methodology

Biometric based authentication are of various types. One of the most efficient type is by using leap motion sensor. Figure 1.1 shows the mechanism of our method through a flowchart. The way it will work is that, an user will enter a password on a device. While typing the password, the leap motion device will scan and analyze the movement of the hands of the user. After the password is entered the system will perform a 2-step authentication. Firstly, it will verify if the password is correct or not. If it is correct, then secondly it will compare the leap motion data of the user with it's pre-stored dataset. If it finds a match, then the user will be authenticated. The user must pass both steps of authentication to be verified. In this way the system becomes more secure even if the password gets leaked.

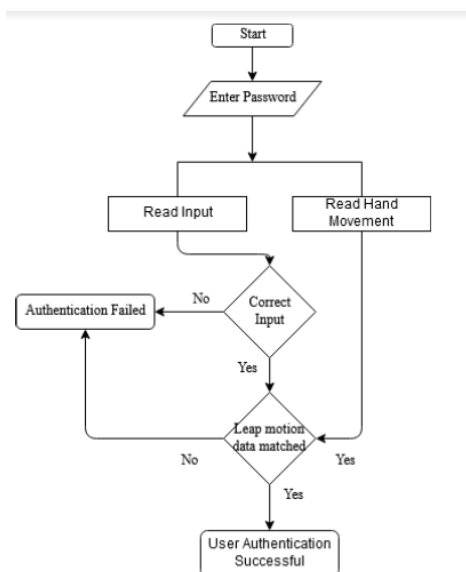


Figure 1.1: Methodology of our proposed method

## 1.3 Thesis Orientation

The rest of our research is organized in the following order:

### Chapter 1

In the introduction section we briefly discussed about the real world scenario. Afterwards we described about the motivation for doing this research work. We then discussed about the problems regarding the recent existing methods and we talked about it's solution. Lastly we discussed about a methodology that we will follow.

### Chapter 2

In the user authentication chapter we discussed about it's definition and different factors, types and benefits of it.

### Chapter 3

In the Leap Motion Sensor we discussed about the Leap Motion device including its history, mechanism and developers community.

### Chapter 4

In the literature review section we discussed and reviewd about the previous arelated works of the similar topic.

### Chapter 5

In the methodology section we discussed about the algorithms that we will use for our research.

### Chapter 6

In this chapter we discussed about the datas we collected for implementation and how we processed it.

### Chapter 7

In this chapter we discussed about the results we got after applying the algorithms. Afterwards we compared diferent outcomes.

## Chapter 8

In conclusion we gave a summary about our works till now and we also discussed about the scopes for future improvements.

# Chapter 2

## User Authentication

### 2.1 Defination of User Authentication

User verification is the authentication of an authorization transmission from individual to device needed to ensure a user's identity; the concept is in contrast to computer verification, which requires automatic not automatic processes need end user entry [8]. In order to access an end user's account, they have to register for a new account with unique ID and password which eventually allow them to access their account later. Nevertheless, modern networks need far more than pure identification of users. With your network protection on the line, you have got a lot to risk by not checking and controlling who is accessing your resources. User checks are performed in almost every non-guest human-to-machine contact, and log into accounts automatically. Verification enables links between people and computers on wired and mobile networks so that they can access the networked devices and services associated with the Internet. Historically, user verification was a basic combination of ID and key. Nonetheless, more verification factors are being added to boost the security of communications. [24].



Figure 2.1: User Authentication System

Here figure 2.1 shows different types of authentication system for an end user. Starting from bottom left a user can secure his data on cloud storage using a unique username and password. After trying to login or sign up to cloud storage using his/her



very own unique ID and password he/she may be asked for a verification code which is sent to his/her mobile device. After successfully going through the steps he/she will be permitted to access the cloud storage. On the bottom right part of Figure 2.1 it shows another method where user can secure his/her data using fingerprint and password. He/she can unlock his desired device using any of these two methods.

## 2.2 User Verification Factors

If the client wishes to demonstrate his identification, he must provide a fact known mostly to the database and the end user. This information is called verification. Mainly three factors are there for user verification. Those are: [24]

1. Factors of expertise: - A element of knowledge is named that must be known to the user for login. It can be a name, key, or pin number. The problem is that they can be weak as regards security since they can be exchanged or estimated.
2. Factors of Ownership: - The procedure an end user must follow to sign up is referred to as the ownership element. Password token, keypads, Identification cards and tangible badges are all called possession factors.
3. Factors of heritage: - Biological features of an individual are known as a heritage factor. Every biometric identification technique, including identification of face and scanning the fingerprints , will fall into this category.

As a fourth authentication feature, user location is often used. Smartphones universality would help to minimize workload there. Most smartphones have GPS, allowing a fair verification of the login location. Including the login point MAC address or the presence test by chips and other ownership factor elements [8].

## 2.3 Types of User Authentication

We've seen over the last couple of years that even the largest businesses are not prone to security breaches. Big wigs like Facebook, Target, Home Depot and Sony Pictures have been breaking into their networks, exposing confidential details about their owners, staff and consumers. With millions of passwords, email addresses and more being revealed, the burden on those who manage corporate security to update their defenses has been rising [32].

Since it's hard to keep up with how easily cyber criminals can advance their device awareness, network administrators have faced several problems and have had to start introducing more advanced ways to authenticate users. The types of authentication system used nowadays are discussed below: -

### 2.3.1 Single Factor Verification

The simplest and most common form of verification is also called primary testing. Of course, only one verification method for equipment or services, including key, encryption code, PIV token and so on, requires a one factor verification. Although these methods are highly accessible and familiar, they are typically connected to the protection below and can easily be intercepted or retrieved by loss of data, deletion or tracking the record of keystrokes.[32].



Figure 2.2: One factor Verification System

In this figure 2.2 an end user will provide his/her username and password to log into his/her device. Verification code or other methods of authentication like FaceID, Voice ID will not be needed here. That is the reason this type of verification is called one factor verification system.

### 2.3.2 Two Factor Verification

The second element for verifying the identity of a user is introduced by 2FV. One Time keys or Pin codes are common examples, generated by a licensed computer. With two verification methods alone, the protection status is dramatically improved according to Symantec's investigation, 80 percent of data breaches can be prevented by 2FV. While the safety benefits of 2FV are well known, acceptance was a common issue. With less than ten per cent of users using 2FV in 7 years since Google first introduced the possibility to add two verification mechanisms to its domains. According to Google, the annoyance triggering the 2FV was that more than 10 percent of 2FV users were unable to enter the password correctly. [32].

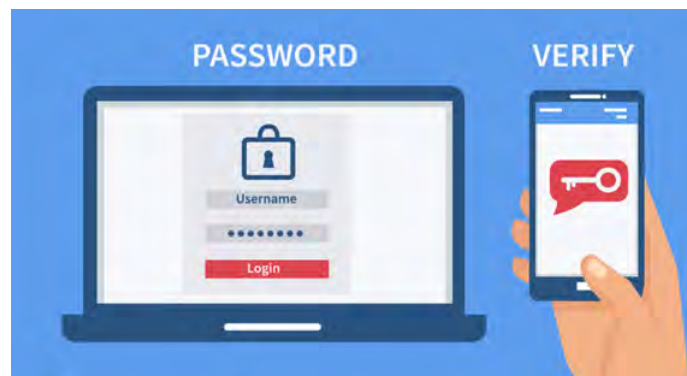


Figure 2.3: Two factor Verification System

Figure 2.3 shows the process of how a user can get access to his/her gadget by two layer of authentication system. First, he/she will enter his/her specific username and password into the login or signup page of the device. A verification will then be sent to his mobile number or email address by which user can verify that he is not an intruder and then he/she will be permitted to enter into their desired device.

### 2.3.3 Verification of Multiple Factors

Multi-Factor Authentication (MFV) is the most advanced form of validation that uses two or more variables to provide authentication to clients to a machine. MFV strategies work in common situations at least two or three classes below. Efficiency in verification is affected not just by the number of different criteria involved but also by the different systems and the way they are implemented. Perfectly constructed and correctly enforced policy ensure security for user verification.

In any case, this is also crucial not to overwhelm customers with difficult validation schedules that lead to infringements that undermine the purpose. Multi-factor tests (MFV) with automated processes boost security and reduce user effort at the same time. [16].

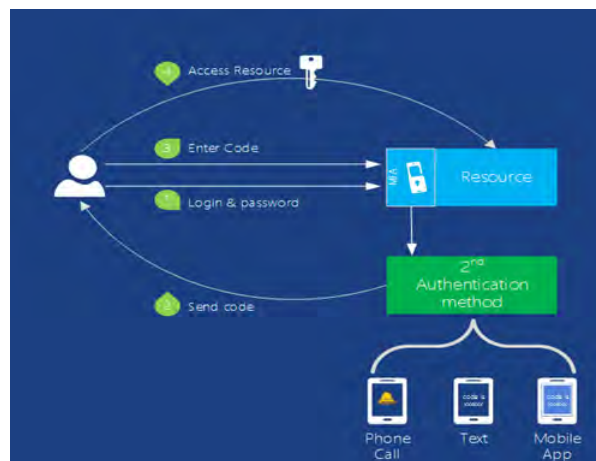


Figure 2.4: Multi Factor Verification System

In Figure 2.4 user have to provide his/her login credentials to access his/her resource. Then the user will get a verification code to his/her mobile device through a phone call or text message. After entering the verification code into the device that he/she trying to login, he might be asked to provide fingerprint or face verification or verify his/her signature to access the resource.

