**Czech University of Life Sciences Prague**

**Faculty of Economics and Management**

**Department of Information Technologies**


**Bachelor Thesis**

# Safety standards while using Fingerprint and Face Recognition Bio-metric system

**Eyoel Mesfin Admassu**

© 2021 CULS Prague

# Table of Contents

# List of Tables



# List of Figures

**ABBREVATIONS**

FPBS – Fingerprint Bio-metric System

FBS – Facial Bio-metric System

FVC - Fingerprint Verification Competition

FpVTE - Fingerprint Vendor Technology Evaluation

FRVT - Face Recognition Vendor Test

# 1 Introduction

For a world that is highly dependent on Biometric security most people aren't aware how it works as well as how important its usage is in our day to day life .As Our world is approaching a globalization age we are becoming more integrated and moving to create a global database which will led to collection of private information that would have been difficult to find 20 years ago. From the phones to the private security systems that we install in our homes each device collects the information and stored in private mainframes that are protected by the biometric security system which became a default for most organization as a result this study will be comparing Effectiveness of Fingerprint Biometric system with face recognition Biometric system as they are the most commonly used . which will look at the private as well as government applications that the public is apart off.

In a world where Individuals are dependent on Identification it is often difficult for government and companies to identify the real identity of an individuals which makes it difficult for controlling fraudulent activities as well as securing the public safety. There are multiple options that a company or a government can follow to achieve a higher security but that will come at a cost as the more steps that an individual has to follow the less cooperative the individual will become as it might try to find a shorter path such as trying to acquire a false identity as well as finding a loophole in the system which can lead to less security .

There are three stages to security which are Individual card Identity (ID) which is quite common and cheap to implement. It is the least effective option as it can be easy to falsify. the second one is using codes such as passwords that can take it to another level of safety, but it is still exposed to leaks as well as dependent on the individual and its safety concerns. The last one and the most effective so far is the biometric which has higher safety as no two human beings have the same biometric even though it can be similar.

In order to advance technological research gathering information is very important and as we are gathering information we usually use biometric security to keep it safe but we tend to forget how vulnerable it is to hackers trying to get access to that information In a world where every key strokes can be recorded as well as monitor the exact screen image it's very easy to collect information .Technology doesn't only solve problems but it also creates one because of this advancements hackers have developed their own systems that gives them access to advanced phones such as iPhone. the word Information can describe from a small contact number to nation security documents which are all protected by using different stages of biometric security systems. We should be careful to define which type of systems are being implemented as there are multiple types. this companies face two types of threat internal and external.

The main cause of internal threat comes from individuals that are unaware how valuable the information they are holding on as most will believe it is useless. This type of problems can only be solved by having a specific rule that the individual must follow when addressing any clients. The external threats come from hackers or compotators and individuals that want to sell the companies details for the highest bidder which will leave the company exposed.

# Czech University of Life Sciences Prague

# Faculty of Economics and Management

# BACHELOR THESIS TOPIC

| | |
|---|---|
| Thesis title: | **Safety standards while using Fingerprint and Face Recognition Bio-metric system.** |
| Objectives of thesis: | The objective of this thesis is to compare the advantages and disadvantages of using the Fingerprint Biometric system and face recognition Biometric system.<br>The partial goals of this thesis will be<br>- To clarify each of these systems and how their security level affects different companies that use them.<br>- To see to what extent it can protect the general public as most governments incorporate it in their system |
| Methodology: | The methodology that will be best in implementing objective is highly dependent on data that is utilized by the private and the public companies that have been working with the systems. After going through multiple options I found the best method to be Multiple Criteria Analysis which is the most logical option as this objective involves multiple scenarios and this analysis option gives multiple tools that can be used to analyze a variety of economic, social and safety concerns While helping me specify in each step the objects and its corresponding attributes. It will not be only dependent on safety, but it will also involve policies and monetary gains. I will also be using weighting and ranking so that the analysis would not be better against one criterion but worse against another one. Another option would be to compare both safety history while holding external variables constant. |
| The proposed extent of the thesis: | 50 |
| Keywords: | Face recognition, Biometric system, Security, Reliability, Fingerprint |

