IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ADVANCE SECURITY OF BIKE USING A LOCKING SYSTEM WITH FINGERPRINT SCANNER KEY

[1]Nitish Kaushik, [2]Gaurav Kumar
[1]Assistant Professor, [2]Assistant Professor
[1]Invertis University,
[2]Shivalik College, Dehradun

CHAPTER 1 : INTRODUCTION

A fingerprint sensor is a digital representation of a fingerprint pattern recorded by a device. A live scan is the image that is captured. The live scan is processed digitally to generate a one-of-a-kind biometric template (a collection of extracted features) that is saved and utilized for matching [3].

Companies in today's world are introducing new technologies to the market. In modern days, vehicles are also using new technology like self-start is also being used with a kick. Only individuals Fingerprint recognition technology can be used by those whose fingerprints have been saved in the memory. Even in the case of a total power outage or battery exhaustion, stored fingerprints are maintained. This eliminates the need to memorize a combination or keep track of keys. PIN stands for Personal Identification Number. Because there are no keys or combinations that can be duplicated or stolen, or locks that can be picked, it can only be accessed when an authorized person is present.

Fingerprints are being used to unlock locks instead of the traditional approach of utilizing keys. Keeping this in mind, we have a sophisticated locking system with keys, since no one can steal a bike with a sophisticated lock and key. Because it will employ fingerprint technology, our locking mechanism will be far more sophisticated than a standard lock [2].

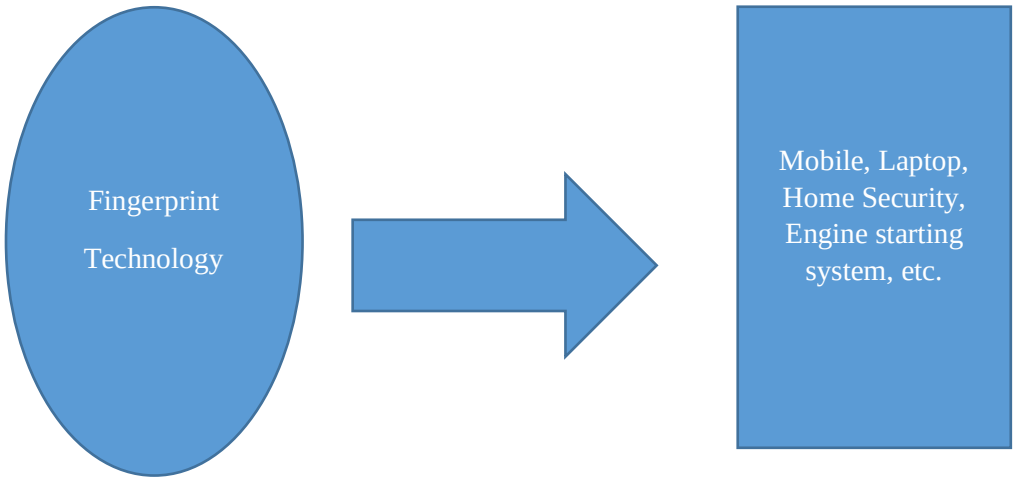


Figure 1.1: Fingerprint Technology Representation

1.1 Fingerprint Technology

One of the most well-known and well-publicized biometrics is fingerprint identification. Fingerprints have been used for identification for over a century due to their uniqueness and constancy through time, but have only recently been automated (i.e. a biometric) due to advances in computing power [1]. Fingerprint identification is popular due to its inherent simplicity of acquisition, the various sources accessible for collection, and law enforcement and immigration's long-standing usage and collecting of fingerprints.

1.1.1 Fingerprint Sensor

A fingerprint sensor is a digital representation of a fingerprint pattern recorded by a device. The image that is captured is known as a live scan. This live scan is digitally processed to create a biometric template (a set of extracted features) that may be saved and used for matching [12].

1.1.2 Types of Fingerprint sensor

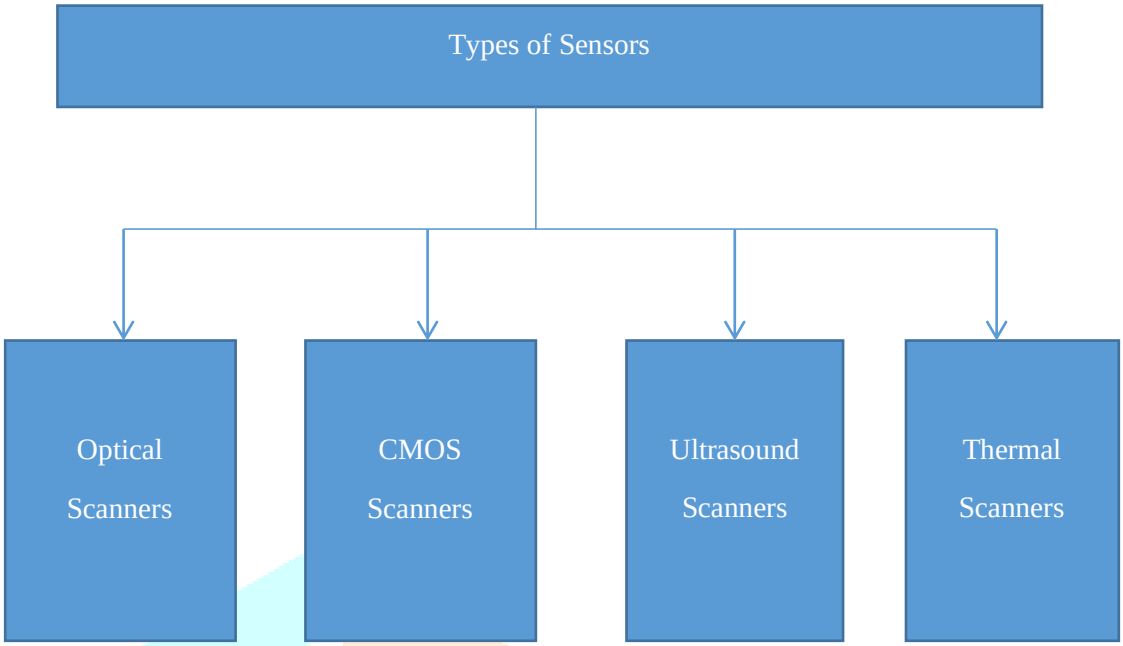


Figure 1.2 : Classification of Fingerprint Scanners

- **Optical scanners** using a digital camera, capture a visual image of the fingerprint Show in (fig 1.3).
- **Capacitive or CMOS scanners** to create a fingerprint picture, capacitors and Therefore electrical current are used show in (fig 1.4).
- **Ultrasound fingerprint scanners** to high-frequency sound waves are employed in ultrasound fingerprint scanners to penetrate the epidermal (outer) layer of the skin, as seen in fig (1.5).
- **Thermal scanner** detects temperature variations between fingerprint ridges and troughs on the contact surface show in fig (1.6).