### 2.3.4 Physiological Biometrics

Physiology verification is a mechanism of protection which depends on a person's biological quality to ensure it is who he or she is. Physiological verification systems equate the capture of biometric data to the registered, accurate data validated in a databasd. If biometric datais suited by both samples, it confirms verification. Physiological Biometric verification is usually used for controlling physical access

control and digital resources such as houses, spaces, and computer equipment. This verification approach is also considered to be one of the safest solutions for users since all biological elements are unique and cannot easily be replicated.

Once seen only in spy movies, physiological biometric authentication is now a days increasing to great extent. The adoption of physiological biometric authentication was also motivated by convenience in extension to protection offered by hard-to-fake individual biological traits: one cannot easily forget or lose one's biometrics. Fingerprinting is the earliest known application of Physiological biometric Identification. As far back as the ancient China, thumbprints made on clay seals were used as a form of distinctive identification. Modern biometric validation has gotten practically quick, with the rise of electronic databases with Analog Data Digitization [6]. It can be clearly seen in Figure 2.5 about different methods of physical biometrics.

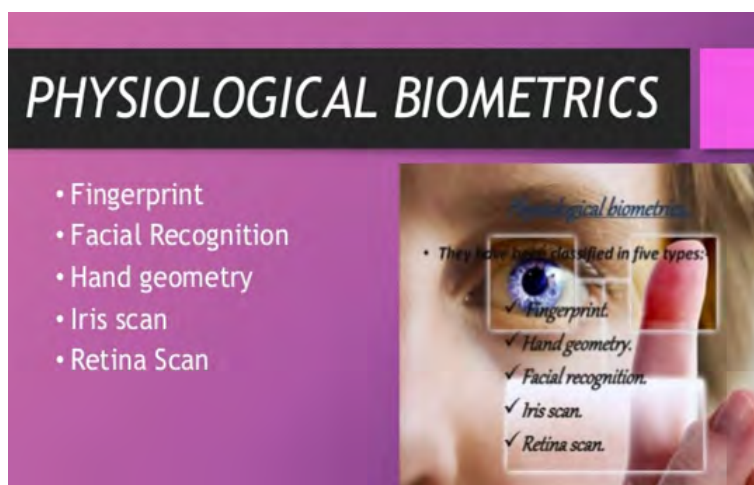


Figure 2.5: Physiological Biometrics System

### Types of physiological biometric authentication technologies

- Retina scans include a picture of the pattern of light-sensitive surface blood vessels which lines the person's inner eye.

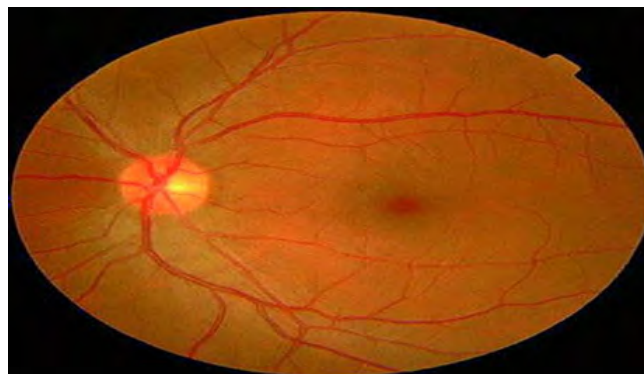


Figure 2.6: Retina scan technology

Fig 2.6 shows blood vessel and retina of a user being scanned for authentication which will be matched with the pre-loaded dataset to him/her give access to system.

- Iris identification is used to identify individuals within the ring-shaped area surrounding the eye pupil, based on unique patterns.



Figure 2.7: Iris identification mechanics

In figure 2.7 mathematical pattern on video images of a user's iris is collected which is distant and special. The iris data of user is matched too with given dataset.

- The finger vein identification is based on the history of the vein of a human.



Figure 2.8: Finger vein identification

Fig 2.8 shows a method that uses a vein pattern within one finger to identify a user and compare his/her finger data with existing dataset to give access to the system.

- Facial recognition mechanisms function with Faceprint numerical codes interpreting 80 nodal based on a human face [6].

### 2.3.5 Behavioral Biometrics

Behavioral biometrics is the area of research related to the identification of unusual patterns that are defined and observable in human activities. The word appears differently in relation to physical biometrics, including inborn human highlights [14].

Biometric behavioral authentication recognizes an individual based on specific patterns when communicating with devices such as a laptop, smartphone or computer (including mouse and keyboard). Considered considerations include everything from the finger pressure on the keypad to the angle at which you are holding your handset. It's about how the individual uses the app with behavioral biometrics — the speed of their typing, how they use their mouse and more instead of if their password has been entered correctly. These patterns allow the user to get a real, passive, or less invasive, frictionless authentication. This is simplified further by using current hardware resources, which prevents additional cost to the sensor. During collection and authentication biometric data is usually encrypted to improve protection and avoid using biometric identity theft credentials. After biometric data has been obtained, the software system selects different data points. The match points of the server are evaluated using a numerical value algorithm. Compare the completeness of the database to the biometric data entered by the end-user and approve and deny authentication. [25].

In Figure 2.9 few types of behavioral biometrics types are shown. Examples of behavioral trends the way people walk, called gait recognition the way people keep and communicate with a phone / tablet the way people use their cursor, known as cursor biometrics, the way people type on their keyboards, known as biometric typing or keystroke dynamics [25].



Figure 2.9: Behavioral Biometrics System

### Types of Behavioral Authentication Technologies

- Keystroke dynamics are the rhythm and timing patterns produced when one person types. Dynamics of the keystroke include:
  1. Average speed Variations in speed traveling between different keys.
  2. Prevalent Errors.
  3. The amount of time keys is depressurized.

A typeprint is an individual's characteristic keystroke dynamic; typeprint analysis is often used as a two-factor authentication feature for password hardening. Used in conjunction with other data, the typeprint analysis can help to define an person positively in circumstances where there is doubt [14].

In this fig 2.10 typing pattern of a user is captured and matched with database while





Figure 2.10: Keystroke biometrics authentication

dwell time is the span of the key stroke and the interval between keystrokes is the duration of flight.

- Voice ID or voice verification is a form of user authentication when using biometrics from VoicePrint, Voice ID is focused on that each person has unique voice Functions, like fingerprints and iris patterns.

Not by more complex considerations, but by the shape of the mouth and throat of the speaker, are the criteria on which a voice ID system dependent decision. Due to the obvious solidity of the track features, the device is not likely to be fooled by attempts to distort the voice and not even by modifications which may make it sound very different from the human ear, such as bad cold or extreme emotional feeling. A user's voice is recorded to establish what is called a voiceprint for comparison with samples for a user identity during a voice authentication system enrollment. To order to frustrate attempts to trick the computer with a previously documented set of voices, people may be forced to read or repeat a random wording list. [14].

- Movement or Gait analysis involves an evaluation of the movement of humans utilized for the assessment and treatment of deficiencies that affect individuals ability to walk properly which can be understand well by the Figure 2.7. The service is available in specialized sport clinics to help athletes train and fly safely and painlessly.

A range of factors may affect posture patterns such as mass, length, gender and age, and external factors such as shoes, apparel and landscape. are included. Substances, personality, body composition and physiological factors, such as medical disorders and abuse, also take into account.

Throughout the movement test, a wide variety of instruments are used to monitor and measure the movements of the feet, knees and hips, so that a person is able to move correctly and recognize any underlying disorders. Physiological processes are also measured. This is achieved in movement labs where many specialist lenses and detectors are installed to enable data collection. [14].

In figure 2.11 a camcorder is set up at long distance to capture the movement and pace of a user for a particular time period from the start of his one heel strike on the ground to another ground strike of that heel. In the middle stages there are

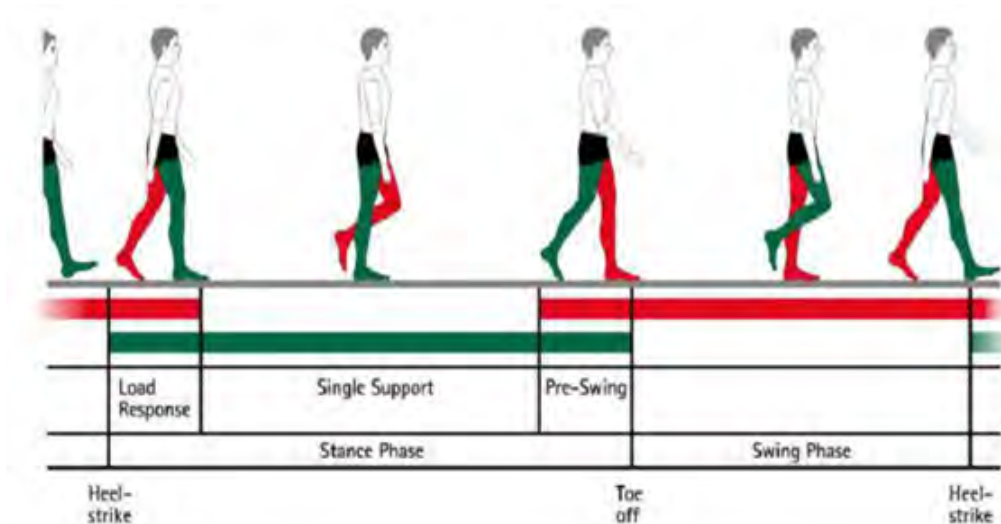


Figure 2.11: Gait Analysis

stance phase when toe properly hit the ground at 180 degree and pre swing and swing period before that particular heel strike again on the ground. Ground have sensors attached and user must wear sensors on his/her legs. Generally movement and pace of a user is unique so it is easy to identify if the user is valid or not.

- Cognitive biometrics is a novel way to deal with client confirmation or potentially recognizable proof that utilizes sensory tissue response(s) which can be understand well by the figure in Figure 2.8. Retina and iris scans, fingerprints and palm logins rely on specific anatomical features that you cannot overlook like a password may be. Cognitive biometrics relies on the subject's reaction when faced with a particular stimulus such as a well-known photo, a melody, a riddle, or even a Rorschach ink spot [14].