Recommended information sources:

1. Accenture. (2012). Biometrics and privacy: A positive match. Retrieved December 18, 2013, from www.accenture.com/accenturetechlabs
2. A. H. Mir, S. R. (2011, December). Biometric Verification: A Literature Survey. International Journal of Computing and ICT Research, 5(2), 67-80. Retrieved September 12, 2012
3. Alyea, J. L. (2008.). Picking the Best Biometric for Your Applications. National Biometric Test Center Collected Works, IADIS International Conference, (pp. 1, 269-275). Retrieved December 10, 2013

Expected date of thesis defense: 2020/21 SS - FEM

Electronically approved: 20. 7. 2020
**Ing. Jiří Vaněk, Ph.D.**
Head of department

Declaration

I declare that I have worked on my bachelor thesis titled " **Safety standards while using Fingerprint and Face Recognition Bio-metric system.** " by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on 20/09/2020 _____

# Acknowledgement

I would like to thank Ing. Tomáš Vokoun, my family and friends for their unwavering support during my studies as well as my work on this thesis.

# Safety standards while using Fingerprint and Face Recognition Bio-metric system.


## Abstract

This thesis compares the main types of biometric systems that are in use today they are Fingerprint and Facial recognition. As the world is becoming aware of security vulnerability of most systems biometrics has become the go-to solution for these problems as a result most of the system that we use in our day to day is somewhat related to biometrics from applying for ID's at government offices , going to work and entering the building , catching a flight or even to gain access to mobile phones and laptops which are all being secured using biometrics (Fingerprint and Facial recognition) systems. With the objective of clarifying for the users what these systems are, their security level and how they protect the public this thesis was able to find a clear result. The theoretical part explains what these biometric systems are and how they work with detail explanation on the process while the practical part used two Suprema HQ inc. products and compared them to each other by using standard factors .The process was concluded with Multiple criteria analysis of the results. Suprema HQ inc. was chosen as it is used by more than a billion people and the two products FaceStation 2 and BioStation 2 were used because of their availability in the Ethiopian market. This thesis has answered the question "which biometric system has a better safety standard for the public" under the specified conditions.


**Keywords:** Face recognition, Biometric system, Security, Reliability, Fingerprint biometric, Safety

# Bezpečnostní normy při používání biometrického systému rozpoznávání otisků prstů a obličeje.

## Abstrakt

Tato práce porovnává hlavní typy biometrických systémů, které se dnes používají, jsou rozpoznávání otisků prstů a obličeje.Vzhledem k tomu, že si svět začíná uvědomovat bezpečnostní zranitelnost většiny systémů, biometrie se stala řešením těchto problémů v důsledku toho, že většina systému, který používáme v našem každodenním dni, je poněkud spojena s biometrií z žádosti o průkaz totožnosti na vládních úřadech , práce a vstup do budovy , zachycení letu nebo dokonce získání přístupu k mobilním telefonům a notebookům, které jsou všechny zabezpečeny pomocí biometrických systémů (otisky prstů a rozpoznávání obličeje).S cílem vyjasnit uživatelům, co jsou tyto systémy, jejich úroveň bezpečnosti a jak chrání veřejnost, byla tato práce schopna najít jasný výsledek.Teoretická část vysvětluje, co jsou tyto biometrické systémy a jak pracují s podrobným vysvětlením procesu, zatímco praktická část používala dvě velitelství Suprema a.s.výrobky a porovnávat je navzájem pomocí standardních faktorů . Proces byl ukončen analýzou výsledků s více kritérii.Suprema HQ inc. byla vybrána, protože ji používá více než miliarda lidí a dva produkty FaceStation 2 a BioStation 2 byly použity kvůli jejich dostupnosti na etiopském trhu.Tato práce odpověděla na otázku" který biometrický systém má za stanovených podmínek lepší bezpečnostní standard pro veřejnost".