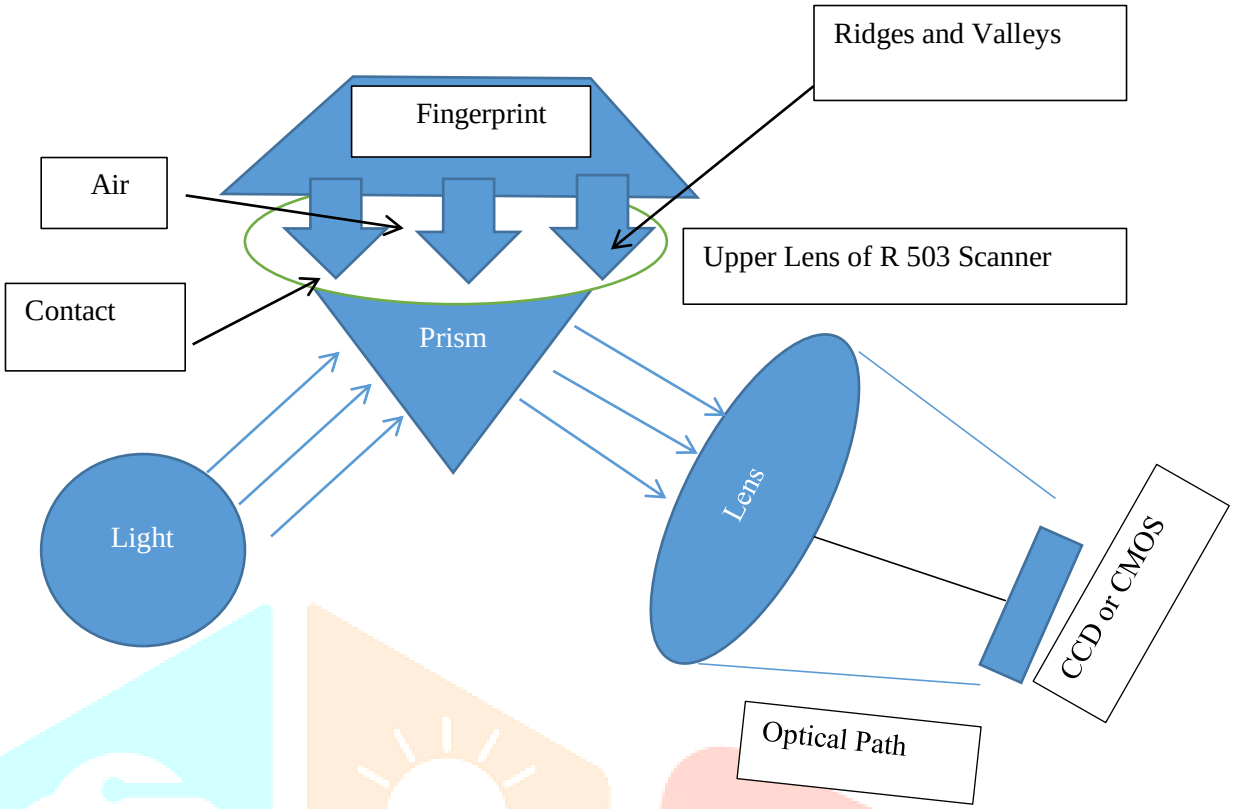


Figure 1.3: Optical scanners

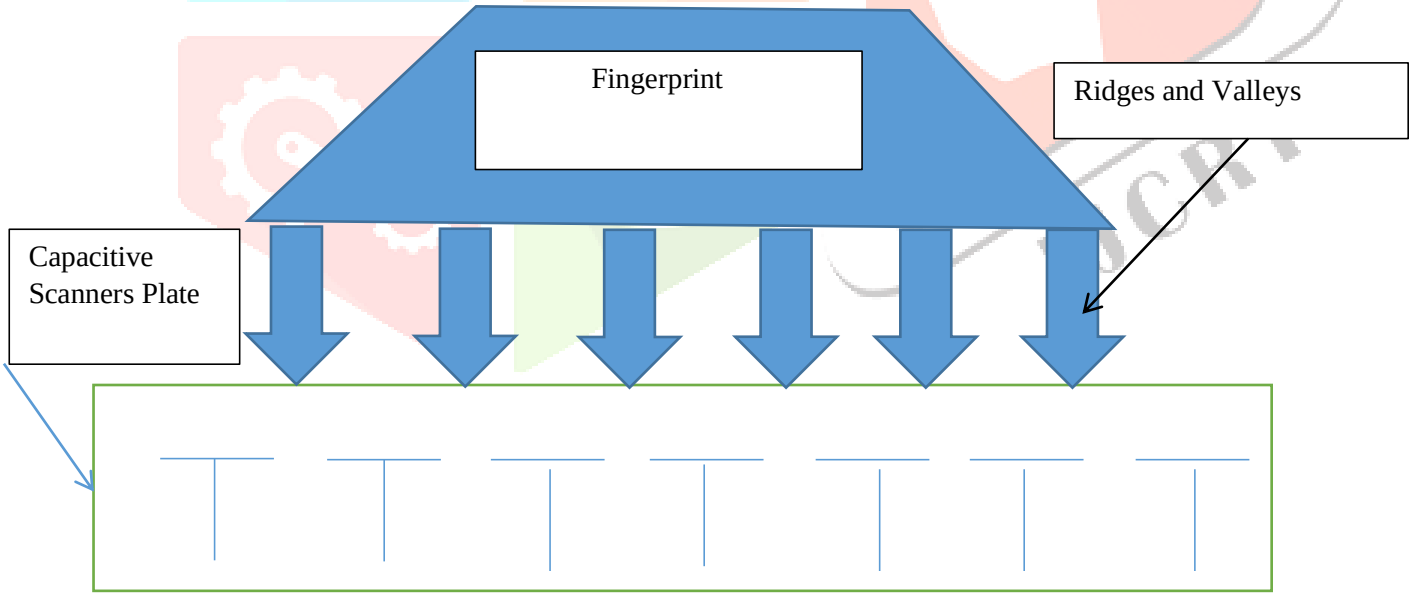


Figure 1.4: Capacitive scanners

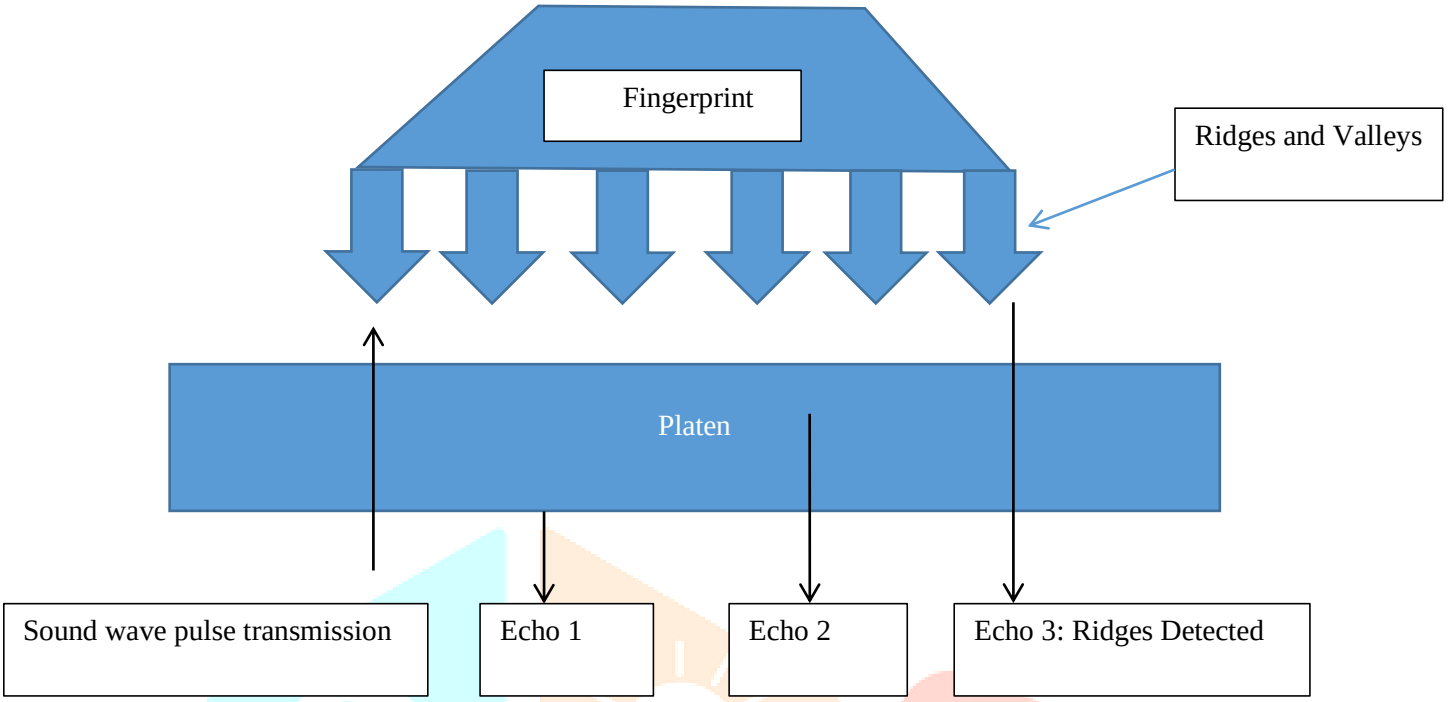


Figure 1.5: Ultrasound fingerprint scanners

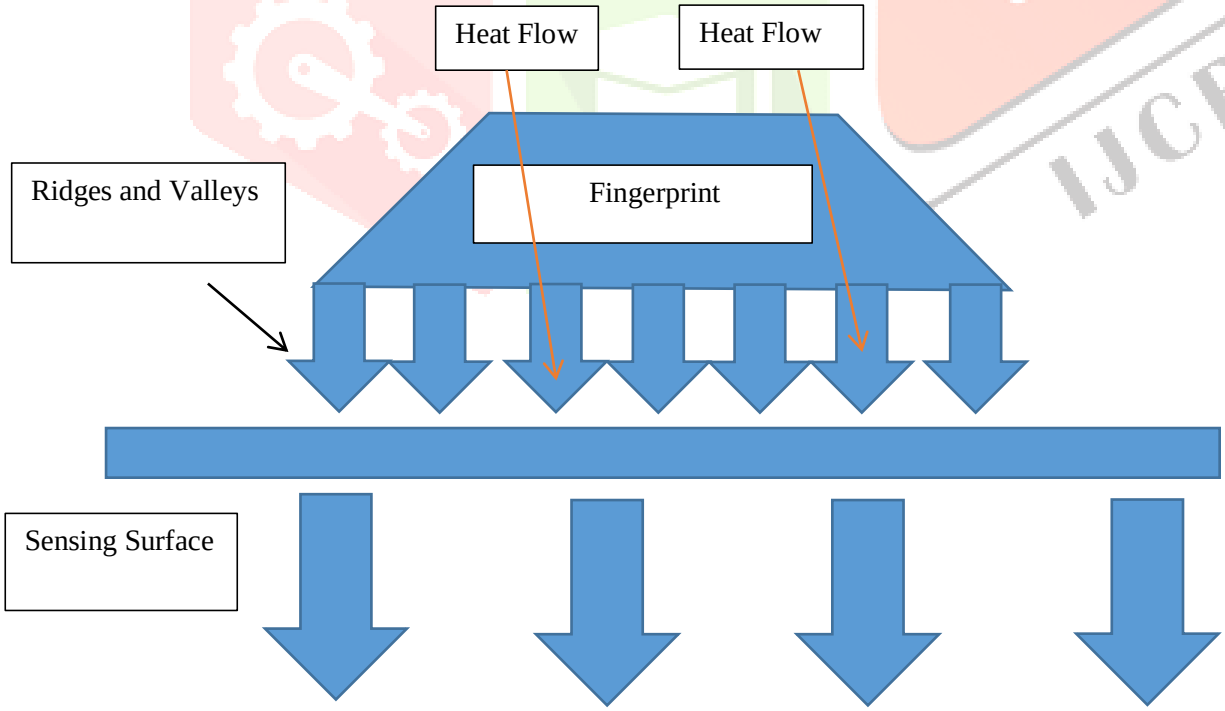


Figure 1.6: Thermal Scanner

1.1.3 Applications of Fingerprint technology in use

Aside from the fact that biometrics are utilized in many smartphones nowadays, biometrics are used in a variety of areas. Biometrics are utilized in the following disciplines and organizations, for example:

- **Law Enforcement** It's utilized in methods for identifying criminals like fingerprint or palm print authentication.
- **Healthcare** It is utilized in systems that employ fingerprints for identification, such as national identity cards and health insurance schemes.
- **Attendance system** Employee fingerprints are used to verify who is actually clocking in and out of work on a daily basis. The technology scans the employee's finger, determines coordinates, and then maps the endpoints and intersections of the fingerprint.
- **Locking system** Personal authentication, such as accessing a computer, a network, an ATM machine, a car, or a house, is a far larger application of fingerprints. The process of validating the fingerprint picture to unlock an electronic lock using a fingerprint recognition system is known as fingerprint verification.
- **Vehicle starting system** the microcontroller is connected to the fingerprint sensor, and we also have an LCD display, as well as push buttons and a starting motor. The motor is used to illustrate how to start a car. This technology uses a fingerprint-based approach to automate vehicle security.

1.1.4 Advantages

- **Authentication with less time** Businesses used to utilize the ‘pen and paper' technique, in which an employee would sign in by writing his signature on a ‘attendance sheet.' The manual method would take time, but the biometric technology eliminates the requirement for physical attendance. Employees may to keep track of their attendance, just sign in using a retina or fingerprint scanner.
- **Enhances the safety system** some people have trouble remembering passwords, pins, and security codes. Biometric technology has eliminated the need for passwords. Retinal recognition, fingerprint scanning, and face scanning are among the techniques available. Fingerprints cannot be faked, thus they may be used to secure sensitive data. On the other side, passwords and pins can be stolen.
- **Convenience is maximized** because it offers valid sign-in and sign-out data, the biometric system is a handy way to track each employee in a business. To compute leaves, late sign-ins, or overtime for specific employees, HR administrators don't have to go through stacks of attendance papers. The helpful tool compiles all of the data for you.
- **Complete Access Management** HR officials and companies may manage who gets access to the office building, vaults, sensitive data, and lockers using physical authentication. They can use the biometric technology to restrict access to unauthorized personnel. All you do is grant access to only the most important people.

- **Scalability** The biometric system is a one-time purchase for each company. Whether it's a new department or an unique initiative, technology may be employed for several aspects of the business. It is the most scalable security solution available today for both large and small organizations. for example, Banks are investing in low-cost mobile app development and biometrics, allowing customers to sign documents with their smartphones' fingerprints!
- **Flexible** The biometric technology allows users to utilize bodily features instead of passwords or pins, giving them more freedom. In today's world, most smartphones include fingerprint scanners that allow users to quickly access their data. Similarly, applications like whatsapp include finger identification, which helps users safeguard their data from unauthorized access.
- **Complete data precision** The data provided by a corporate biometric is completely accurate and reliable. The biometric technology, which only gives authorized personnel access, keeps intruders out. Data security is provided once a physical characteristic has been introduced into the system by limiting outside access.

1.1.5 Limitations

- **Disabilities Physical** The authentication system only recognizes the features that were input, and if the user's physical characteristics alter even slightly, the system will fail to recognize them. The reason is when a finger that has been burned or injured.
- **Physical characteristics cannot be modified** the biometric system, like any other system, isn't flawless. In order to enhance, the system is still improving. As a result, consumers are unable to trust the protection of their personal information. They can't try to 'modify' their identification characteristics in the same way they may change passwords after a data breach [7].

- **Malfunctioning Software** Because it is an automated system that runs on energy, the biometric system is also unreliable. No one can enter or depart if there is a power outage. Furthermore, if the program has a problem or fails for any reason, users' access will be restricted until the software is restored.
- **No Remote Access** User personnel cannot access the system ‘remotely' in a crisis, such as a security breach, to try to remove sensitive data, which is a fundamental flaw in the system.
- **Breach of Security** In the event of a security breach hackers frequently take all data in order to subsequently get access to illegal areas of the organization. No one can do anything after the data has been taken since it cannot be changed.

1.2 Motivation of Research

Biometric authentication is the automatic identification or verification of persons based on their unique physiological or behavioral features such as fingerprints, gait, iris, and so on. Fingerprint biometrics is a notion that has been around for thousands of years. East Asian potters used to leave their fingerprints on the clay

while it dried. In the nineteenth century, criminologists utilized fingerprints to identify chronic offenders. Biometrics, on the other hand, originally debuted as an automated technique in the 1970s [8]. Biometrics was first used in commercial applications to restrict physical access to facilities.

This tendency is expected to continue as technology advances. Fingerprint biometrics has become a highly popular and frequently utilized technology due to the growing requirement to minimize fraud and enable safe access to physical and logical assets.

Fingerprint authentication is a highly powerful authentication technique since it is based on something you are rather than something you know or have. Passwords and tokens are extremely vulnerable to loss or theft. The most common cause of data leaks and security breaches is a weak or hacked password. Passwords are the weakest link in a company's security system, and even the strongest passwords are vulnerable to sophisticated hacking assaults. In addition, the expenses of maintaining password and token-based systems are prohibitively expensive and inefficient. IT support time is wasted resetting lost or forgotten passwords, which affects employee productivity.

1.3 Problem Statement

The primary objective of this study is to decrease data loss. fast detection process in less time, improve accuracy.

1.4 Objectives

Objectives of this work precise as follow:

- How to detect a Fingerprint by a Scanner
- Store Fingerprint data in a system
- Define Matching Process
- Study of Highest Alignment Algorithm
- BLAST Algorithm

1.5 Thesis Organization

This thesis comprises of following six sections which are as follow:

Chapter 1: A brief review of fingerprint systems, the requirement of a bike locking security system, the project's inspiration, and the thesis's aims.

Chapter 2: This covers the background of the research.

Chapter 3: This covers the literature survey of different Model.

Chapter 4: This covers the proposed approach defined to store and matching data using Algorithm.

Chapter 5: This covers the results of implemented approach

Chapter 6: This concludes the research with conclusion and future scope

CHAPTER 2 : BACKGROUND WORK

I had read many papers on this topic over the past 1 year and found out about several challenges and advantages. There are numerous concepts and ideas that have been useful in my choice of topic. This topic is from a well- known area but it suffers from many limitations due to the presence of an adversarial environment. Therefore, a lot of work will need to be done as it is challenges and adventure for making enhancement in this field.

2.1 Background

We will give the highest level of security in this project since the engine will be started using a fingerprint. So, to start our bike, we must first lay our finger on the finger print scanner, which will then scan our finger. With the serial interfacing, it is connected to the Grow K-202. The data from the scanner (R-503) is read by the Grow Microcontroller Board, which then allows authorized users to start the bike. Grow will deny the security request if any unauthorized user attempts to start the bike.

Finger Print Sensor Module or Finger Print Scanner is a Grow Microcontroller module that takes a finger's print image, transforms it into a comparable template, and puts it in its memory on selected ID (place). The microcontroller is in charge of the entire operation [1].