Figure 2.12: Cognitive Biometrics of Human Brain

Figure 2.12 shows biological sign and method of thinking of human brain is recorded through electroencephalogram (EEG), electrocardiogram (ECG) etc. which can later be compared with pre-loaded database and give access to a particular user.



- Signature study is a two-pointed method: -

1. Sign assessment is a study of individual forgery recognition signatures. To analyze a personal signature means to recognize a signature using advanced software, not only the contours, but also movements that were originally made. Smaller than authentic, fake signatures surface. The movement vs period activity that would take place with a true signature cannot be doubled even though the author accelerates the falsification process. A partnership can also exist between many signatures. Because of the changes in many individual signatures, any signature captured electronically can be used only once. Because of the differences found in the multiple signatures of a single individual, each signature captured electronically can only be used once [14].

2. For manual technology, the study of signature is a debugging method where an AC pulse has a particular waveform (usually a sine wave) signal applied to the unit. The following part, named the simple label, of the current versus volt, is an oscilloscope with the present indicated along its upward hub and the waveform on the bottom. Of each specific kind of "proof" element (e.g. capacitor, preamplifier, inverters), the resulting ana-log signature is unique. Any divergence from the standard sign shows clearly that there is a fault in this component [14].

Comprehensive end-user checks are essential, as they are the mechanism that prevents unwanted client access to unstable material. Verification ensures that user A only has permission to the material it wants and cannot see confidential data from user B. If your client is not authenticated, cybercriminals can manipulate the program and get the data they require. Sites like NetEase, eBay and Canva that were victims of data abuse are key indicators of how corporations fight to protect their sites. Just approved users access sensitive information by permission. Without a safe mechanism of authentication, the organization could be at risk.

## 2.4 Physical Biometric Authentication vs Behavioral Biometric Authentication

Researchers have suggested that physical biometric authentication is not much reliable as behavioral biometric authentication [30]. The reasons are: -

- Anybody can't do biometrics:

If you've ever done large- biometric systems — ten thousand to hundreds of thousands of users — then you'll know that for a number of reasons you'll have people who'll never be able to authenticate using a particular biometric attribute. I am not thinking about people with glass eyeballs or no fingerprints, but people who can never recognize their submitted biometric entry on subsequent applications, for reasons that we do not always understand. They never seem to suit.

- Biometrics aren't hidden:

Biometrics, including a password or private encryption key, are not secrets. Sometimes the biometrics are all over the place (e.g., fingerprints or face) or can be no-

ticed by someone who follows you around. No other kind of authentication is so readily visible and available. This causes the other problems.

- The biometric data can be copied easily:

The main issue with a non-secret authentication element is that they can be copied easily for malicious reuse. Your face and fingerprints are practically everywhere and can be quickly identified, copied and reused. If someone else has captured them, how can any program relying on those biometric attributes trust you to be who you think you are? Recently a study said that fingerprints can be copied using artificial intelligence which can eventually unlock your precious device very quickly.

- Biometrics are terribly incorrect:

Most people believe biometrics are amazingly accurate, since they are marketed in this way. Although this may be almost true, the description of how your biometric attribute is stored is nowhere near as accurate and specific as the real and true biometric element being measured. Although your fingerprint can (nearly) be unique in the world, what is processed and then measured during authentication is not. Your fingerprint (or iris, retina, nose, etc.) is not stored as a highly detailed image and is calculated. A calculation of the different distinguishing characteristics of the biometric identification is what is stored and evaluated.

- Biometrics are anything but difficult to trick:

The vendors are challenging these apparently hard-to-hack devices, often involving 3D or temperature sensors, to make it "hard" for another person to duplicate a copied or stolen biometric attribute. Vendors may use very tough-to-fool biometric scanners, but these are typically often very difficult to use, even for legitimate users. These are slower and contribute to much more false-negatives than the more reasonable goods of other vendors. Biometric products 'overall claims of accuracy are a sideshow carnival marketed to naive admins who don't really understand how they function. Perhaps they understand how they're operating but agree they're not all that reliable [30].

## 2.5 Benefits of Behavioral Authentication

In contrast to physical biometric authentication, behavioral authentication has some usefulness that is accepted and getting popularity around the world and bigger companies who care about their information and data are adopting behavioral authentication over physical authentication [25]. Here are some benefits which is provided by behavioral authentication: -

- Better experience for consumers:

It is passive to register and authenticate, preventing an awkward user experience.

- Fast and cheap deployment:

The easy-to-use API allows developers to quickly integrate the service into existing hardware, thereby eliminating the need for expensive additional hardware equipment.

- Flexibility:

Several features of behavioral biometrics can be studied, so that you can find a different choice for your needs.

- Increased safety:

Certain biometrics, including a fingerprint or a facial scan, are easy to counterfeit. However, what spoofing cannot do is completely imitate the manner in which someone types. We all have a special approach of clicking and using a keyboard, just like we all communicate in a slightly different way with our smartphones. Typing biometrics can thus help determine identity theft and reduce the risk of fraud online. Overall, you'll be able to say whether the user is a person or bot using behavioral biometrics.

- Specificity:

Besides being able to say whether a user is actually human, you will also be able to tell whether they complete or apply multiple times for the items. By detecting mouse movement, you can also calculate the user's degree of engagement.

- Regulatory compliance:

Consistent with 2FA specifications such as EBA / PSD2, NIST, PCI DSS.

Ultimately, the use of behavioral biometrics is non-intrusive to the user's experience while offering reliable details for identity determination, making it a highly safe method of authentication. Some businesses are starting to use behavioral biometrics, but it was most common in the finance and banking industries because their consumer information is highly sensitive and confidential. Although companies do not often disclose the ways they use behavioral biometrics, several prominent companies such as Mastercard, Experian and Deutsche Bank have been discussing their behavioral biometrics implementation.

Although it is mostly used for security purposes, there is also the potential for using behavioral biometrics to improve customer service. Companies may use behavioral data to better understand and know clients, predicting what they may need. This customer service application will likely continue to increase in popularity as behavioral biometrics continue to evolve [25].

# Chapter 3

## Leap Motion Sensor

### 3.1 Defination of Leap Motion Sensor

Leap Motion sensor is basically a computer hardware sensor device that was developed by an American company which we can see in Figure 3.1. It was designed in San Francisco by a company name Leap Motion Incorporation. It takes hand gestures as input, however it does not need any sort of hand-contact or contacting. It basically tracks hand gestures and through that virtual and augmented reality can be reached to interact with a new world. Working with various other equipment the Leap Motion sensor adds another approach to collaborate with the computerized world. The programs which are designed for this sensor can be used to play games, create new designs and many more. Till this point about all collaborations with PC programs required a delegate step such as mouse, console, etc to interact between the human hand and the digital condition. To fulfil this gap this leap motion sensor is very big step in this modern era to interact with different digital substance like modern world objects.



Figure 3.1: Leap Motion Sensor

## 3.2 History

Literature from [10] stated about the history of Leap Motion device. It was first developed by co-founder David Holz while he was pursuing his Ph.D in Mathematics. In 2010 he and Michael Buckward founded this company. Around June 2011 they received a funding about 1.3 million dollars with investments from ventures capital firms which was Founders Fund. There were several other investors as well. The first Leap Motion product was The Leap which was announced on 21st of May in 2012. In Oct 2012 the company released a software of their own and gave away about 12000 units of hardware products to various developers to work with it. By 2014 about 500000 units were sold. which was a bit short than initial expectation. So as a result they announced layoffs for about 10% from various sectors. In 2014 the version of leap motion sensor was released. In August of that year they released a VR tracking mode in its core software which was designed to provide handtracking while the device was connected with the software. In that year they also launched a game jam where they got about 150 submissions. Again 2015 there was another competition which had about 189 submissions. A special software known as Orion was released by leap motion which was built specifically for VR. In 2019 the company was named 'UltraLeap'. Figure 3.1 shows a Leap Motion Device.

## 3.3 Mechanism

Leap Motion Sensor has come a long way from where it has started. A lot of questions has already arisen about the mechanism of this device. Alex[5] has described about both the hardware and software part.

### 3.3.1 Hardware

The hardware part of the Leap Motion Sensor is quite simple. It mainly consist of two cameras. It also has three infrared LEDs. The infrared rays have a minimum 850 nanometres wavelength which is beyond the part of light range on which the light is visible. As a result the infrared rays cannot be seen with naked eyes. Due to the device's wide angle camera it has a pretty large interaction space. The viewing range of this device was limited to 2 feet previously but by using the software named Orion beta it has increased and limit till 2.6 feet. The gadget's USB tester adds the device information to its nearby memory. After that it plays out all fundamental resolution changes. In Figure 3.2 it is seen that the information appears as a grayscale sound system picture from the close infrared luminous range, isolated into both sides of the cameras. The objects that are directly illuminated from the device's LEDS are the ones that can be viewed.

### 3.3.2 Software

After the image enters the PC the software takes the floor. Despite all the misconceptions it does not generate any depth map rather it does some advance algorithm to the raw sensor data. The software that processes and forms the picture in the computer is called The Leap Motion Service. In the wake of making up for foundation



Figure 3.2: Hand Illuminated by Leap Motion Controller's LEDs

objects, the images are analyzed for remaking a 3-Dimensional portrayal. The tracking layer extracts the data for example the finger movements afterwards. The Leap Motion device at that point takes care of the results which furthermore communicates as a evolution of casitngs. The customer library composes the information into an application program interface structure and gives assistant capacities. From that point, the program integrates with the input, permitting a movement's experience.