**Klíčová slova**: Rozpoznávání obličeje, Biometrický systém, Zabezpečení, Spolehlivost, Biometrické otisky prstů, Bezpečnost

# 3 Literature Review

## 3.1 The Theory behind Biometric

Biometric can be defined as a systemic method of identifying an individual's identity of a person by using their physiological or behavioral characters.

Biometric is a preferred form of authentication as it provides security as well as assurance. It requires no previous experience for using the authentication it is all non-transferable which will make it impossible to copy and implement in a controlled environment as it is unique for everyone. It requires moments to put a user in a specific system. It can be used for attendance and is able to handles more people as the system is implemented in different sections of a company another best part of biometric is its inability to be forgotten or lost as it is part of everyone.

While explaining the best part we should not be able to forget its weaknesses which will make users think twice. Even though it is the most secure option on the market it can still have inaccuracy such as false positives and may have bias which have to be reviewed. Majority of the time biometric is used for security which brings its own privacy concerns such as tracking the data that can lead to government surveillance of the user as well as data breaches that occur frequently in this day and age which can leave a user in a bad situation . Unlike any other security system, a biometric ID can't be reset and once it is stolen which makes it unusual. It can also be very expensive to install the system in the whole company so companies should do their research before trying to implement it.

## 3.2 Types of Biometrics Identifiers

#### Biometric Identifiers

There are also two types of Biometric identifiers (1):

1, Behavioral

2, psychological (Physical)

**Behavioral Biometric identifier**

Is a type of identifier that verifies users following patterns in their behavior. This type of authentication uses human behavior as it is regularly repeated. Interactions that the user has is authenticated in real time using regular day to day technology such as mobile phones. The movements of every individuals differ such as body movement, voice and walking patterns could be a good example once these patterns start changing the person won't be authenticated unless the user changes to other method of authentication.

**Psychological Biometric identifier**

As the name indicates it involves analyzing physical characteristics which are different for everyone.

Example of physical identifiers can be

- Fingerprints
- Voice
- Facial Recognition
- Signature
- Voice
- DNA
- Image

When it comes to Behavioral identifiers this are the most common patterns

- Typing patterns
- Engagement patterns
- Navigation patters
- Physical movements

# 3.3 Authentication in Biometrics

Biometric authentication techniques are system based highly dependent on digital computer. It is sometimes referred to as "Anthropometric authentication".

The history of Biometric authentication began around 1870s and the system that we use for measurement was set up by Alphonse Bertillon. Sir Francis Galton, Henry Faulds and William Herschel suggested the idea of sing Quantitative identification using fingerprint as well as facial measurements.

Alphonse Bertillon was able to develop and measure foot length, arm and the skull diameter which was very useful considering the usage in prison systems in North America in

1920s. Automatic human identification was implemented following the new development of digital signal processing in 1960s. (2)
It was in the same year that fingerprint recognition begun to be explored making it the first of its kind. Its potential was further recognized for implementation in high security controls in financial transaction as well as personal locks. Hand geometry, face and Iris recognition were developed 1970s and 1990s respectively.

The authentication in biometric can be processed in different dimensions because of the type of characteristics it has as well as requirements that are being implemented.
A single-entry one-dimensional signal such as voice recognition
Simultaneous entry in one-dimensional signals example can be handwriting
For single entry but two-dimensional image we can take fingerprint as a good example which requires the use of a single finger.

Multiple entry 2 dimensional measures we can take hunt geometry again as a careful field both the criteria's
A time dependent 2-dimensional image these are the types that are used for face and iris recognition.
The most common one is the 3-dimensional image as most people know is used for security systems in different parts of the world nowadays.