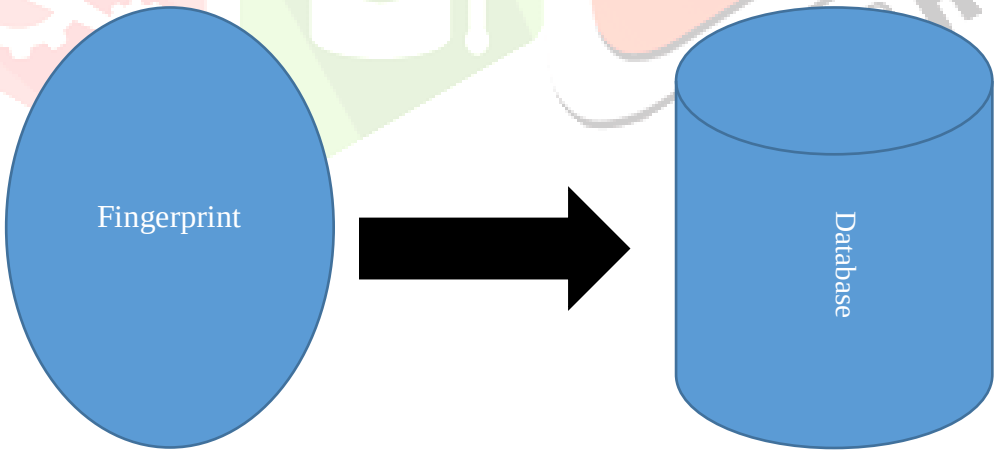


Figure 2.1: Strore Fingerprint Data in different format

2.2 Store Fingerprint Data in Database

Store fingerprint data in a database, a microcontroller using different types of Alignment algorithms. The structure of this data is matrix type. The data is divided into two parts [13].

1. Text data
2. Query Data

2.2.1 Text Data

When a new user stores the data in microcontroller memory, then this type of data is called Text data.

2.2.2 Query Data

When an authorized user puts a fingerprint on the scanner, then an algorithm works on this data and the process is started to match this data to the text data. This type of data is called query data.

2.3 Algorithms

Sequence Alignment is simply the alignment of two sequences or more. Each sequence consists of an amino acid or nuclear acid. A sequence defines an oxygen level, muscle, DNA in humans etc. This Algorithm is used for maximum Matching Process between Query and Text data. It is divided into many parts:

when a data is consist only two sequences S1,S2 then it is called single Sequence Alignment Algorithm and a data is consist a many sequence S1,S2,S3,.....,Sn it is called Multiple sequence alignment Algorithm. The Alignment Algorithm is called Pairwise Algorithm because it consists of data in pairwise [14].

The algorithm is divided into two parts.

1. Global Alignment Algorithm
2. Local Alignment Algorithm

2.4 Classification of Algorithm

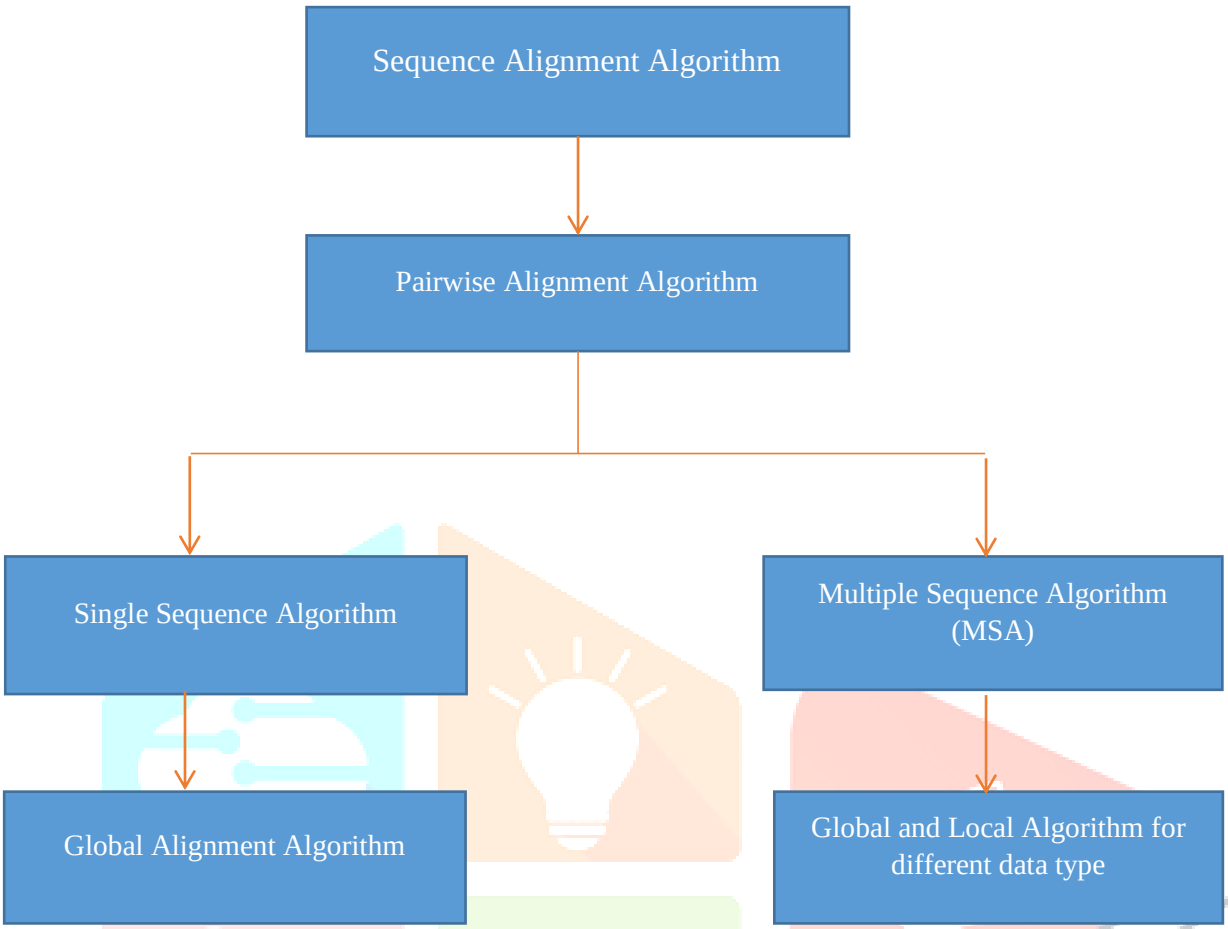


Figure 2.2: Classification of Algorithm

2.5 Difference between Local and Global Alignment

Global	Local
Best score from among alignment of full length.	Best score from among alignments of partial sequence.
Developed by Needelman -Wunch.	Developed by Smith & Waterman.

Table 1: Local and Global Alignment Algorithm

CHAPTER 3 : LITERATURE SURVEY

The previous work on the Fingerprint System is summarized in this chapter.

3.1 Introduction

The main goal of our project is to secure the bike by using a fingerprint sensor to scan the fingerprints of n people. Authorized people must register their fingerprints with the system using the fingerprint sensor, and each person is given a unique ID that is stored in the data. Authorized people are the only ones who can start the bike, while the rest of the people cannot.

3.2 Related Work

Fitria Hidayanti et al. a fingerprint sensor is used to build a motorcycle security system that increases security on bikes that employ a two-channel relay module as a hardware-software interface. The fingerprint sensor is a device that compares a person's fingerprint pattern to a pattern stored in the sensor's memory and may be used to start the motorcycle instead of the ignition key. The Arduino Uno is a microcontroller-based tool for receiving responses and issuing commands based on those responses, thus the security system that uses this fingerprint can only access and start the engine if the owner's fingerprints are registered in the fingerprint sensor [1].

Dr.V.Nandagopal, Dr.V.Maheswari et al. focused on The use of a biometric system can help to decrease the problem of vehicle hijacking or auto theft caused by simple access to the vehicle's functioning system. The requirement of starting a vehicle's engine as a means of protection and access restriction in many high-value assets has become more critical. Biometric systems have been around for quite some time. It has been used as a robust security solution in a variety of applications and will be used in more industry of automobiles [2].

Aditiya Shankar et al. concentrating on a project involving the replacement of traditional locking systems approaches. They used biometrics to replace conventional techniques such as lock and key and password authentication. They essentially utilized fingerprints for the authentication method; anyone with a fingerprint recorded in the database may simply access the locker. They also provide an alarm system to notify neighbours if an unauthorized person or thief attempts to get access to the locker. They must scan their fingerprint pictures to confirm that they have permission to unlock the locker door. The scanner will be controlled by an 8051 microcontroller, which will be connected to the scanner [3].

Omidiora E.O et al. they rejected traditional ways of bike locking and instead created a finger print-based locker, which is a reliable security mechanism in a variety of security domains. In their prototype, a software module is utilized to store legitimate users' information in a database, and hardware is given for interfacing. Visual Basics, Visual C, and Visual C++ were used for programming. This prototype was created using Visual

Basic 6.0 Enterprise Edition. Twenty test photos were placed in the database to test the prototype. The installation went well, and authorized and unauthorized users were clearly distinguished on the microcontroller. For authorized users, logic 1 is sent, whereas for unauthorized users, logic 0 is transferred [4].

Karthikeyan.a et al. focused on every person has a unique fingerprint, according to legend. They included a secure keypad for adding and removing people from the database, which is a great idea. NITGEN's FIM3030fingerprint module is utilized for this. Microcontroller AT89C52 is utilized to control the whole drive unit. A LCD display is also available for displaying information about permitted and unauthorized users. Because the decoder has a low propagation latency, it may be used for data routing and interfacing with rapid memory units. The latch 74HC373, which is a high-speed Si-gate CMOS device, is included. A relay serves as an interface between the microcontroller output and the car's ignition system [5].

Pavithra. b.c et al. in this project, I am mostly concerned with security. As a scanner, they utilized R303A. The ROM, DSP, and RAM of this module are all built-in. The fingerprint module can save the fingerprints of up to 100 people. The Master and User modes of operation are available for this module. The fingerprints are registered in master mode and saved in the scanner's ROM with a unique id. For the final phase of verification, they gave a unique identification number that allows for three incorrect tries. At each locker's door, install a digital code lock that is controlled by a password. The password consisted of six numeric integers only, with no other characters. For password storage and verification, this locking mechanism is connected to a microcontroller. This lock has an LCD screen, a keyboard, and an 8051 microprocessor. Because it is commercially available, it may be used at any door locker [6].

Crystalynne D. Cortez et al. focused on the creation of a biometric locker system based on a microcontroller with a short messaging service. The system was powered by a 9-12Vdc supply. The Arduino board's microprocessor ATMEGA 644 was used to connect the input and output hardware components. The fingerprint sensor for biometric recognition, the keypad for passcode encoding, and the real-time clock for displaying the current date and time are all input devices. The Arduino Integrated Development Environment is used to program the microcontroller. The system's microcontroller was an ATmega644, which was placed in an Arduino board. It was in charge of the biometric locker system's functionality. The ATmega644 is an 8-bit microcontroller with 40 pins and a low-power complementary metal oxide semiconductor (CMOS) design based on the AVR improved reduced instruction set computer (RISC) architecture. By executing strong instructions in a single clock cycle, the ATmega644 can reach throughputs of up to 1 million instructions per second per MHz. This enables system designers to optimize power usage vs processing performance. It has a memory capacity of 64 KB for program instructions [7].

Jyoti Lakhani et al. focused on Needleman–Wunsch, noblest, Emboss-Needle, ALIGN, LALIGN, FOGSAA, DIALIGN, ACANA, MUMmer, and a few more algorithms that are widely used for global pair-wise sequence alignment include Needleman–Wunsch, noblest, Emboss-Needle, ALIGN, LALIGN, FOGSAA, DIALIGN, ACANA, MUMmer, and others. The Needleman–Wunsch method is one of the most common pair-wise

sequence alignment techniques, although the algorithm output is associated with significant time and space complexity [13].

S. No.	Author	Project Name	Technology	Implementation
1	Fitra Hidayanti, Fitri Rahmah, Araya harma Wiryawap	Motorcycle Security system with fingerprint sensor using Arduino Uno Microcontroller	Arduino Uno with fingerprint Scanner	Yes
2	Dr V. Nandgopal Dr.V.Maheswari, C. Kannam	Vehicle starting system using fingerprint	Arduino Uno, 2 channel relay, R 307 fingerprint scanner	Yes
3	A.Aditya Shankar	A fingerprint based door locking system	8085 Microcontroller with scanner	Yes
4	Karthikayan	Fingerprint based ignition system	Microcontroller AT89C52 with FIM 3030 fingerprint scanner	Yes
5	Pavithra b. c	Fingerprint based bank locker system	R- 303A scanner with microcontroller	Yes
6	Crystalynne D. Cortez	Development of microcontroller based biometric locker system with short msg services	ATMEGA 644 microcontroller with Arduino Uno board	Yes

7	Jyoti Lakhani	MPSAGA: A matrix based pairwise Alignment algorithm	LALGIN, ALIGN, FOGSAA	Yes

Table 2: Compare of Related work

CHAPTER 4 : PROPOSED METHODOLOGY

4.1 Proposed Solution

In our day-to-day lives, security is a key concern, and digital locks have become an integral element of these security systems. Our Bike may be secured using a variety of security methods. In this post, we'll connect a fingerprint sensor module to a Grow Board and create a biometric security system based on fingerprints to start a vehicle engine. Fingerprints are regarded one of the safest keys for locking or unlocking any device since they can distinguish any individual and are difficult to copy.