### 3.4 Developers

Literature in [9] stated about the developer community of Leap Motion Controller. During the end of 2013, Founders Fund and SOSV reported the LEAP.AXLR8R which was a business accelerator agent for new businesses utilizing the Leap Motion controller. The projects that came from accelerator, a tech startup which is known as Diploia has used the Leap Motion Controller for lazy eye sufferers. MotionSavvy is developing a Leap Motion enhanced tablet which can be used for American sign languages. They also have an appstore of their own where they sells apps developed by their developers. By mid 2014 they already released about 200 apps in their appstore including Google Earth Integration, Digital Musical Instrument, Virtual Clap Sculpting app etc. The Leap Motion Controller has been used by medical surgeons for medical purposes, automobile engineers, aerospace engineers etc.

# Chapter 4

## Literature Reviews

Leap Motion sensor is relatively new in the tech market, giving the user innovative features to aid in their research or any other tasks. It has found its use mostly in the field of user authentication in various topics dealing with degree of accuracy and scope of recognition. In this section, we will discuss about some related studies on user authentication.

A biometric user verification system using hand gestures during login of personal computer and online verification was proposed by Chan et al.[12]. The study composed of two parts- the first part required provisional authentication where the user is assumed to login using Leap Motion authentication. The second part described online verification where the user is assumed to browse websites for practical use scenarios. According to the provisional authentication, for a few seconds the user is suppose to put his hands over the device. Afterwards, the system analyses the physical aspects of the user's hands to resolve who he/she is. To find out if the user is a genuine and authentic user he/she is told to draw a circle using one finger. materialistic aspects includes length and width of multitude of every finger, hands and arms. After that the physiological aspects comprise of time taken to draw the circle, radius of circle drawn, and acceleration of finger movement. The experiment was carried out by 16 testers and used the random forest algorithm. The results of static authentication correspond to accuracy of 99.97%.

Tien et al.[23] presented authentication which is related to challenge-response and it's mechanism is using on-air handwriting. Their method is mainly to cope with internal aggressions implementing biometric verification. It also implements challenge-response authentication(MoCRA). During the authentication phase, MoCRA requests the user to write in air a string picked at random while the Leap Motion records the movement of his/her hands. The user's factors are extracted by MoCRA from the writing feedback during verification. Normally, simply using challenge-response authentication will not prevent any attacks from individuals who already know the password. However, with the aid of behavioral features of users, MoCRA can deal with the imposter attacks. The experiment showed 98.82% authentication accuracy for 24 testers. About 17 seconds on an average is required to to write about the inquired string.

In another paper, biometric authentication system by acquiring handwritten ges-

tures are suggested by Kamaishi et al.[19]. Behavioral verification is associated with the hand features obtained from a user when he/she signs in the air and the signature itself. The goal is to observe varying biometric verification and it will be done through adopting tokens and biometric information. Using Leap Motion, the trait and speed of the user's fingers can be computed for authentication grounds. In the proposed method, the users were made to draw simple movements for primary stage. 86.57% verification accuracy demonstrates the experimental outcomes.

There exist few other scenarios regarding biometric hand-gesture signature, Xiao et al.[17] oversaw experiments for investigating the effect of consequences of using physical and behavioral attributes through Leap Motion Controller. A system was built where the users will provide their signatures and it will authenticate based on the hand structure and behavioral traits of that users. From 10 testers the analysis data was taken and the outcome was assessed by false rejection rate (FRR). The results indicate that by using behavioral information they were able to achieve an average EER of 3.75%. This means they achieved authentication accuracy of 96.25% according to (1-EER) value. However, for verification the time period is a bit high because of the limitations in their method.

Moreover a new system was suggested by Nigam et al.[7] which combines handwritten signature and face authentication. In doing so, they increased the authentication accuracy compared to each process could provide alone. In their experiments, data was gathered from 60 participants and an acceptance rate of 91.43% was accomplished.

There is one paper with similar mechanism as ours which had been suggested by Manabe et al.[31]. A two-factor authentication system was introduced in this paper where input biometric authentication and password are both combined together. Leap Motion measured the physical and behavioral features of the user's hands. subsequently, random forest classifier is applied to determine whether the hand data is genuine or not. the authentication process comprises of a few seconds taking finite data obtained when users enter a password. The edge over other methods is that it prevents intrusion even if the password is stolen thanks to biometric authentication. The experimental results for 21 testers which exhibits with an accuracy of 94.98% and an average of 2.52 for inputting a password.

In a paper by Atas[18], he explicitly discussed about a biometric recognition system using Leap Motion Controller which was based on a hand tremor. He used various extraction methods, including statistical, discrete wavelet transform, fast Fourier conversion, and 1-dimensional binary model. the goal is to authorize a stable identification system to avoid incursion of attackers. Naïve Bayes is utilized for analyzing recognition implementation. the experimental showed promising results of 95% accuracy rate. Along with Naive Bayes, Multi-Layer Perception is also utilized.

Imura et al.[26] presented similar method of hand gesture-based biometric authentication via Leap Motion. Using biometric data, seven 3D gestures which was divided into three categories was also proposed. The experiment was carried out by nine participants and it was evaluated to show results of true acceptance rate (TAR)



of greater than 90%. The error rates was equal with not more than 4%. for our convenience, we assume accuracy to be 96%(1-EER).

Additionally, Maruyama et al.[20] introduces user authentication using positions of finger joints via Leap Motion. In this paper, the user is analyzed and verified by doing a comparison between inter-digit and intra-digit feature amount from which the finger joint coordinates were cancelled. About twenty participants were part of the experiment and the hand was measured 30 times for each user. The results showed to get identification rate of 84.65% in light of separations between joints as intra-digit highlight as it were.

Fong et al.[3] has devised a biometric verification method which was related to hand and it was based on the user's hand indication assessment while they are incorporating sign language. In their paper, they addressed that simply typing 'iloveu' in text is vulnerable so instead, they encoded a string of hand signs as biometric password. A classification model was established to check whether it is the actual user. This included image processing algorithms such as color histogram, intensity profiling and dimensionality analysis as well as algorithms like Decision Tree and also Naive Bayes. The model showed 93.75% recognition accuracy.

Sharma et al.[15] proposed yet another similar approach of numeral gesture recognition via Leap Motion. To capture in-air numeral gestures was it's main function. After that Geometric Template Matching method was applied to classify the inputs. 70.2% average classification rate was found on the experimental results.

In another paper few researchers developed a behavioral authentication system which utilizes biometric data from hand geometry and gesture of users via Leap Motion. The sensor will check the dimensions of palm and fingers of users and then match with the legitimate ones. This removes any fear of intruders gaining access with same gesture.

# Chapter 5

## Proposed Model

For our research purpose, we have chosen to implement two algorithms for authentication which are Dynamic Time Warping(DTW) and Naive Bayes. Prior to previous papers within the field of user authentication, these two approaches stand out the most in getting the most optimum results. In this chapter, we will discuss in depth of each algorithm that was used in our work.

### 5.1 Dynamic Time Warping (DTW)

Dynamic Time Warping is a sequence identification algorithm which determine the space between two analytical series on time axis and then iteratively adjust them until there is an ideal match[1] . Figure (5.1) illustrates this method. This algorithm has been used extensively by Vikram et al.[4] and Riofrío et al.[21] for their work of user recognition.

Series A(t) and b(t) in Fig. (5.1) are represented as the following:



Figure 5.1: Two analytical series adjusted by DTW

$$A = [ a_1 a_2 \dots a_i \dots a_n ] \text{ ---(1)}$$

$$B = [ b_1 b_2 \dots b_i \dots b_m ] \text{ ---(2)}$$

These two series can be placed on both sides of the grid, vertically and horizontally respectively, as shown in figure (5.2) . They each start from the bottom left corner and continue onward.

The space between each component of two series is calculated in each cell of grid. The aim is to search for the best route which decreases total distance between them.

In order to do so, find all viable paths and calculate overall distance. Overall distance is the minimal sum of distance between each component divided by sum of weighing function, where weighing function is used for homogenizing path length. The key constraints of DTW are noted by the type of path through the grid:

- Monotonic status: the direction will either remain constant or gain but it will never decrease.
- Continuity status: the path moves by one step at once.
- Boundary status: the path starts from bottom left and finishes at top right.
- Warping window status: the path is permitted to wander within window width.
- slope constraint status: the path is not allowed to be too steep or shallow.

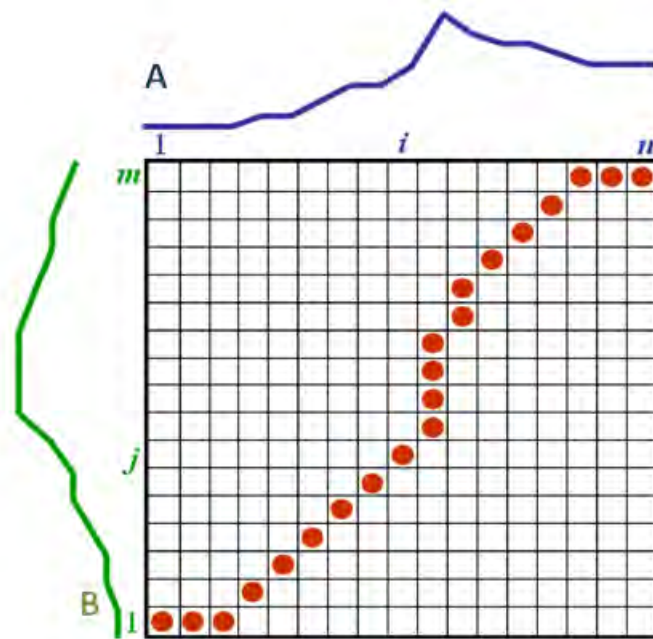


Figure 5.2: Graphical representation of DTW

## 5.2 Naive Bayes

Naive Bayes is probabilistic machine learning algorithm which is based on Bayes theorem  $P(A|B) = \frac{P(B|A)P(A)}{P(B)}$  which is illustrated below:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \quad (5.1)$$

Here, A is hypothesis and B is evidence and both features are assumed to be independent of each other. It is mainly used in spam filtering, sentiment analysis, etc. It is simple and quick to carry out but predictors need to be independent. Acharya et al.[2] and Saini et al.[22] have both utilized this method in their work to achieve their desirable results. There are three types of Naive Bayes classifier and they are as follows:

- Multinomial - used mainly for document classification issue where the predictors are the word repetition in document.
- Bernoulli - identical to multinomial but for Boolean variables
- Gaussian - used for continuous value from Gaussian distribution sample which can be seen clearly in Figure 5.3.