There are multiple characteristics of a biometric and the most common one's could be classified into 5 these are (3) :

1, **Acceptability**: when we define Accessibility, it is the people's acceptance or volunteerism it can be measured by pulling a device user

2, **Accessibility**: it is when it comes to TT to provide the option to multiple people in specific area for example at office can be qualified by throughput rate individuals that can be processed in the unit I.

3, **Availability**: It should be available to old people that need to use the system ideally it should be accessible to many people example could be an airport where there are at least multiple options to get authenticated. it can be measured by failure to enroll rate

4, **Robustness:** when we say robustness, we mean system should maintain a standard of strength and consistency can be measured by false not much weight which mostly referred to as type 1 error.

5, **Distinctiveness**: it should clearly distinguish one from another. Can be measured by false match rate and this is referred to as type 2 error.

# 3.3.1 Biometric Authentication Methods

1. **Voice Recognition**: As everyone has their own unique vocal notes as well as characteristics it's easier for a machine to identify a specific voiceprint of different people. It is usually applied in call centers.
2. **Engagement Pattern**: This are the pattern a person follows while accessing a specific system .it can identify devices that is being used and how frequently the user accesses this system. These types of pattern help distinguish humans from bots.
3. **Keystrokes Dynamics**: Every keystroke can be detected, and everyone has their own typing pattern when they use a keyboard. Different factors affect keystroke detection these can be pressure being used, speed, interval between keystrokes and many other helps identify users especially while using chatbots.
4. **Navigation Patterns**: These are the pattern a person follows while using mouse as well as finger movement on pads, it is sometimes used for authentication