Fingerprint Sensor Module, also known as Fingerprint Scanner, is a module that takes a finger's print image, transforms it into an analogous template, and saves it in Grow's memory on a specified ID (place). Grow controls every step of the process, including collecting a fingerprint image, converting it into templates, and saving the location.

Our suggested solution solves all of the present system's security issues while also providing high security and efficiency. This is an excellent/ideal option for avoiding the inconvenience of a stolen/lost key or an unwanted entrance. Fingerprinting is a fantastic answer for these issues since it has a high level of identification accuracy. Friction ridges are a flow-like pattern of ridges seen on the skin of our palms and soles. Each finger's pattern of friction ridges is distinct and unchangeable. As a result, fingerprints are a one-of-a-kind form of identification for everyone.

Users' fingerprints are scanned using a R-503 fingerprint scanner, which is used to ensure authentication. Fingerprint scanning is a more accurate and cost-effective approach, with almost no duplication. Verification is simple using a fingerprint recognition system. The system compares an input fingerprint to a user's enrolled fingerprint to see whether they are from the same finger, and if they are, the engine is started.

4.2 Hardware Description

4.2.1 Grow K-202

With an inbuilt STM8 microprocessor, the Grow K202 Low Power Consumption Control Board is an all-in-one control board. The fingerprint access control system can use this module as a stand-alone system. The board has an inbuilt relay that the microcontroller activates when the fingerprint is recognized. A multi turn potentiometer that can be changed from 0.5 sec to 13 sec may control the relay's activation time.

- After being powered up, the module will be in its original factory mode, and any fingerprint will be able to activate the relay.
- Long-press the SET button for 3-4 seconds to register the fingerprint; the module is ready to register the fingerprint when the BLUE LED starts blinking. After the five beeps, remove the finger you want to register from the scanner. Simply add additional fingerprints or wait until the LED stops blinking if you want to add more.
- After the LED stops blinking, you may use the registered fingerprint to activate the relay. When a registered fingerprint is read, a BLUE led will illuminate surrounding the sensor, and if an unregistered fingerprint is discovered, a RED/ORANGE led will glow.
- The relay's SET time may be adjusted using the multi-turn potentiometer.

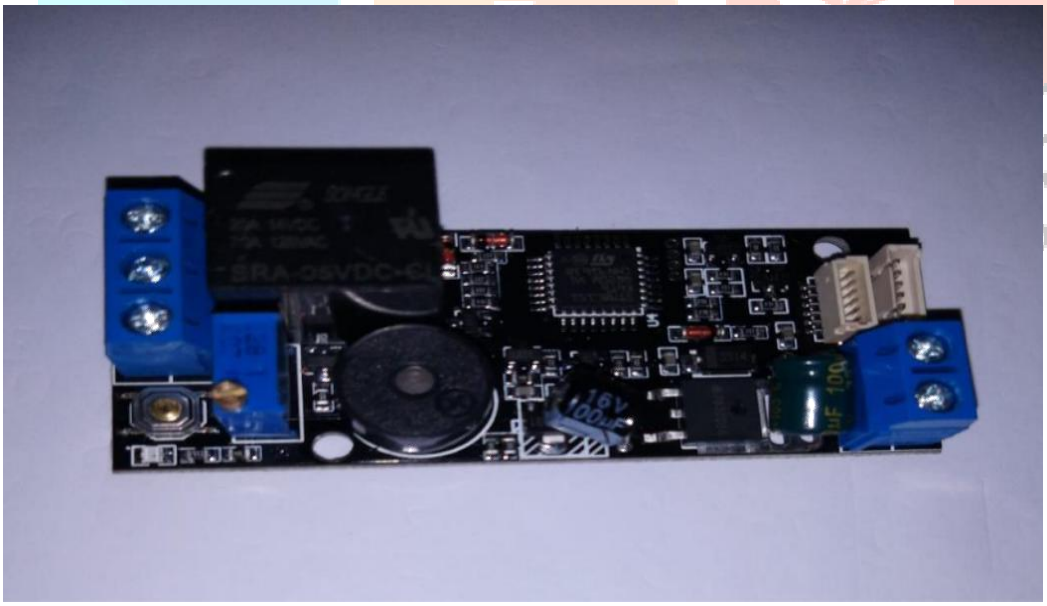


Figure 4.1 Grow K202 Board

4.2.1 8-bit microcontroller STM8S

The STM8S 8-bit Microcontroller (MCU) series from STMicroelectronics combines cutting-edge performance, ruggedness, peripherals, and cost-effectiveness. The STM8S MCUs from STMicroelectronics have a 20 MIP A robust design (dual watchdogs, clock security, and IEC61967-compliant EMI emission), a rich peripheral set (10-bit ADC, advanced timers, CAN, UARTs, SPI, I2C), and maximum integration are all features of the STM8 8-bit core with Harvard Architecture and 3-stage Pipeline (true EEPROM, 16MHz and

128KHz on-chip RC oscillators). STMicroelectronics' STM8S family meets the stringent requirements of industrial and appliance applications while also providing a variety of other benefits, such as high performance and code density, memory scalability, and lower system cost and external component needs.

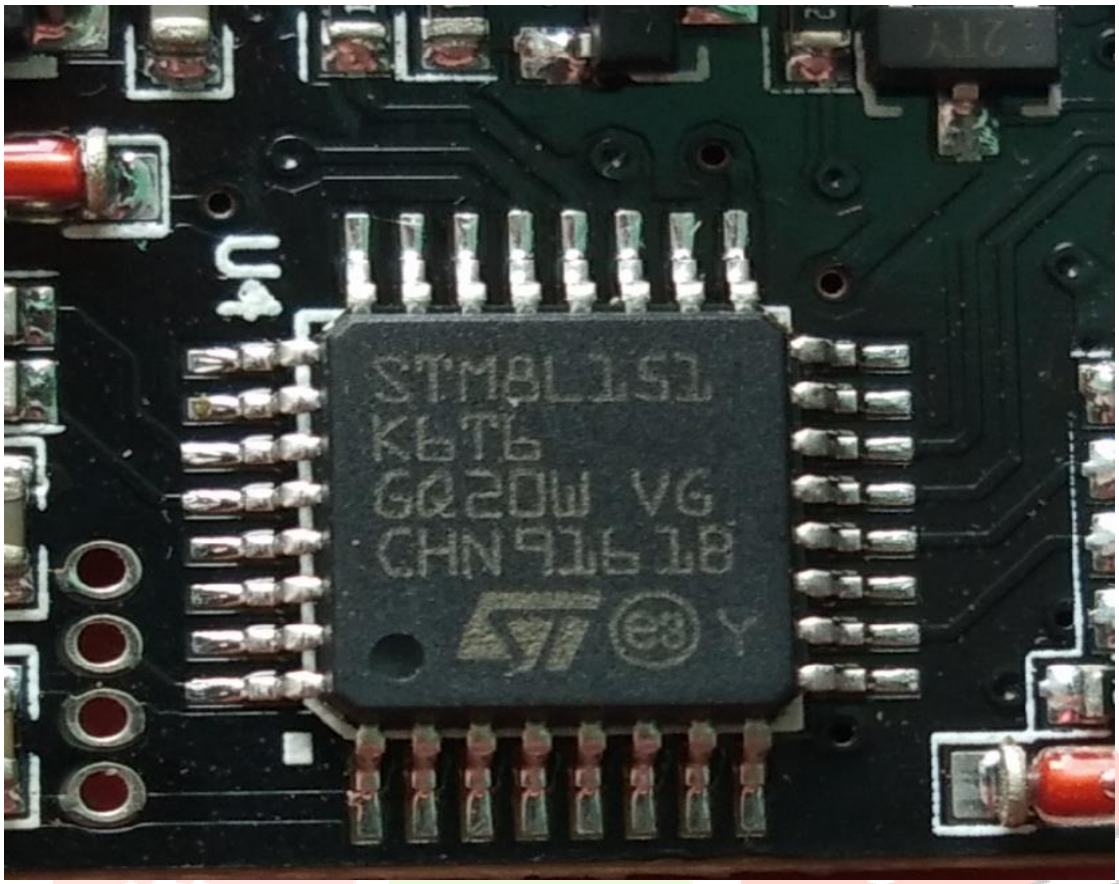


Figure 4.2: STM8 Micro-Controller

4.2.3 Features

Model	K-202
Processor	STM8
Operating Voltage (VDC)	10-24
Output Type	Relay(max current: 10A)
Standby current	15uA
Fingerprint Capacity	250
Flash Memory	32 kb
EEPROM Memory	1 kb
RAM	2 kb
Scanning Process Speed	Less than 0.2 second
Matching Process Speed	Less than 0.3 second
Matching Method	1:1, 1:N
FRR	< =1%

Operating Temp. (degree C)	-20 to 60
Working Humidity Range	10 to 85%
Shipment Weight	0.08 kb
Dimensions	5*4*2 cm
Pins	28
Support Scanner	R 503, R 307, R 305, etc.

Table 3: Features of Boards

4.2.4 R 503 Fingerprint Scanner

The R503 is a fingerprint sensor that scans and saves fingerprints when they are put on the sensor's face. These fingerprints are stored in a database and may be viewed quickly. With this all-in-one optical fingerprint sensor, adding fingerprint detection and verification will be a snap. For a better user experience, it also features a built-in LED ring around the detecting pad that can be adjusted to red, blue, or purple. Up to 250 fingerprints can be stored in the onboard FLASH memory.

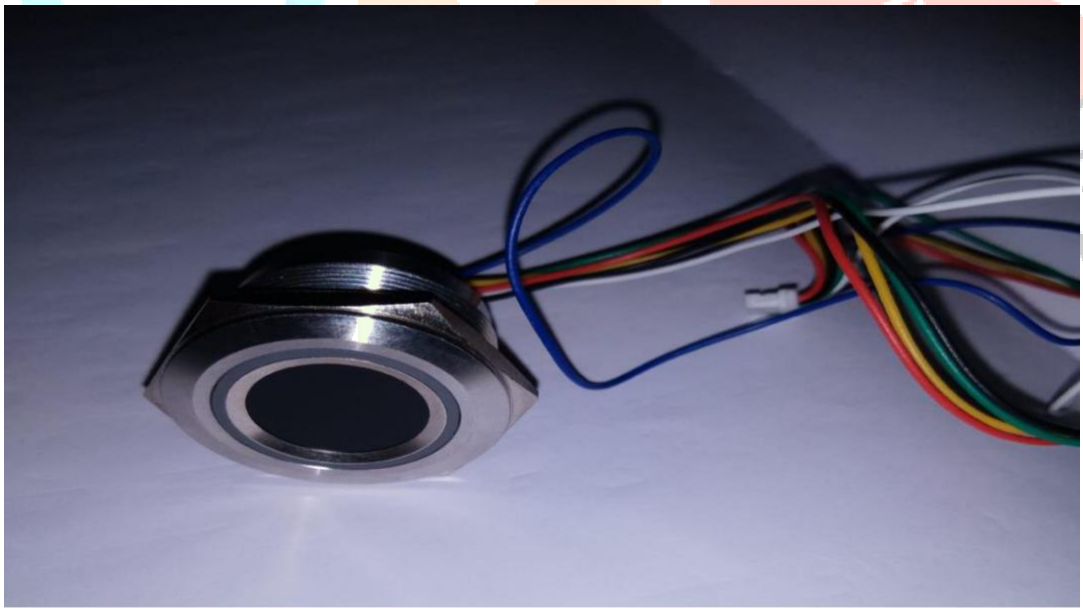


Figure 4.3: R-503 Fingerprint Scanner

4.2.5 Background Working

The friction ridges of a human finger leave an impression, which is referred to as a fingerprint. They quickly adhere to smooth surfaces such as glass, metal, or polished stone. When a finger contacts the top side of a glass prism, the ridges make contact with the prism surface, while the valleys stay at a distance. A diffused light is utilized to illuminate the left side of the prism [5].

Light enters the prism and is reflected in the valley before being absorbed at the ridges. The ridges can be distinguished from the lowlands due to the absence of reflection. The light rays escape the right side of the prism and are focused onto a CCD (Charged Coupled Device) or CMOS sensor through a lens (Complementary Metal-Oxide Semiconductor). These feature a fast response time, low sensitivity, and a lot of fixed pattern noise. For live scan acquisition, this method is known as FTIR (Frustrated Total Internal Reflection Techniques) [12].