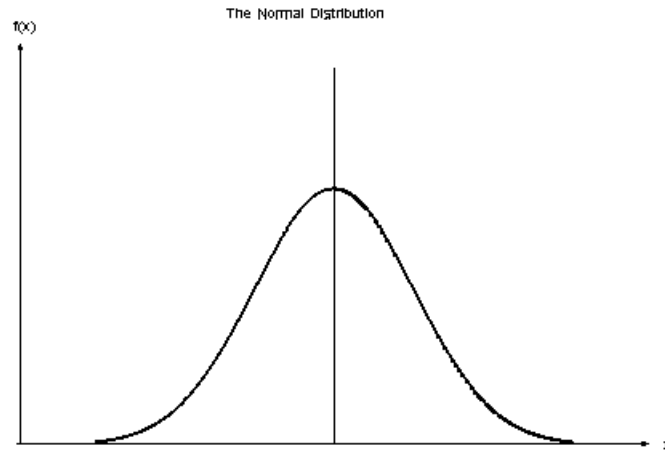


Figure 5.3: Normal distribution for Gaussian Naive Bayes

### 5.3 Mechanism of the Proposed Model

Our proposed system will work in the following way. First the user will enter their user data such as username and password. After entering that, the system will ask the user to enter motion data by placing their hands on the Leap Motion device for about 10-15 seconds. Once the system collects and processes the motion data it will store it in the database, as illustrated in figure 5.4.

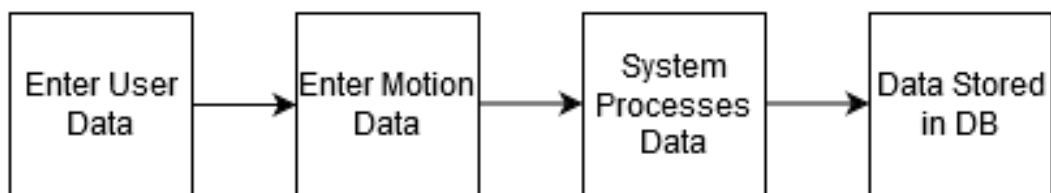


Figure 5.4: Block Diagram of Registering User in the System

After the user data is registered into the database, they are secured for authentication. During the authentication phase, the user will attempt to login to their desired workplace by entering their user name and password. During the process, a Leap Motion Device will capture the hand motion data of the user, as shown in Figure 5.5. This is the first security layer of user authentication for the system. If the user enters the correct username and password they will be qualified for the second security layer of user authentication. Otherwise they will be rejected.

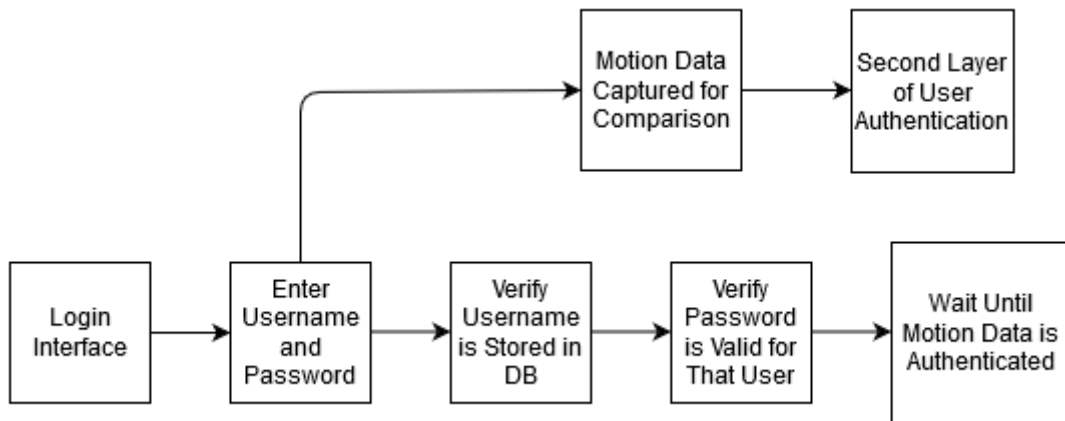


Figure 5.5: First Layer of User Authentication

In the second security layer, the system will pull up the stored motion data for the entered username and temporarily store it in memory. Afterwards, the system will compare the captured motion data during user input earlier with the motion data stored in the database. If the data matches, then the user will be authenticated as a valid user and they will be successfully able to login, as illustrated in Figure 5.6. Otherwise the user will be rejected.

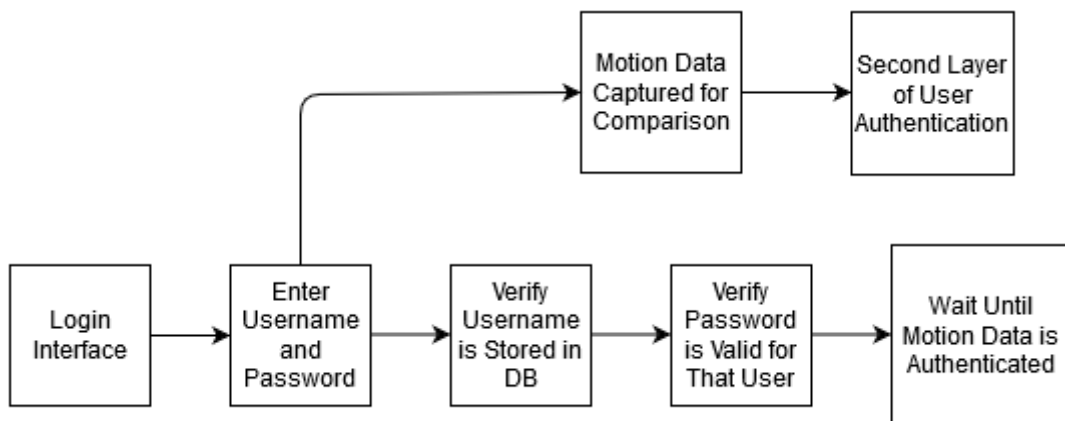


Figure 5.6: Second Layer of User Authentication

# Chapter 6

## Collecting and Processing The Dataset

### 6.1 Dataset Collection

To properly authenticate the user through Leap Motion sensor, we must first store their authentication data in the dataset. Since we are only working on authentication through hand motion we will store the user's hand and finger data on a frame-by-frame basis. The user will first enter their user data(name, password etc) and then will store motion data.

#### 6.1.1 Frame Data

The Leap Motion device can capture starting from 20 frames till 200 frames per second which varies on the system setting. For our system we have set the device fps to be 60. As a result, when the user puts their hand on top of the device it will immediately start capturing 60 frames worth of data every second. Each frame of data will consist of a unique frame ID, the timestamp of the captured frame, the number of hands as well as the number of fingers visible on the Leap Motion. While capturing and saving these data in the dataset, we will simultaneously capture and store the hand and finger data as well.

#### 6.1.2 Hand Data

For the hand data first the system will first detect how many hands the user is using. If they are using both hands the system will run as intended. However, if the user is only using one hand then the system will run a simple if-else condition to check which hand is being used before storing that hand's data. By implementing the code in Figure 6.1 hand type can be determined.

```
43 String handType = hand.isLeft() ? "Left Hand" : "Right Hand";
```

Figure 6.1: Code for determining hand type

It has to be noted that if the user is only storing one hand's motion data then they will not be properly authenticated when using the other hand to enter input in the

system. So both hand's data should be entered in the dataset.

As the hand data is being saved on a frame by frame basis, each frame will contain a unique ID which will be the same as the frame ID above, which hand/hands are being used and the position of the palms. It must be noted that the last variable is given in the form of a vector type data, which contains the 3-dimensional coordinates of the palm center point(in millimeters) from the Leap Motion origin. In addition to this, the system will also compute the hand orientation by using the pitch which is the angle around the x-axis, yaw which is angle around the y-axis and roll which is the angle around the z-axis. Originally in vector type data, the system will convert them to degree. This all will take place by applying the code in Figure 6.2.

```
50     Vector normal = hand.palmNormal();
51     Vector direction = hand.direction();
52     double Pitch = Math.toDegrees(direction.pitch());
53     double Roll = Math.toDegrees(normal.roll());
54     double Yaw = Math.toDegrees(direction.yaw());
```

Figure 6.2: Code for calculating pitch, roll and yaw

These will all be stored as hand data of the user in the dataset. To reduce the FRR of the system as much as possible, the user will need to give hand data in different hand orientations.