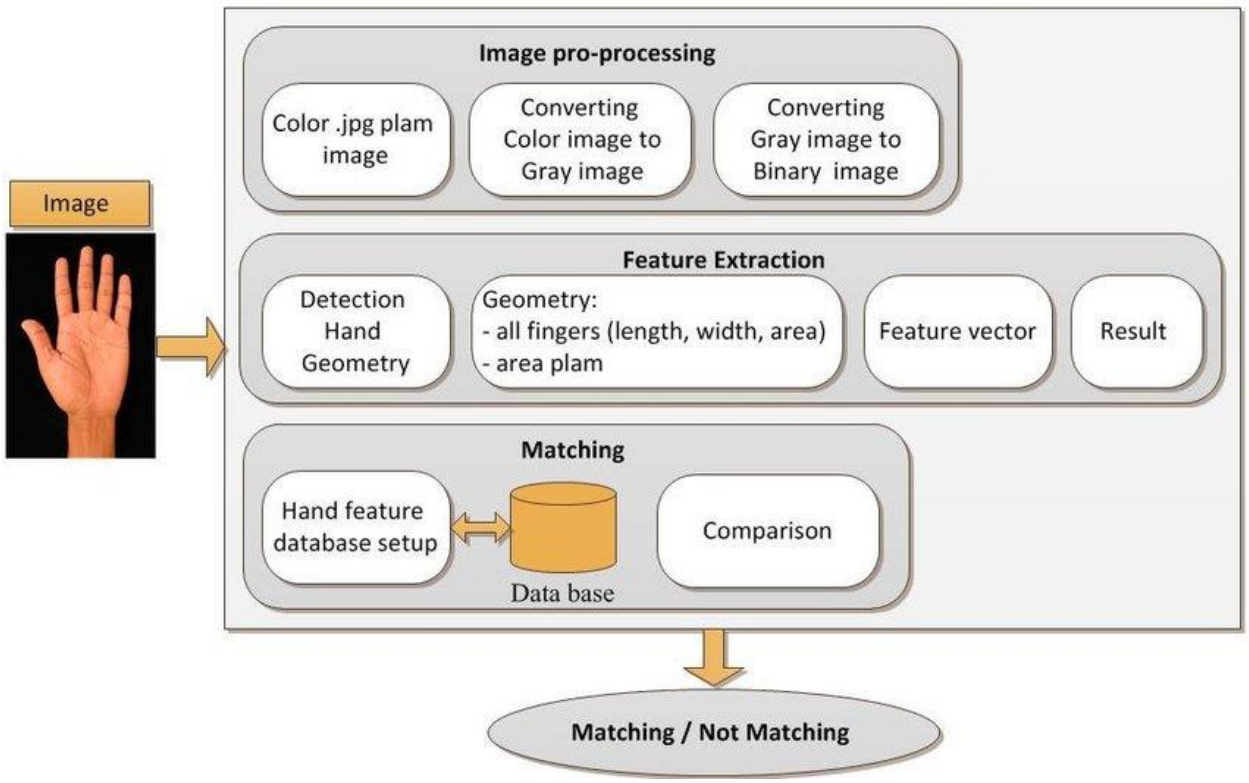



*Figure 1 Multimodal biometric architecture, (Source: https://www.researchgate.net/profile/Shihab-Shawkat/publication/335240929/figure/fig5/AS:793609364328448@1566222625091/The-proposed-architecture-of-multimodal-biometric-Hand-biometric-verification-systems.jp)*

# 3.3.2 Verification & Identification system in Biometric

Biometric verification refers to computerized verification based on some precise biometric facets derived from his/her physiological or behavioral characteristics. A biometric verification system has greater functionality to distinguish between a permitted individual and an imposter than the ordinary structures that uses a card or a password. (4)

In biometrics, a character could be diagnosed primarily based on who that person is as an alternative than what that person has (ID card) or what that person is aware of (password). A biometrics gadget is an awareness system that requires acquiring biometric records from an individual, extracting characteristic units as well as evaluating it with the template set in the database. Depending upon the software in use, we can identify the identity of an individual by two ways: verification and identification. (5)

In the former, a person is recognized by submitting a claim, which will be either approved or rejected depending on the validity. In the latter, a person is recognized by using a man or woman claiming to be as the person identified.

Verification authenticates a person by means of evaluating one specific biometric stored in the database, while identification involves checking and comparing to all the biometrics data that has been saved. Verification is sometimes referred to as one-by-one identification process. Verification is, of course, much faster than identification.

Biometric structures can be used in two modes (6) :

Verification (one to one): is used to know whether a person is who that person claims to be. In the verification mode, the device validates the person's identification by comparing the captured biometric with the saved data in the database.

Identification (one to n): identifying who the individual is. the gadget will identify the individual by going through all customers in the database to find a match.

The way biometric system works involves acquiring biometric information from an individual, then extracting characteristic set from the data that has been collected which is followed by comparing the characteristic set with the template in the database.

# 3.4 Design of Biometric

As the world is becoming more dependent on technology security is becoming very important part of design especially in biometric as it involves collecting sensitive information. There is a need to make sure that curtain standards of common understanding is being fulfilled such as the privacy protection which are set up to protect the integrity of the information that is being collected , stored and processed by the system . It must be implemented in the starting phase as it has to be in the core values as there will be privacy concerns that needs to be addressed it will also help to avoid future loses by the company as it will be curbed before it brings long lasting consequences .

With that being stated there are security requirements that a biometric security design must include these are availability, authenticity, integrity, and non-repudiation which are important and needs to be considered as a security target as it will involve safety. (7)

**Availability:** there needs to be an understanding when it comes to access as there are resource which can be considered as an entity but if all members of the set can access the resource it will have high reachability. An attacker might prevent the user from accessing the system and prohibit the use of authenticated applications and services. This type of prevention (Denial-of-Service (DoS)) are caused by the availability.

**Authenticity**: There are two main ways of discovering the authenticity of a biometric system this are the entity authenticity and data origin authenticity.

Entity authenticity are part of the overall process that checks the authenticity of each entity in the process. It is used to identify an individual as originators as well as sensors and their roles. While Data origin helps to ensure the authenticity of our data. the information that was received must come from original sensors.

**Integrity**: It refers to all resources such as hardware as well as software components that are in the process. Integrity of system refers to a state of being unaltered or manipulated. The system should not be modified as it will be compromised. There are multiple levels to data integrity which are High, middle, and low. Even though there are three levels for biometrics the level should always be High as to avoid any change to the system while it's in process and in storage.