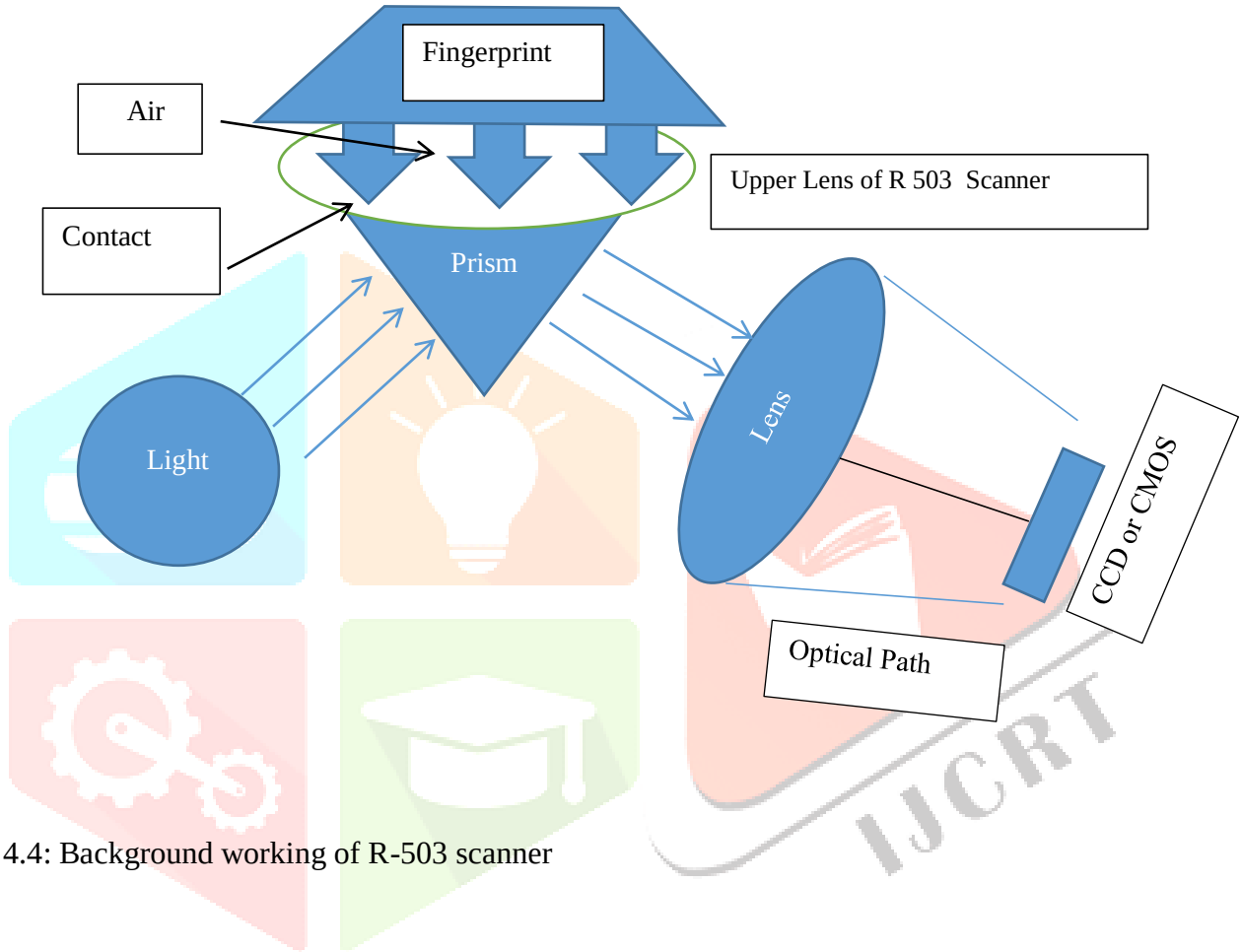


Figure 4.4: Background working of R-503 scanner

4.2.6 Flowchart

Step 1: Start.

Step 2: Connect system on +12v dc Battery.

Step 3: After connection system is ON.

Step 4: Touch a fingerprint on a scanner to store data in a database.

Step 5: Start process for detection of fingerprint ridges show in fig.(4.4).

Step 6: After ridges detection apply Local Alignment Algorithm.

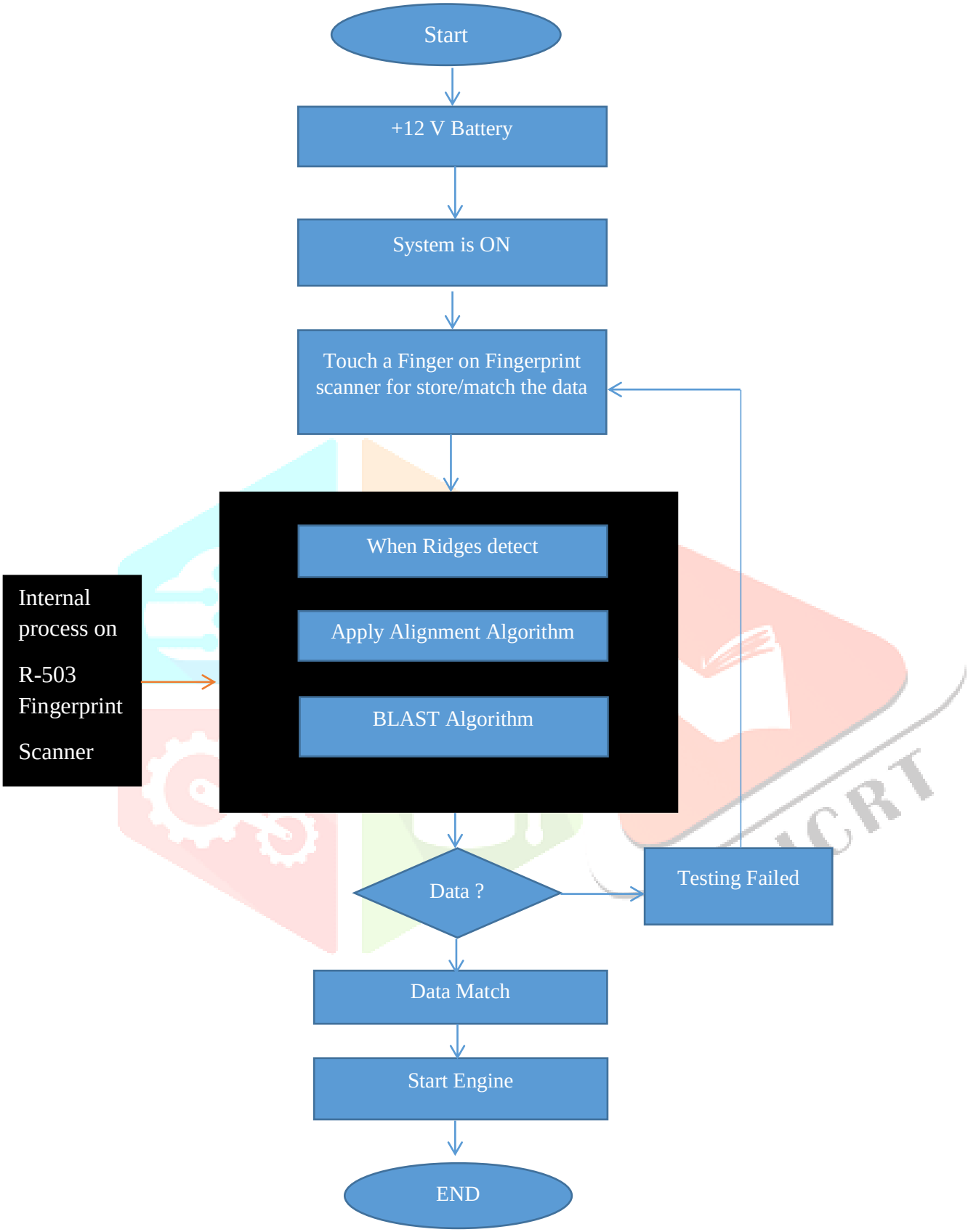


Figure 4.5: Flowchart

Step 7: After the Local Alignment Algorithm, then apply the BLAST Algorithm.

Step 8: The BLAST Algorithm is a tool of the Local Alignment Algorithm, which is used to store data in a database. This data is a matrix data type which is called Text Data.

Step 9: When fingerprint data is stored in a database, then an authorized user scans a fingerprint with a scanner for the matching process.

Step 10: After ridge detection The Alignment Algorithm works on matching data to authorized user data. The data is called Query Data.

Step 11: When authorized user data is matched, then the bike's engine starts.

Step 12: When data is not matched it follows Step 9 (When an unauthorized user scans a fingerprint, then it is denied request each time).

4.2.7 Functional Block Diagram

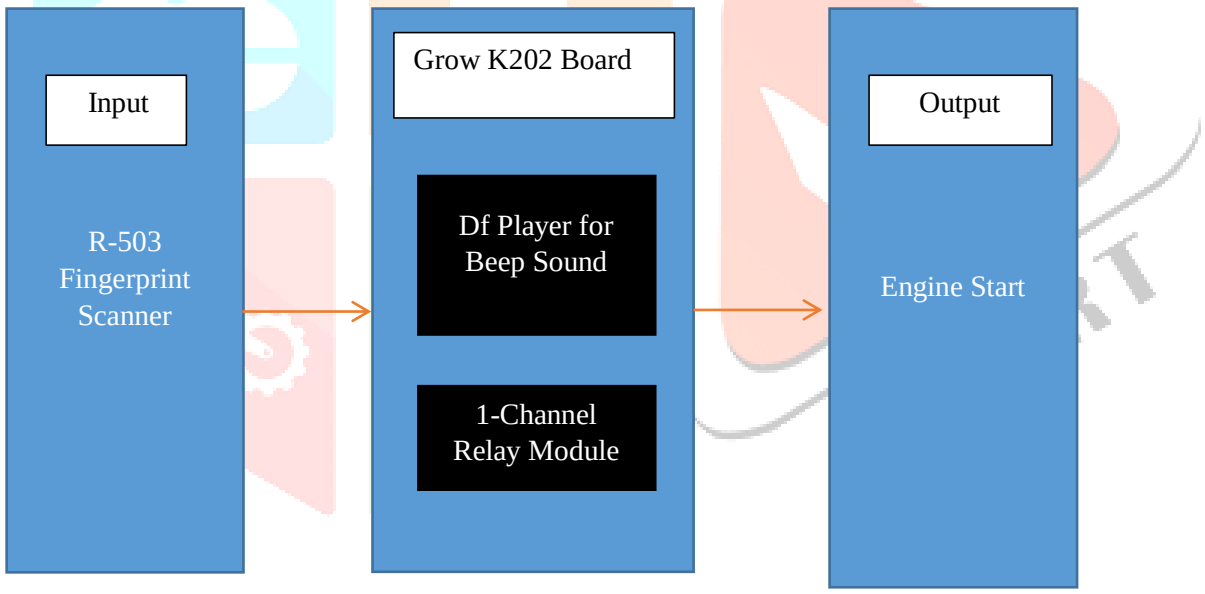


Figure 4.6: Functional Block Diagram

The Functional Block Diagram is divided into three stages.

Input Stage: In this stage, users store fingerprint data in a database and match authorized users' data by high performance Fingerprint scanner (R-503) using different type process .

Microcontroller: In the second stage, data is stored in memory and matches the data. It uses an STM8 Microcontroller which has fast speed for scanning and matching process. In which used inbuilt Relay and mini speaker for beep sound which is useful in many times.

Output: When data is matched, then the bike's engine is start.

4.3 Alignment Algorithms

The Alignment Algorithm is used for maximum matching between two or more sequences. The sequence of data in store in a database which is called Text data and which sequence matches the Text data is called Query data [16].

4.3.1 Sequence Alignment Algorithm: Sequence Alignment is simply the alignment of two sequences or more. Each sequence consists of an amino acid or nuclear acid. A sequence defines an oxygen level, muscle, DNA in humans etc. This Algorithm is used for maximum Matching Process between Query and Text data.

4.3.2 Multiple Sequence Alignment Algorithm :

- When a data is consist only two sequences S1,S2 then it is called single Sequence Alignment Algorithm and a data is consist a many sequence S1,S2,S3,.....,Sn it is called Multiple sequence alignment Algorithm. The Alignment Algorithm is called Pairwise Algorithm because it consists of data in pairwise.
- Two similar amino acids (e.g. arginine and lysine) receive a high score, two dissimilar amino acids (e.g. arginine and glycine) receive a low score. The higher the score of a path through the matrix, the better the alignment. The matrix K is found by progressively finding the matrix elements, starting at K(1,1) and proceeding in the directions of increasing m and n .

4.3.3 Pairwise Alignment Algorithm: When Query data and Text data is matched in Pairwise, this type of alignment is called Pairwise Alignment Algorithm. This is also part of the Sequence Alignment Algorithm.