### 6.1.3 Finger Data

For the finger data, the system will determine what type of fingers are on the device in Figure 6.3.

```
63     FingerList fingerType = frame.fingers();
```

Figure 6.3: Code for determining finger type

The method `finger.type()` works in such a way that it returns a value which determines what type of finger is being captured by the Leap Motion device.

```
FingerTypeThumb = 0
FingerTypeIndex = 1
FingerTypeMiddle = 2
FingerTypeRing = 3
FingerTypePinky = 4
FingerTypeUnknown = -1
```

As the finger data is also being saved on a frame by frame basis, each frame will contain a unique ID which will be the same as the frame ID, which fingers are visible on the device, each finger's length and width(both in millimeters). These will all be stored as finger data of the user in the dataset. Similar to the hand data, the user will

need to give finger data in different finger positions to reduce the FRR of the system.

Since Leap Motion device captures data very quickly, the dataset may become overloaded with too much frame data which in turn may slow down the system. Which is why the proposed system will at most have about 1000 frames worth of data in the dataset for each user. When any new data is entered into the dataset, it will replace the least recent frame data to compensate. The system will then compute an average value of hand and finger data from the dataset it contains to use during the authentication phase. Since the system will run in a dynamic environment, we will allow for a deviation of around 4 out of 100 of the system computed average value to be accepted as valid which is within the acceptable error margin.

## 6.2 Processing the Dataset

As stated above, the data collection from the Leap Motion device is a continuous process. So we cannot immediately store it on a database for authentication use due to risk of system performance declining. Which is why, our system will first collect up to the most recent 1000 frames worth of user data which will then be converted to a sequence of bytes through serialization. The code in Figure 6.4 states about the code to serialize frame data. To spare a few edges to a similar record, we initially make an approach to declare about the starting and ending of the frames. The range of the data varies. For all that, our system uses the following method, by storing a 4 byte integer which carries the data size immediately before the data itself.

```
45     Path outputPath = Paths.get("frames.data");
46     Controller controller = new Controller();
47     OutputStream out = Files.newOutputStream(outputPath);
48     for (int f = 0; f < 1000; f++) {
49         Frame frameToSerialize = controller.frame(f);
50         byte[] serialized = frameToSerialize.serialize();
51         out.write(ByteBuffer.allocate(4).putInt(serialized.length).array());
52         out.write(serialized);

```

*Figure 6.4: Code for serializing frame data*

Figure 6.4: Code for serializing frame data

This saves the serialized frame data in a file called “frames.data”. After having a finite number of frames to work with, the system then passes the sequence of bytes to a deserializer to convert the bytes back into frame data. To interpret the frame data from “frames.data”, the system then reads the first 4 bytes to know about the amount of data that it have to read through to achieve a full frame. After that, it keeps on repeating the process until arriving to the destination of the file. Code in Figure 6.5 is the code for deserialize frame data.



```

16 Path inFilePath = Paths.get("frames.data");
17 byte[] data = Files.readAllBytes(inFilePath);
18 int c = 0;
19 int nextBlockSize = 0;
20 if(data.length > 4)
21     nextBlockSize = (data[c++] & 0x000000ff) << 24
22     |(data[c++] & 0x000000ff) << 16
23     |(data[c++] & 0x000000ff) << 8
24     |(data[c++] & 0x000000ff);
25 while (c + nextBlockSize <= data.length){
26     byte[] frameData = Arrays.copyOfRange(data, c, c + nextBlockSize);
27     c += nextBlockSize;
28     Frame newFrame = new Frame();
29     newFrame.deserialize(frameData);
30     if(data.length - c > 4)
31         nextBlockSize = (data[c++] & 0x000000ff) << 24
32         |(data[c++] & 0x000000ff) << 16
33         |(data[c++] & 0x000000ff) << 8
34         |(data[c++] & 0x000000ff);

```

Figure 6.5: Code for deserializing frame data

As a result, a new copy of the frame dataset is created which we can store in the database. Each frame data will be stored separately in the database with their own unique ID, hand and finger data.

# Chapter 7

## Result Analysis

Our main goal is to authenticate the user through Leap Motion data as accurately and quickly as possible, while they are giving their password input. Which is why we decided to use DTW (Dynamic Time Warping) and Naïve Bayes Algorithm to check for the accuracy of the system as well as how quickly it responded. For the experiment, we captured the Leap Motion data of 8 people and stored them in the database for user authentication and another 8 people were used as third party users. Moreover, as the password is being typed into the keyboard, it is important to restrict the intrusion of malicious third party users. Therefore, we aim to reduce False Rejection Rate (FRR), False Acceptance Rate (FAR), False Rejection (FR) which incorrectly identifies a valid user as invalid user and False Acceptance (FA) which incorrectly identifies an invalid user as a valid user. To calculate these parameters we use the following parameters. Specifically, numT, numF, numFR, numFA which are defined below.

numT = Total test data for valid users

numF = Total test data for invalid users

numFR = Total false rejections during experiment

numFA = Total false acceptances during experiment

Furthermore, the following equations determine FRR and FAR.

$$FAR = \frac{numFR}{numT} \quad (7.1)$$

$$FRR = \frac{numFA}{numF} \quad (7.2)$$

### 7.1 Applying DTW Algorithm

DTW or Dynamic Time Array is an algorithm which allows us to compare or calculate the distance between two arrays of different length. In our case, this algorithm can be used to compare the frame data some user is providing while typing the password through the Leap Motion Device with the user frame data stored in the database. Which is why during authentication phase, the system generates a DTW matrix by using a 2-dimensional array which contains the average frame data computed from the database which we will call the Source Matrix. Additionally, the frame data being captured during the authentication phase are also converted into a

2-dimensional array which we will call the Converted Matrices. These are temporarily stored until comparison phase ends. The length of the Converted Matrices may or may not be the same as the Source Matrix. The comparison process starts once the user hits the enter key, which will prompt the system to start comparing the Converted Matrices with the Source Matrix one by one. As mentioned above, we allowed for a deviation of up to 4% to be considered as acceptable. If all Converted Matrices are within 4% deviation of the Source Matrix at that point the user will be successfully authenticated. If not, the user will be denied even if they entered the correct password.

## 7.2 Results of applying DTW Algorithm

To test the effectiveness of the system, each users were told to try to authenticate 5 times, for a total of 80 authentication attempts from 16 users. Additionally, for testing the behavioral properties of the particular system we ran 3 trials on separate days at different times. Table 1 shows the accuracy as well as the FAR and FRR of each trial.

Experimental Trial	Accuracy(%)	FAR(%)	FRR(%)
First Trial	79.64	3.46	17.79
Second Trial	82.13	2.66	16.10
Third Trial	80.92	2.48	16.05

Table 7.1: Experimental result for DTW algorithm authentication

Table 7.1 shows that if the system applies DTW algorithm, then we get an average of 80.9% accuracy which is not satisfactory for reliable security. In addition, the False Acceptance Rate (FAR) was also abnormally high at an average of 2.87. We speculate that the proposed system might not be compatible with DTW in this regard. The False Rejection Rate (FRR) however had slowly declined with each trial which was one of the main goal of our system which we can see at th graph of Figure 7.1.

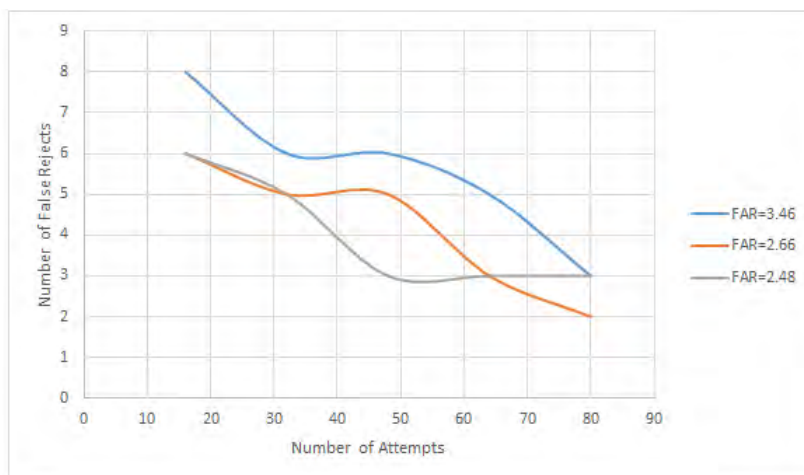


Figure 7.1: Relationship between number of inputs and number of false rejections

### 7.3 Applying Naïve Bayes Algorithm

As Naïve Bayes algorithm is very adaptable and a quick learning algorithm when assigned many features, we allowed the classifiers to learn as much as the user data as possible through 14 features which is explained briefly in Table 7.2.

Feature	Explanation
Finger length(5 features)	The length of each fingers(in millimeters)
Finger width(5 features)	The width of each fingers(in millimeters)
Time needed for password input(1 feature)	The average time needed to enter password (in seconds)
Palm position(3 features)	The pitch, roll and yaw of the hand during password input(in degrees)

Table 7.2: Features used for Naive Bayes authentication

During the authentication phase, when the user is giving password input the system will capture the Leap Motion data until they hit the enter key. Afterwards the system will give a binary input of 0 or 1. We guess that the user needs x number of frames to input the password into the system, while the Leap Motion device also computes the same features x number of times as the password is being entered by the user. For every one of the x data sets, the system then judges whether or not the data set is that of a valid user. If the dataset where the user is verified to be genuine becomes equal or more than some value z is when the system decides that the user is genuine and returns output 1. Here, we determine the parameter z by basing it on the data set used for parameter adjustment. On the other hand, if the system decides that the user is an intruder or invalid, then it returns output 0.

### 7.4 Results of applying Naïve Bayes Algorithm

Similar to testing the accuracy of DTW algorithm, each users attempted for authentication 5 times, for a total of 80 authentication attempts from 16 users. To test the behavioral aspect of the system we ran 3 trials on separate days at different times. Table 3 shows the accuracy as well as the FAR and FRR of each trial.