**Non-repudiation**: Each entity that is involved in the process needs to have a binding agreement it also means having accountability for the information that the person might be exposed to in the line of work. senders and receivers of these sensitive information will be liable if a leakage occurs, there won't be an option to deny. It can also refer to making sure that there is legal repercussion if the user doesn't fulfil the obligation in the agreement.

When it comes to privacy and confidentiality regarding the user action there needs to be further security actions such as: unlikable, pseudonym, anonym and unobservable. Anonymity Is the action taken to make information indistinguishable or make it unidentifiable in a specific set. It helps make the origin of a set information in a communication line difficult to determine.

There are multiple levels to anonymity which are Absolute privacy, beyond suspicion, probable exposed, possible innocence, exposed, provably exposed this helps to identify the different safety levels. (8)

The process of biometric authentication starts by Data collection (Sensors) which will be measured electronically which will also be converted by analog-digital conversation then the signal will be processed according to the type of sensor used. Its concluded by comparing the data that are already collected to the information that is stored.

The information that is already stored should be integer (not manipulated) and authentic, each entity should be authentic and must ensure data authenticity as well as data integrity.

There are two main goals:

(a) The first and most important goal is making sure that the software and hardware components of the process comes from genuine sources and confirm that the information that is being received comes from a human rather than AI

(b) The second main goal is to cross check the collected data and ensure that data integrity, data authenticity and entity authenticity are all fulfilled.

# 3.4.1 Architecture of Biometric Security system

There are different types of biometrics systems which are based on different use and characteristics. They have two main phases (9) :

1. **Enrollment phase:**
   This is the first step where the data is received from the person. Even though the person might be required to try multiple times it is a one-time process as measurement needs to be done precisely.
2. **Recognition phase:**
   This phase is the follow up from the first step in which a recognition phase helps determine the data's accuracy as well as determine if its authentic.

Architecture of biometric system has six components (9)

**1.** Sensor

**2.** Pre-processing

**3.** Feature extractor

**4.** Template generator

**5.** Matcher

**6.** Application device

The components are stated below:

1. **Sensor:**
   It is the interface that is used to collect the data from the person. it is also connection between the system and the human, the usual sensors are for-image collection, but it can also depend on the type of biometric system in use.

2. **Pre-processing:**
   It's the next step which enhances the data input and filters artifacts such as background noise.

3. **Feature extractor:**
   This is the most important step as it will be used to identify the features to compare them to our database later in next stages.

4. **Template generator:**
   The extracted features are used for authentication as there will be a need to generate template with a unique tract, these templates are created using the characteristics collected previously which will be compared later with our database.

5. **Matcher:**
   This is the stage where the new template is compared to the previously collected templates using different algorithms like Hamming distance and then generated.

6. **Application device:**
   This device processes and applies the result from the components above.