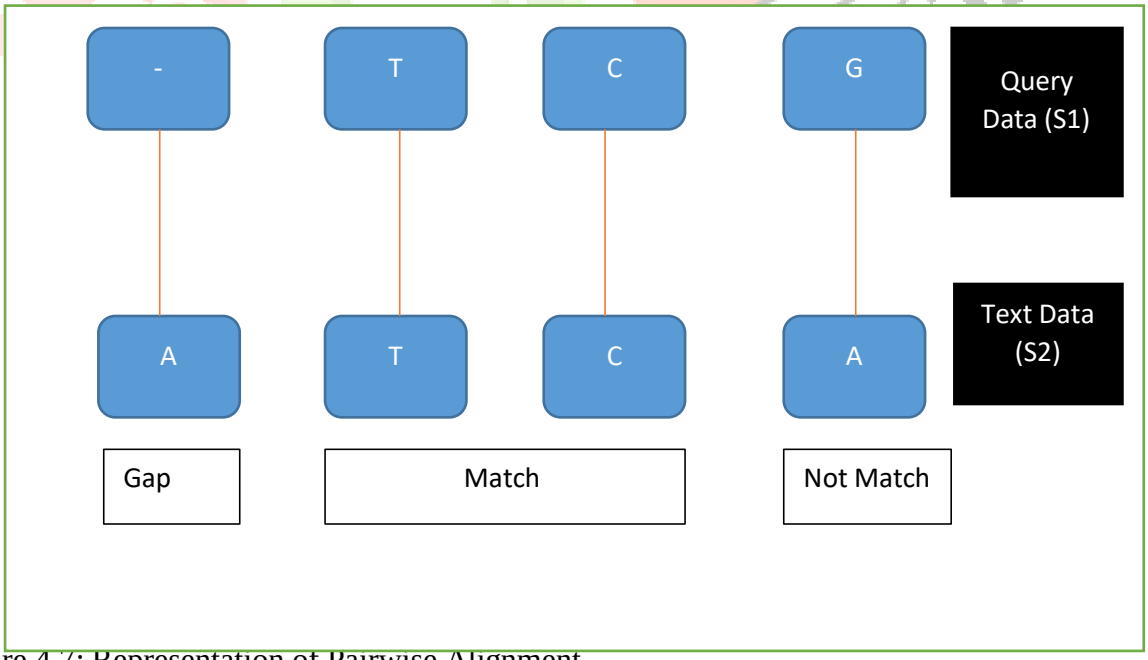


Figure 4.7: Representation of Pairwise Alignment

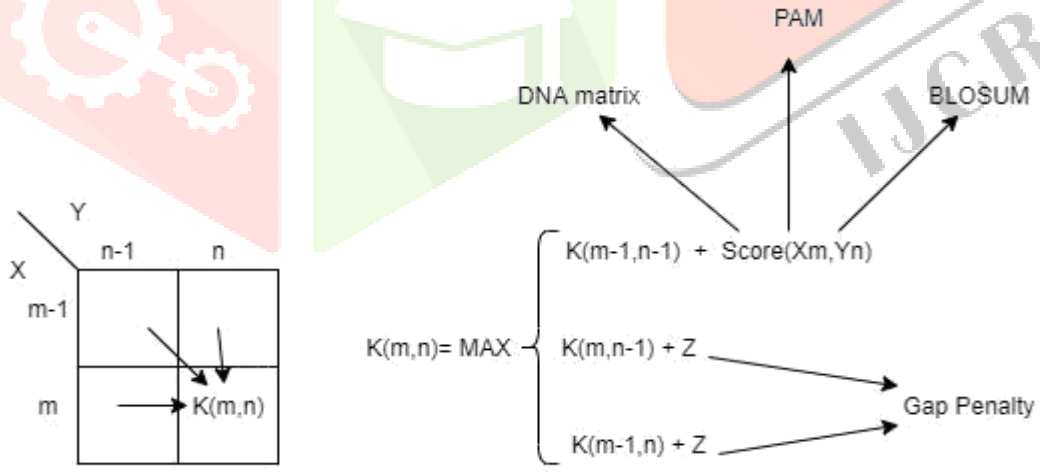
- The Sequence alignment of two sequences i and j is found using a dynamic programming technique. The alignment technique is based on identifying the elements of a matrix K, where K (m,n) is the best score for matching /aligning the sequences (i1,i2,i3,.....,in) and (j1,j2,j3,.....,jn) Where, we can mark this process by a mathematical value.
- For Gap we mark (-2) , Match (+2), Mismatch(-1).
- Total score = (- 2 + 2 + 2 - 1) = +1
- It is divided into Two parts.

1) **Global Alignment Algorithm:** Best Score from among of full length sequence and it is called Needelman - Wunch Algorithm.

2) **Local Alignment Algorithm:** Best Score from among alignments of partial sequence and it is also known as Smith and Waterman Algorithm.

- I used the Local Alignment Algorithm because it is used for multiple sequences. It is scoring the gaps more accurately & fast implementation of affine gaps.

4.3.4 Local Alignment Algorithm: The Smith–Waterman method determines comparable areas between two strings of nucleic acid or protein sequences by performing local sequence alignment. The Smith–Waterman method analyzes segments of all conceivable lengths and optimizes the similarity measure rather than looking at the complete sequence.



4.3.5 Characteristics

- To compare a little and a big Sequence.
- To compare a single sequence to a database in its entirety.
- To compare a partial sequence to a whole sequence.
- Recognize the newly discovered Sequence.
- Compare new gens to known ones.
- The alignment can start/end at any point in the matrix.

- No negative scores in the alignment.

4.3.6 Steps of Algorithm

Step 1: Initialization

K(0,0) = K(0,n) = K(m,0) = 0

Step 2: Iteration

- for m = 1,…, i
- for n = 1,….., j
- Calculate Optimal K(m,n)
- Store Ptr(m,n)

Step-3 : Termination

- Find the end of the best alignment with K(opt)= max{m,n} * K(m,n) and trace back
- Find all alignments with K(m,n) > threshold and trace back

4.3.7 PAM, BLOSUM and DNA

- It is used for Human Organism in Alignment. It is a Matrix which stores data and matches the data. It is part of the BLAST Algorithm and we know that BLAST is a tool of the Local Alignment Algorithm.
- Both the PAM and BLOSUM matrices have substitution scores. Obtained from a study of well-known alignments of proteins that are connected to evolution.
- The point mutation per 100 amino acids is known as a Point Accepted Mutation (PAM).

A. PAM1 denotes a 100-amino-acid point mutation.

B. Different PAM matrices are created by multiplying the PAM1 matrix; this is because numerous replacements might occur at the same time.

- The BLOSUM matrices are newer and are thought to be superior.

A. BLOSUM62, for example, is a matrix derived from observed alterations between proteins with at least 62 percent sequence similarity, and so on.

- **DNA:** If we try solve some distinct Organism then select DNA.

4.3.8 GAP (z):

- **Penalty for constant gaps:** The constant gap penalty, -z, indicates that each gap, regardless of size, receives the same negative penalty.

1. It is the overall number of gaps that matters, not the duration of the gaps.
2. Reduces the amount of gaps in the data.

- **Penalty for linear gaps:** The linear gap penalty is proportional to the magnitude of the gap. The penalty per unit length of a gap is represented by parameter, -z.

A. The penalty for a single large gap is the same as the penalty for numerous minor gaps.

- **Penalty for affine gap**: In biological sequences, a single large gap of length 10 is more likely to occur than ten tiny gaps of length 1.

a. As a result, affine gap penalties prefer larger gaps over single gaps of equal length.

b. They use a gap opening penalty, $o < 0$, and a gap extension penalty, $e < 0$, such that $|e| < |o|$, to encourage gap extension rather than gap introduction.

c. A gap of length L is then given a penalty $z = o + (L-1)e$.

4.3.9 Relation between FASTA and BLAST Algorithm

- For comparing a Query sequence against a database, FASTA stands for First Fast Sequence Searching Algorithms.
- Basic Local Alignment Search Techniques (BLAST) is stand for Basic Local Alignment Search Techniques. It is a FASTA enhancement.
- Both BLAST and FASTA look for local sequence similarity; however, they employ somewhat different algorithms and statistical techniques to achieve their aims.
- Benefits of BLAST

i) User friendly

ii) High speed for searching

iii) Statistical rigor

iv) More sensitive

4.3.10 BLAST Algorithm

Step 1: BLAST is stand for Basic Local Alignment Search Tools. It's a technique. Make a list of all neighboring "words" that score above a certain threshold for each "word" (fixed-length) in the query sequence.

Step 2: Look for these terms in the database.

Step 3: Execute (ungapped) "hit extension" until the score reaches the threshold.

Step 4: Stop when you've reached the maximum scoring extension.

CHAPTER 5 : RESULTS AND DISCUSSION

5.1 Result

5.1 Introduction

Fingerprint Sensor Module, also known as Fingerprint Scanner, is a module that takes a finger's print image, transforms it into an analogous template, and saves it in Grow's memory on a specified ID (place). Grow controls every step of the process, including collecting a fingerprint image, converting it into templates, and saving the location.

Our suggested solution solves all of the present system's security issues while also providing high security and efficiency. This is an excellent/ideal option for avoiding the inconvenience of a stolen/lost key or an unwanted entrance. Fingerprinting is a fantastic answer for these issues since it has a high level of identification accuracy. Friction ridges are a flow-like pattern of ridges seen on the skin of our palms and soles. Each finger's pattern of friction ridges is distinct and unchangeable. As a result, fingerprints are a one-of-a-kind form of identification for everyone.

Users' fingerprints are scanned using a R-503 fingerprint scanner, which is used to ensure authentication. Fingerprint scanning is a more accurate and cost-effective approach, with almost no duplication. Verification is simple using a fingerprint recognition system. The system compares an input fingerprint to a user's enrolled fingerprint to see whether they are from the same finger, and if they are, the engine is started.

5.2 Project Output

The following graphic depicts the overall picture of the project, followed by the predicted project performance. Each image explains one of the project's execution steps, and each figure depicts the result.

5.2.1 General view of the project

When a new user stores a fingerprint in a database, then it clicks the set button and scans a fingerprint with a scanner.

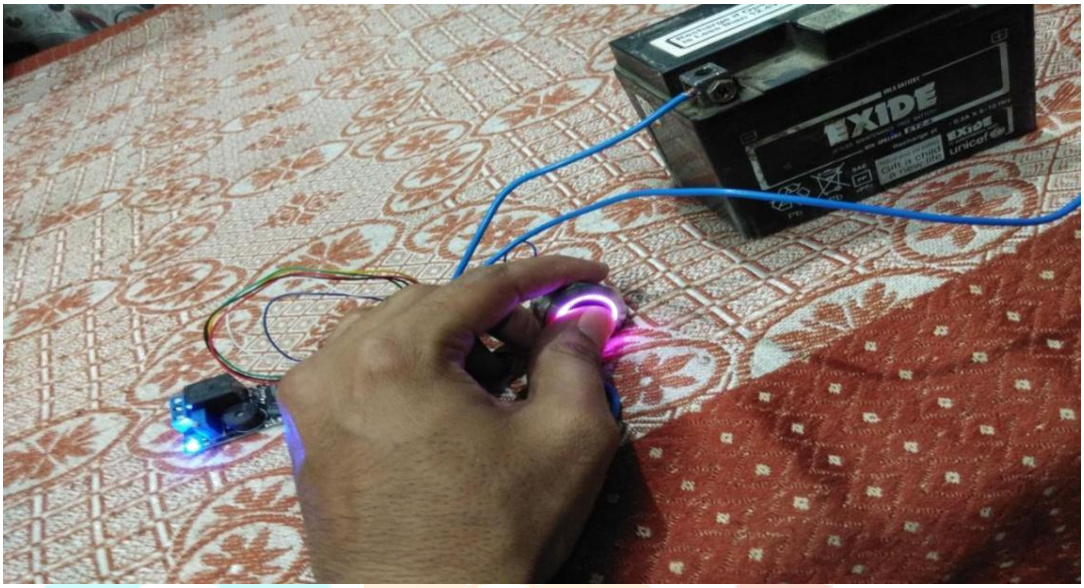


Figure 5.1: Starting Phase

5.2.2 Data Format

Data is stored in FASTA format which is defined as a ">" symbol. It consists of a unique Id, Job title and Protein, etc .