Experimental Trial	Accuracy(%)	FAR(%)	FRR(%)
First Trial	92.22	1.78	19.32
Second Trial	89.74	2.79	18.38
Third Trial	89.94	1.40	12.53

Table 7.3: Experimental result for Naive Bayes algorithm authentication

Table 7.3 shows that by applying Naïve Bayes Algorithm, the system gave an average of 90.63% of accuracy. Additionally, it is evident that FRR while having high percentage in the first and second trial, it was greatly reduced by the third trial. By looking at the graph of Figure 7.2 we speculate this is due to the fact that the users had gotten used to using the system.

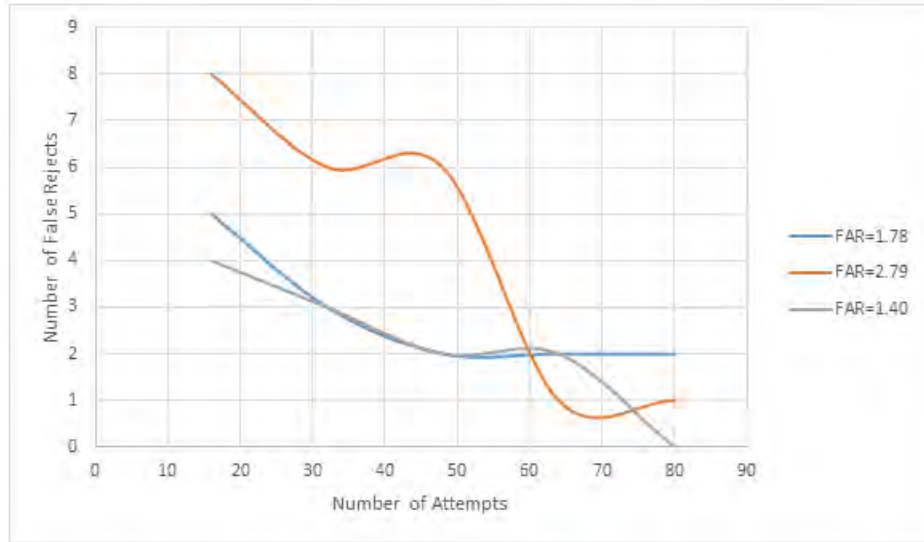


Figure 7.2: Relationship between number of inputs and number of false rejections

It must also be noted that, the FRR would be even less if we removed the behavioral features from Figure 7.2, such as time needed to input password and palm position and only used physical features like finger length and width. This is because behavioral features are less likely to be accurate than physical features when users holds not to be used to typing their password input.. Behavioral features gradually become more effective as users get used to typing their password.

Experimental Trial	Accuracy(%)	FAR(%)	FRR(%)
First Trial	92.22	3.56	14.23
Second Trial	92.54	3.79	13.89
Third Trial	93.94	1.39	9.53

Table 7.4: Experimental result for Naive Bayes algorithm authentication(without behavioral features)

As evident in Table 7.4, the FRR is significantly reduced, with an average of 12.53% which is a 4.21% reduction from before. The accuracy also rises, with an average of 2.27% increase. Even though the FAR is much higher compared to before (averaging at 2.91%), as we also need to consider easy user interaction with the system we have determined it to be within acceptable values.

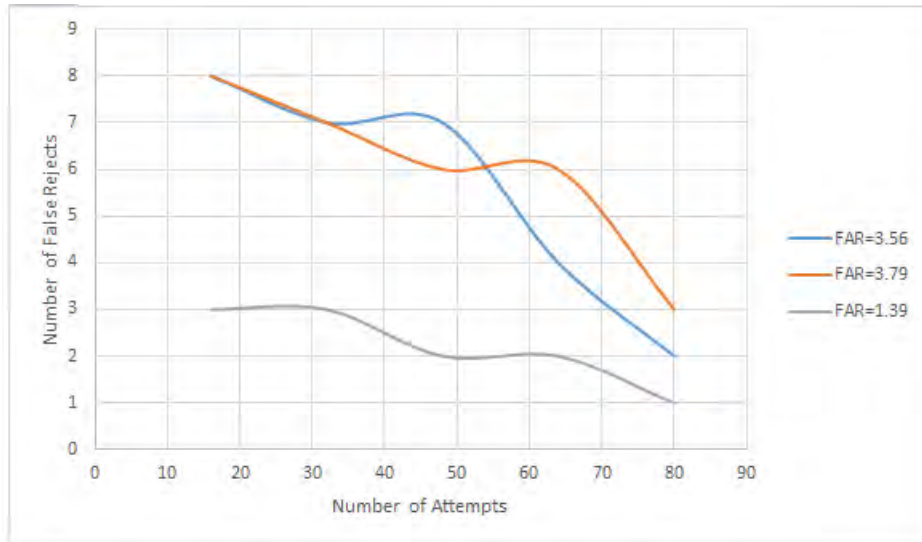


Figure 7.3: Relationship between number of inputs and number of false rejections

## 7.5 Comparison of Results

Based on the above results we can see that compared to DTW algorithm, Naïve Bayes algorithm returned more accurate results. Even though, DTW had less False Rejection Rate than Naïve Bayes, when comparing the average the FRR was only at a 0.31% reduction. In addition, as mentioned above, The FRR of Naïve Bayes would be reduced more if we removed the behavioral features and only used the physical features. Lastly, the system also adapted and responded much quicker when Naïve Bayes was applied. So considering the accuracy, the negligible difference in FRR and the response time, Naïve Bayes algorithm is better suited for our system. Figure 7.4 gives us a better understanding of the comparison between the two algorithms.

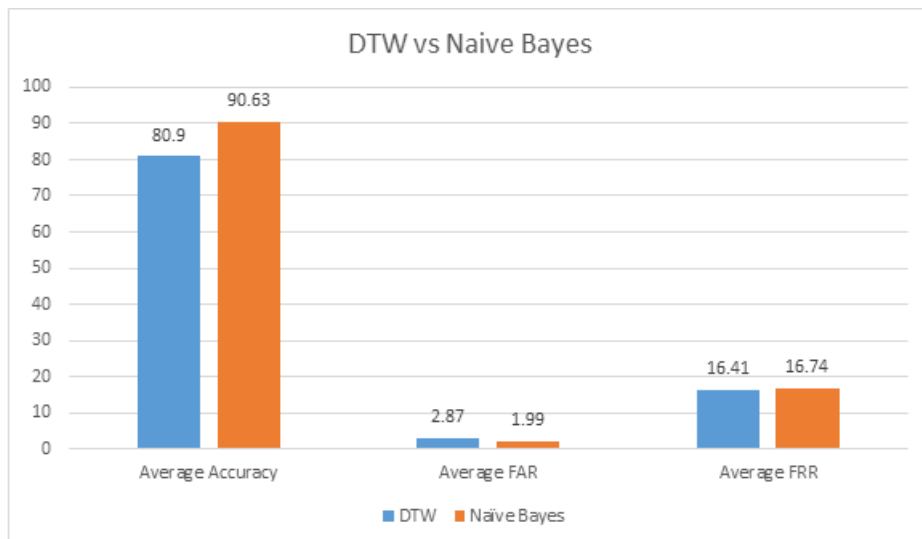


Figure 7.4: Comparison chart between DTW and Naïve Bayes

Meanwhile Figure 7.5 shows us the comparison between the two when we remove the behavioral features from the Naïve Bayes Classifier.

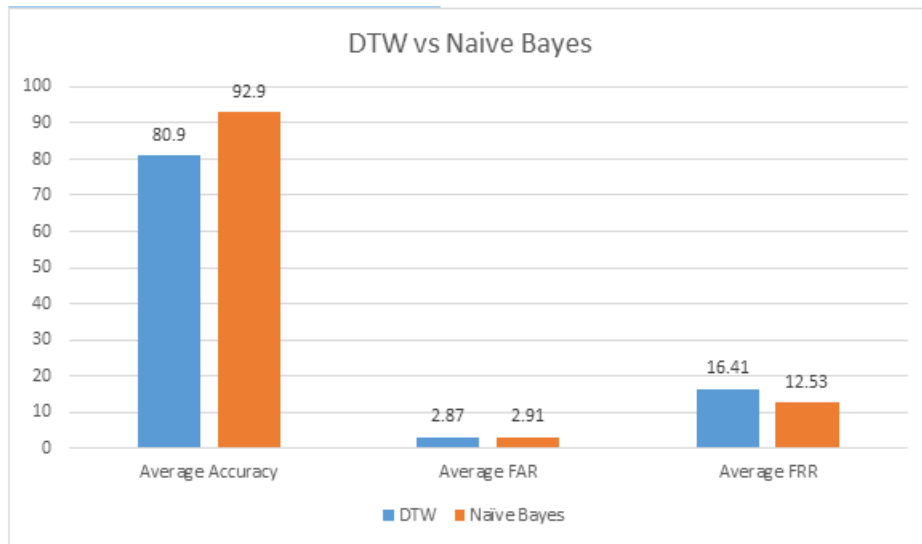


Figure 7.5: Comparison chart between DTW and Naive Bayes(without behavioral features)

# Chapter 8

## Conclusion

User verification or authentication is now a trending topic worldwide. As the world is going more towards digitalization, organizations or people like us are preferring behavioral verification over physiological verification. According to FBI's internet crime report of 2019, ransomware attackers breached into end user's personal devices like computer, laptop or smartphone who have used ordinary and tiny password and didn't utilize two or multi factor authentication for its complexity. The amount of loss which FBI measured was around \$8,965,847 USD [33]. Moreover, eSentire annual threat report of 2017 said that brute force and dictionary attacks have increased up to 400 percent because the company experienced brute force and dictionary attempts per hour ranging from 100 to 600, coming from 10 to 20 different IP addresses [27]. In our model we have implemented a system where we are taking behavioral hand data and password from a user instead of only physiological data like fingerprint, FaceID, iris scanner etc. which can be easily cloned by using artificial intelligence. An end user's behavioral hand data is unique and varies from time to time. So, we are storing data of a user's hand gesture from different time period on a database from where we can verify a particular user which is very difficult to duplicate by the hackers. The experimentation we have done so far using Naive Bayes algorithm provided the best accuracy rate of 93% compared to Dynamic Time Warping algorithm. In contrast to other existing methods, our method is easy to implement because of its quick learning capability and quick response time.