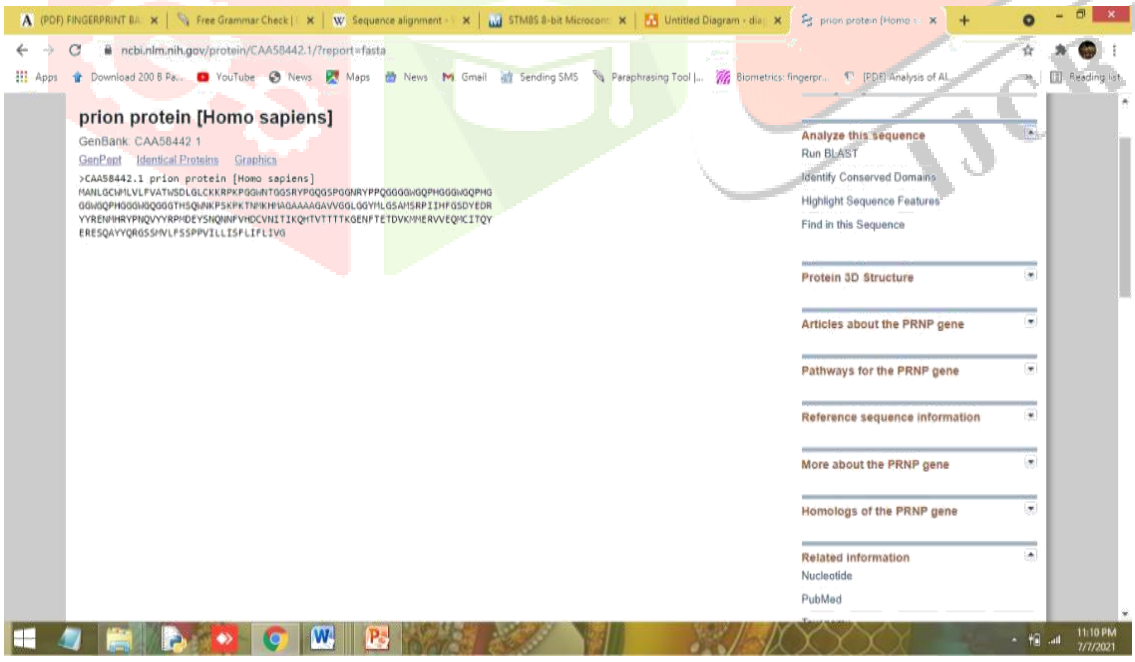


Figure 5.2: Data store in database

5.2.3 Graphical Representation

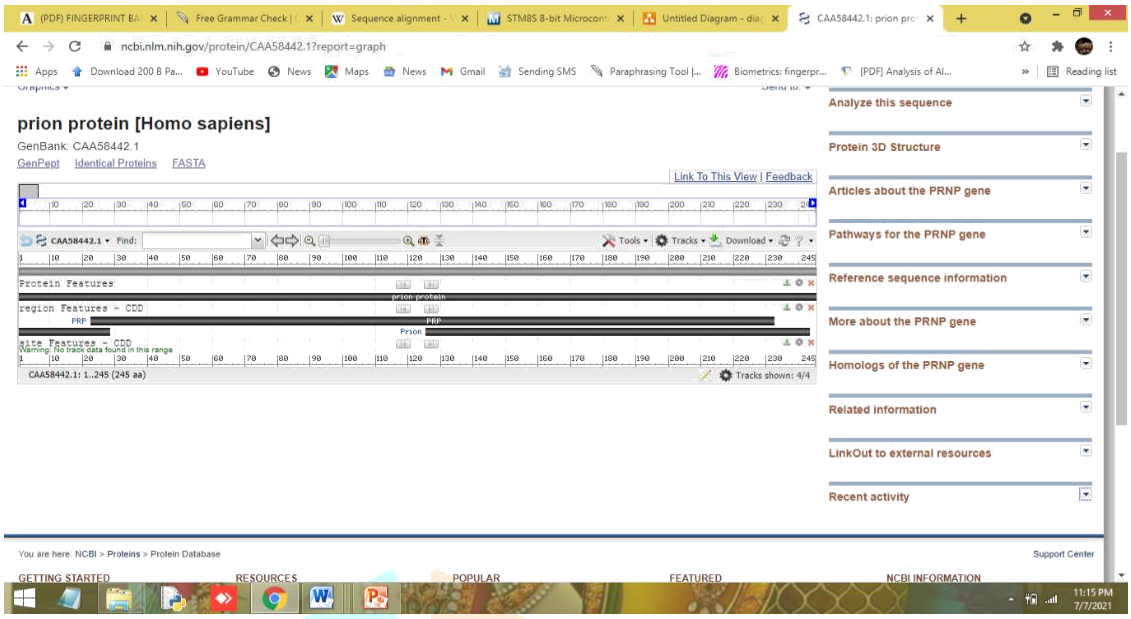


Figure 5.3 Graphical representation

5.2.3 Matching Process

When an authorized user scans a fingerprint to match the data, then the Local Alignment Algorithm starts for matching using BLAST Algorithm.

- Data is matched then Blue Light is on and relay is help for a spark for starting the bike.
- Otherwise, a beep sound is heard it means your data do not match.

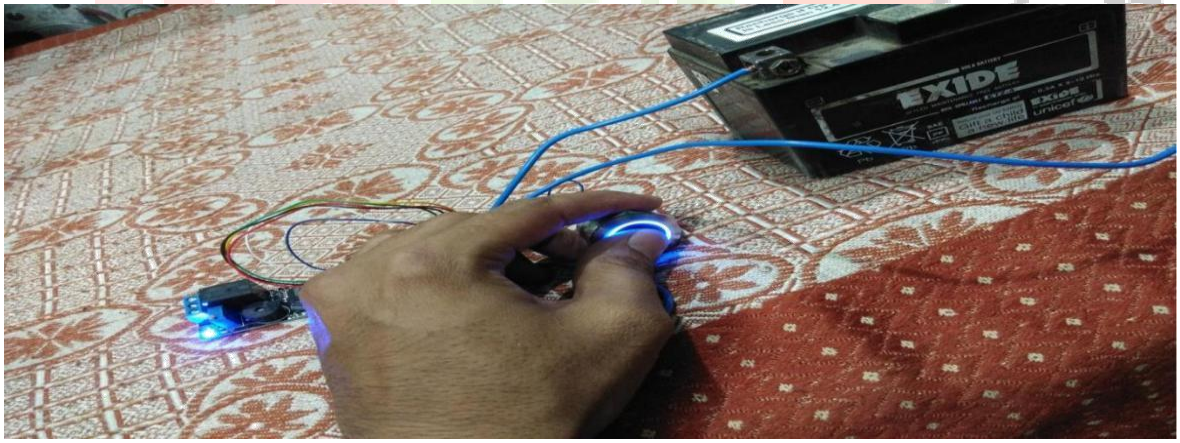


Figure 5.3: Match data

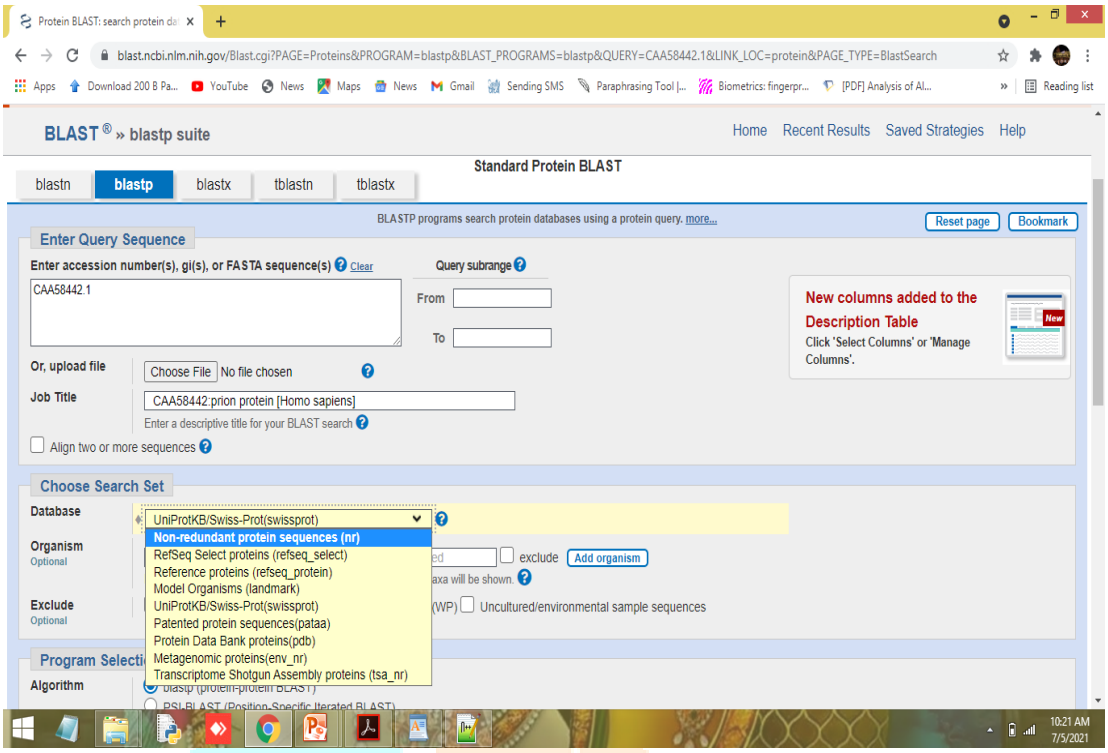


Figure 5.4: Example of Behind process start for match data

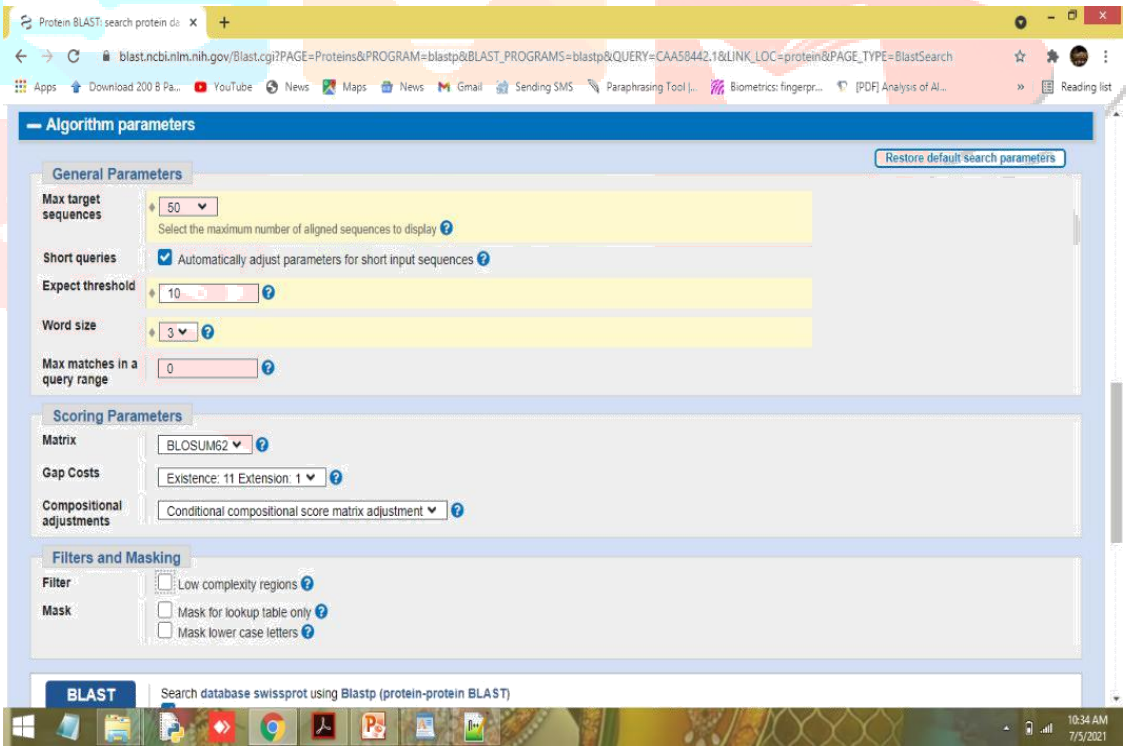


Figure 5.5: Next part

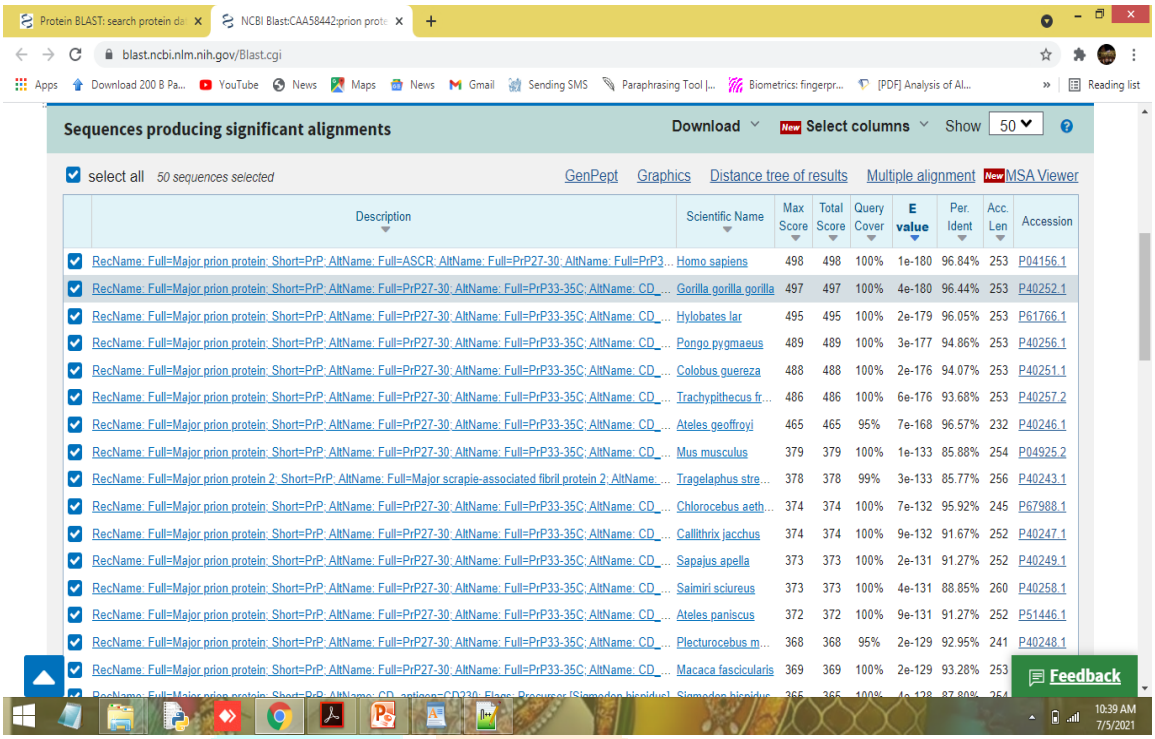


Figure 5.6: Complete 50 process and get highest score

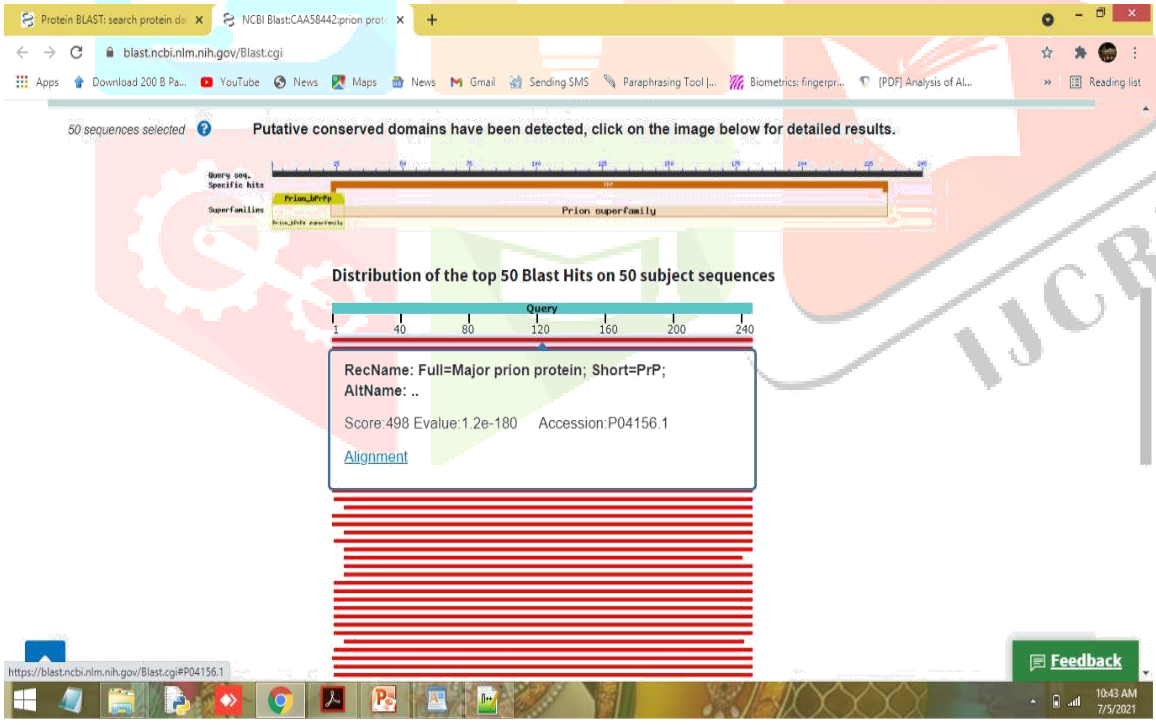


Figure 5.7: Graphical Represent for highest score value

5.3 Compare Result

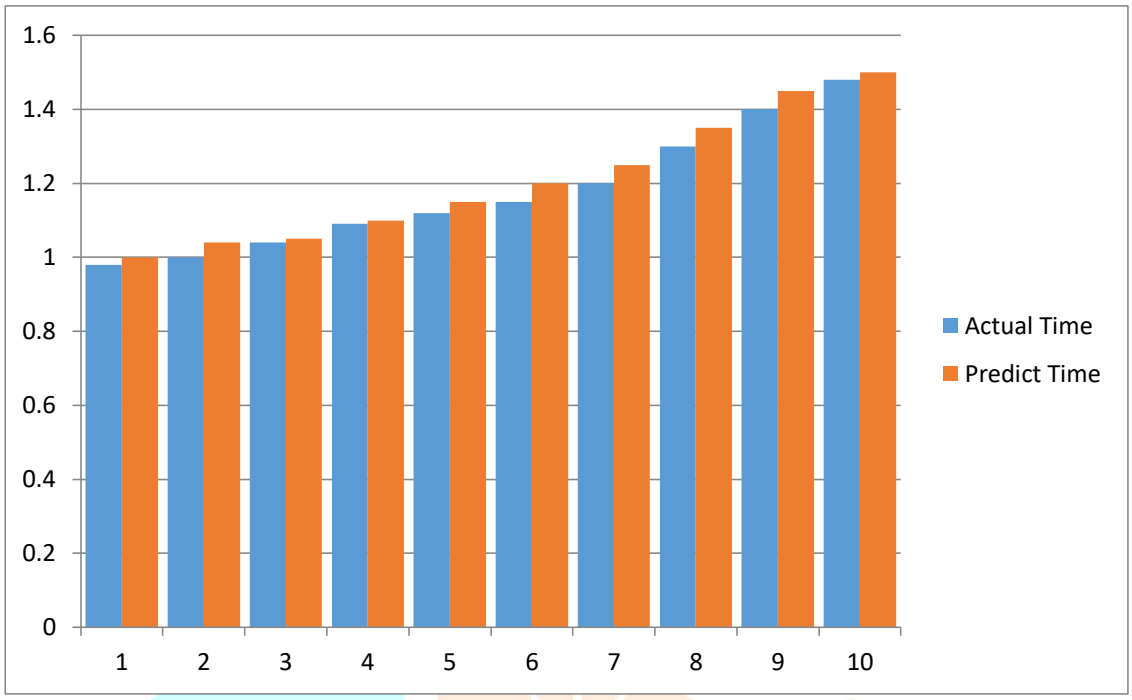


Figure 5.8: Analysis of Monitored Time value and Predicted Time value

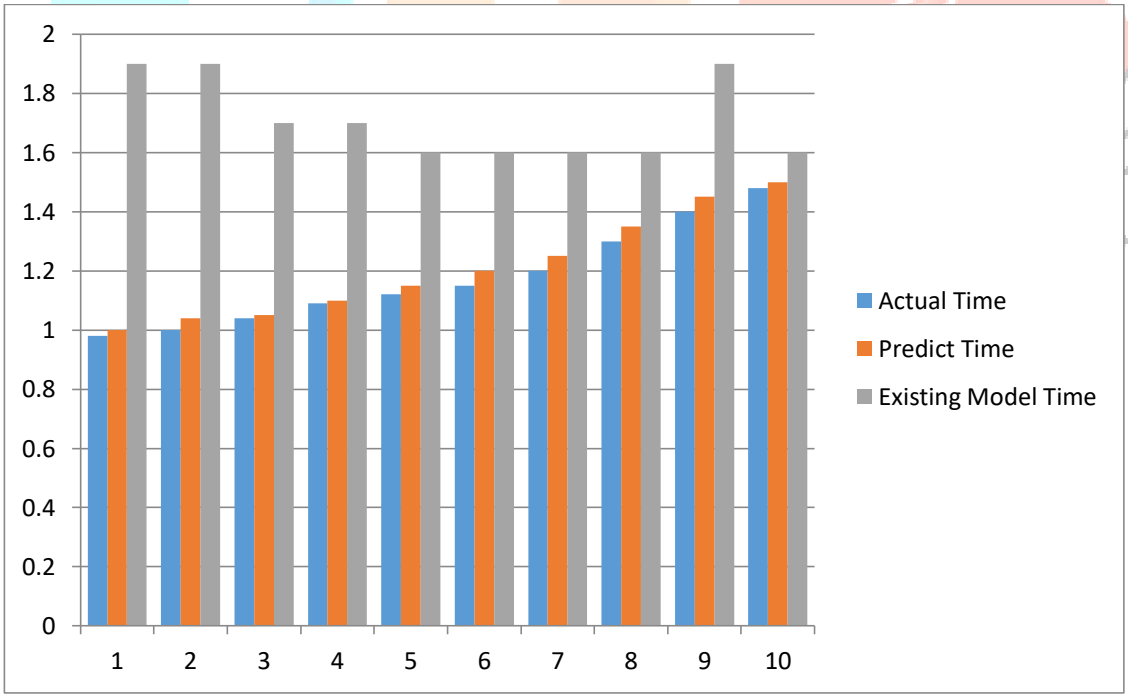


Figure 5.9: Comparison between Existing Value and Proposed Value

CHAPTER 6 : CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

The following is a summary of the performance of our suggested project:

- When compared to current systems, it delivers increased security and faster detection.
- It is simple to set up and for the user to access.
- In this module, there is less data loss and less time is consumed.
- This paper discusses bike security using low-cost scanners and other components.
- In this model, a high-performance r503 scanner is used with a growing k202 board. The result is better than the 2020 module (Arduino UNO + R 307).

6.2 Future Scope

Fingerprint detection can be utilized in the future to improve the vehicle's engine starting system while also providing robust security. It may be found in banks, workplaces, and houses, among other places.

6.3 Advantages

- The bike cannot be started without a human interaction.
- A safe and secure environment
- Simple to use
- Quick and effective

REFERENCES

[1] Motorcycle Security System with Fingerprint Sensor using Arduino Uno Microcontroller by Fitria Hidayanti, Fitri Rahmah, Aryadharma Wiryawap[International Journal of Advanced Scienceand Tchnology Vol. 29, No.5,(2020),pp.4374 – 439].

[2] Vehicle Starting System using Fingerprint by Dr.V.Nandagopal, Dr.V.Maheswari, C.Kannan [International Journal of Pure and Applied Mathematics Volume 119 No. 18 2018, 1753-1760].

[3] A Finger Print Based Door Locking System by A. Aditiya Shankar [IJECS Vol. 4 Issue 3 March, 2015 ISSN: 2319-7242].

[4] A Prototype of A Fingerprint Based Ignition System In Vehicles by Omidiora E.O [European Journal of Scientific Research ISSN 1450 – 216X Vol.62 No.2 ,2011].

[5] Fingerprint Based Ignition System by Karthikeyan.a [International Journal of Computational Engineering Research / ISSN: 2250 – 3005].

[6] Fingerprint Based Bank Locker System Using Microcontroller by Pavithra. b.c.[IRF International Conference, 05th April-2014, Pondicherry, India, ISBN: 978-93-82702-71].

[7] Development of Microcontroller - Based Biometric Locker System with Short Message Service by Crystalynne D. Cortez [Lecture Notes on Software Engineering, Vol. 4, No. 2, May2016].

[8] An Identity-Authentication System using Fingerprints by Anil k. Jain, Ling Hong, Sharath Pankanti, Ruud Bolle [IEEE Vol.85 No.9 September1997].

[9] Bank Lockers Security System using Biometric and GSM Technology by Sagar S.Palsodkar [SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE) Volume 2 Issue 4 – April 2015].

[10] Biometrics Authentication Technique For Intrusion Detection Systems Using Fingerprint Recognition by Smita s. Mudholkaretal [International Journal of Computer Science,Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012].

[11] Fingerprint Identification in Biometric SecuritySystems by Lourde R Mary, Khosla Dushyant [International Journal of Computer and Electrical Engineering, vol. 2, no. 5, October2010].

[12] A Tutorial on Fingerprint Recognition by Davide Maltoni [Biometric Systems Laboratory - DEIS - University of Bologna via Sacchi 3, 47023, Cesena (FC) – Italy].

[13] MPSAGA: a matrix-based pair-wise sequence alignment algorithm for global alignment with position based sequence representation by Jyoti Lakhani, Ajay Khunteta, Anupama Choudhary and Dharmesh Harwani [Indian Academy of Sciences 2019].

[14] A benchmark study of sequence alignment methods for protein clustering by Yingying Wang, Hongyan Wu and Yunpeng Cai [29th International Conference on Genome Informatics Yunnan, China. 3-5 December 2018].

[15] Two Wheeler Vehicle Security System by Prashantkumar R. [International **J**ournal of Engineering Sciences & Emerging Technologies, Dec. 2013. ISSN: 2231 – 6604 Volume 6, 2013].

[16] Overview of research activities behind data submissions by Okubo K, Sugawara H, Gojobori T and Tateno Y [2006 DDBJ in preparation for Nucleic Acids Res. 34:6–9].