### 8.1 Future Uses

We are planning to do further research on our proposed system to improve user interaction with the system and get accuracy close to 100%. As we had to collect data from a user multiple times for gathering his/her real time hand gesture from different time period and make our own database, we could have tested only 16 users through our system. Out of them 8 users had hand data stored in the database and 8 didn't. Our proposed model somehow works well than other existing methods because of its quickness in learning and quick response time. It might be useful system for general and corporate users because our system collects real time hand data of a user which is difficult to implicate or cracked. But there is more we can work on this offered system. We will try to implement keystroke dynamics on our project that would gather user's force on the keys of a keyboard while they will type password to log into a device. Initially we made this project for our experimentation



cause but we will do our best to launch it on the marketplace so that we can offer a cost-effective user verification system which will prevent cyber-attacks of hacker groups and keep the data of a user shielded.

# Bibliography

- [1] E. Tsiporkova, “Mining of gene expression time series with dynamic time warping techniques”, *GenTWarper mining tool*, pp. 25–29, 2008. [Online]. Available: <https://www.psb.ugent.be/cbd/papers/genxwarper/index.html>.
- [2] S. Acharya, A. Fridman, P. Brennan, P. Juola, R. Greenstadt, and M. Kam, “User authentication through biometric sensors and decision fusion”, *47th Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, pp. 1–6, 2013.
- [3] S. Fong, Y. Zhuang, I. Fister, and I. Fister, “A biometric authentication model using hand gesture images”, *BioMedical Engineering OnLine*, *12(1)*, 2013. DOI: 10.1186/1475-925x-12-111.
- [4] S. Vikram, L. Li, and S. Russell, “Writing and sketching in the air, recognizing and controlling on the fly”, *Extended Abstracts on Human Factors in Computing Systems*, vol. CHI’13, pp. 1179–1184, 2013.
- [5] A. Colgan, “How does the leap motion controller work?”, Aug. 2014. [Online]. Available: <http://blog.leapmotion.com/hardware-to-software-how-does-the-leap-motion-controller-work/>.
- [6] C.-S. Koong, T.-I. Yang, and C.-C. Tseng, “A user authentication scheme using physiological and behavioral biometrics for multitouch devices”, *Intelligent User Interface for Interactive Multimedia: Emerging Techniques and Services*, Jul. 2014. [Online]. Available: <https://doi.org/10.1155/2014/781234>.
- [7] I. Nigam, M. Vatsa, and R. Singh, “Leap signature recognition using hoof and hot features”, *Proceedings of 2014 IEEE International Conference on Image Processing*, pp. 5012–5016, 2014.
- [8] E. Tsiporkova, “User authentication”, *Web authentication and access control*, Dec. 2014. [Online]. Available: <https://searchsecurity.techtarget.com/definition/user-authentication>.
- [9] Wikipedia, “How does the leap motion controller work?”, 2014. [Online]. Available: [https://en.wikipedia.org/wiki/Leap\\_Motion](https://en.wikipedia.org/wiki/Leap_Motion).
- [10] —, “Leap motion”, 2014. [Online]. Available: [https://en.wikipedia.org/wiki/Leap\\_Motion](https://en.wikipedia.org/wiki/Leap_Motion).
- [11] A. Atia, S. N. Abdulkader, and M.-S. Mostafa, “Authentication systems: Principles and threats”, *Computer and Information Science*, vol. 8, Jul. 2015. DOI: 10.5539/cis.v8n3p155. [Online]. Available: [https://www.researchgate.net/publication/282966029\\_Authentication\\_systems\\_principles\\_and\\_threatshttps://www.researchgate.net/publication/282966029\\_Authentication\\_systems\\_principles\\_and\\_threats](https://www.researchgate.net/publication/282966029_Authentication_systems_principles_and_threatshttps://www.researchgate.net/publication/282966029_Authentication_systems_principles_and_threats).

- [12] Chan, Halevi, and Memon, “Challenge response authentication using in air handwriting style verification”, *Springer, Cham (2015)*, vol. 9190, pp. 13–22, 2015. [Online]. Available: [https://doi.org/10.1007/978-3-319-20376-8\\_2](https://doi.org/10.1007/978-3-319-20376-8_2).
- [13] Cmarsden, “4 reasons why biometric security is the way forward”, Aug. 2015. [Online]. Available: <http://www.digitus-biometrics.com/blog/4-reasons-why-biometric-security-is-the-way-forward/>.
- [14] M. Rouse, “Behavioral biometrics”, *Authentication, access control*, Mar. 2015. [Online]. Available: <https://whatis.techtarget.com/definition/behavioral-biometrics>.
- [15] J. Sharma, K., R. Gupta, and V. Pathak, “Numeral gesture recognition using leap motion sensor”, *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, 2015. DOI: 10.1109/cicn.2015.86.
- [16] K. Jetter, “That insane, \$81m bangladesh bank heist? here’s what we know”, *he International Conference*, May 2016. [Online]. Available: <https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/>.
- [17] G. Xiao, M. Milanova, and M. Xie, “Secure behavioral biometric authentication with leap motion.”, *Proceedings of IEEE 4th ISDFS 2016*, vol. Article No. 7473528, 2016.
- [18] M. Atas, “Hand tremor based biometric recognition using leap motion device”, *IEEE Access*, 5, 23320–23326, 2017. DOI: 10.1109/access.2017.2764471.
- [19] R. Kamaishi S.and Uda, “Biometric authentication by handwriting with single direction using self-organizing maps”, 2017.
- [20] K. Maruyama, J. Shin, C. Kim, M., and C. Chen, “User authentication using leap motion”, *Proceedings of the International Conference on Research in Adaptive and Convergent Systems - RACS 17*, 2017. DOI: 10.1145/3129676.3129698.
- [21] S. Riofrio, D. Pozo, J. Rosero, and J. Vásquez, “Gesture recognition using dynamic time warping and kinect: A practical approach”, *International Conference on Information Systems and Computer Science (INCIS-COS), IEEE*, pp. 302–308, 2017.
- [22] B. S. Saini, N. Kaur, and K. S. Bhatia, “Keystroke dynamics based user authentication using numeric keypad”, *2017 7th International Conference on Cloud Computing, Data Science Engineering - Confluence, Noida*, pp. 25–29, 2017.
- [23] Tian, J., Cao, W. W. U.and Xu, and S, “Challenge response authentication using in air handwriting style verification”, 2017. [Online]. Available: <https://doi.org/10.1109/tdsc.2017.2752164>.
- [24] “Understanding user authentication: 3 basics you should know”, Dec. 2017. [Online]. Available: <https://swoopnow.com/user-authentication/>.
- [25] “Behavioral biometrics authentication”, *Identity Access Management Solutions*, 2018. [Online]. Available: <https://optimalidm.com/solutions/identity-access-management/behavioral-biometrics-authentication/>.

- [26] S. Imura and H. Hosobe, “A hand gesture-based method for biometric authentication”, *Human-Computer Interaction. Theories, Methods, and Human Issues Lecture Notes in Computer Science*, pp. 554–566, 2018. DOI: 10.1007/978-3-319-91238-7\_43.
- [27] R. Millman, “Brute force and dictionary attacks up 400 percent in 2017”, *FBI Cyber Crime Report Shows the Weakness of Password Protection*, Feb. 2018. [Online]. Available: <https://www.scmagazineuk.com/brute-force-dictionary-attacks-400-percent-2017/article/1473168>.
- [28] J. Shin, K. Maruyama, and C. M. Kim, “User authentication using leap motion”, *he International Conference*, Feb. 2018. [Online]. Available: [https://www.researchgate.net/publication/320759796\\_User\\_Authentication\\_using\\_Leap\\_Motion](https://www.researchgate.net/publication/320759796_User_Authentication_using_Leap_Motion).
- [29] M. Ghadawala, “7 key benefits of security with the addition of biometrics”, Jul. 2019. [Online]. Available: <https://www.globalsign.com/en/blog/7-benefits-security-with-biometrics>.
- [30] R. A. Grimes, “6 reasons biometrics are bad authenticators (and 1 acceptable use)”, *Biometrics-only authentication is inaccurate, hackable and far from foolproof*, Jan. 2019. [Online]. Available: <https://www.csoonline.com/article/3330695/6-reasons-biometrics-are-bad-authenticators-and-1-acceptable-use.html>.
- [31] T. Manabe and H. Yamana, “Two-factor authentication using leap motion and numeric keypad”, *HCI for Cybersecurity, Privacy and Trust Lecture Notes in Computer Science*, pp. 38–51, 2019. DOI: 10.1007/978-3-030-22351-9\_3.
- [32] J. Shepherd, “The ultimate authentication playbook”, *Security Blog*, Feb. 2019. [Online]. Available: <https://www.okta.com/security-blog/2019/02/the-ultimate-authentication-playbook/>.
- [33] R. A. Grimes, “It’s time we see passwords for the paper tigers that they are”, *FBI Cyber Crime Report Shows the Weakness of Password Protection*, Feb. 2020. [Online]. Available: <https://www.nextgov.com/ideas/2020/02/fbi-cyber-crime-report-shows-weakness-password-protection/163337/>.