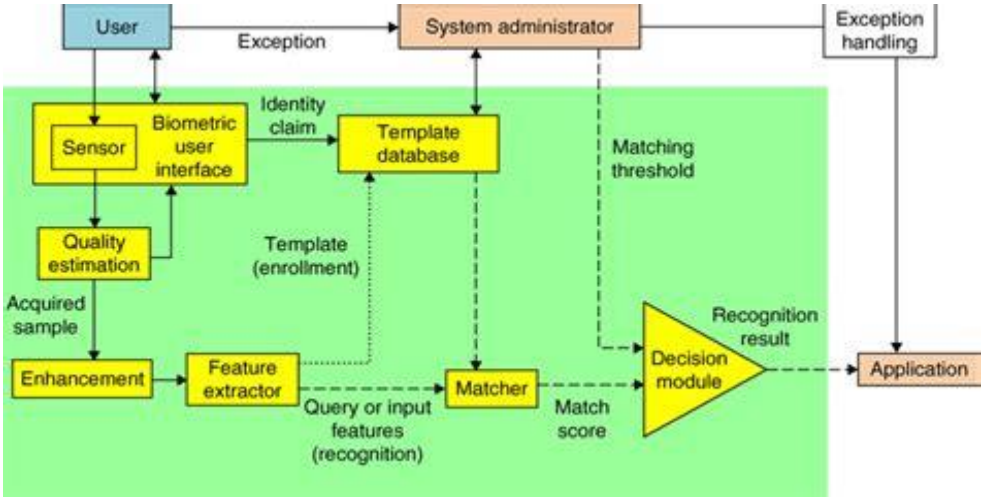



*Figure 2 Architecture of biometric (Source: https://link.springer.com/referenceworkentry/10.1007%2F978-0-387-73003-5_183)*

# 3.5 Reliability of biometrics

One of the core reasons why biometrics is preferred currently is because of its high level of reliability as it is required for such systems.

**Reliability** can be defined as " ability of a functional unit to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided" (10)

Every generic system is composed of three components, which are:

1, Availability

2, Maintainability

3 Reliability

Reliability is described as a system functionality without failure which can be represented in two main ways

1) MTFB - Mean time between failure
2) MTTF – Mean time to failure

Availability in a system can be defined as the acceptability of the system when there is a need to use it. Maintainability Can be described as the ability of having quick response in case of system failure or prevention of future failure if it is already operational.

The main factors of Maintainability are:

• Mean time to repair (MTTR)

• Maximum time to repair (MaTTR)

"Failure can be defined as the condition in which a system or part of it presents an abnormal behavior" (11).

The Actual approaches will be briefly described below:

Biometric system evaluation can be performed by measuring the performance of biometric system as well as comparing them to the reference values according to standard.

These procedure for evaluation of biometric uses different methods such as:

The different tests of reliability for analyzing frequency of errors and the ability to function after the error occurs.

Biometrics is usually used for safety as well as monitoring other systems so there is a need for frequent checks for the security levels and vulnerabilities.

It is checked by:

- Degree of satisfaction of the requirements (safety)

- Resistance to possible attacks from outsiders

There might be a need to do vulnerability assessment of biometric which usually involves penetration testing.

The process begins by collecting potential threats which is followed by looking at the probability of system exploitation which will be assessed thoroughly after which there will be a need to create an attack scenario which involves penetration testing. The steps above help close any vulnerable part of the system.

There should be a compliance with regulations that the information collected is used as well as disposed of properly. The operational functions and the compliance documents must be checked to follow the goals of compliance.

Reliable evaluation methodology should involve the environment and technology as well as consider technical system reliability (software and hardware components) and the parameters for statistics. (12)

- False Non-Match Rate (FNMR)

- False Rate Match (FMR)

- Failure to Acquire (FTA)

- Failure to Enroll (FTE)

Components of biometric system environment:

• Physical environmental factors/attributes

• Atmospheric environmental factors/attributes

When using biometric we should put the social, artificial as well as natural environment under consideration user's aspects can be composed of:

• User characteristics

• User personal influential factors

It can be described as the size of the impact of the system on the immediate user when initiating the process through collection of biometric characteristics. In addition, physical, behavioral as well as personal factors affect the user while accessing the system.

# 3.6 Factors Under Consideration (13)

**1, False Match Rate (FMAR)**

It is the rate of accepting invalid matches. The system shows a successful match even though its false, it is very sensitive since it is there to prevent access to certain individuals.

**2, False Non-Match Rate (FNMR):**

It is the rate of rejecting valid matches stating failure even if the user was in the database.

**3, Relative Operating Characteristic (ROC):**

We can reduce the effects of both FRR and FAR by manipulating the threshold which is commonly referred to as parameters. This is done by graphing both FRR and FAR values and altering the variables.

**4, Detection Error Tradeoff (DET)**

We obtain DET by graphically plotting FRR and FAR, it will have an inverse relation with error rates as it becomes more linear.

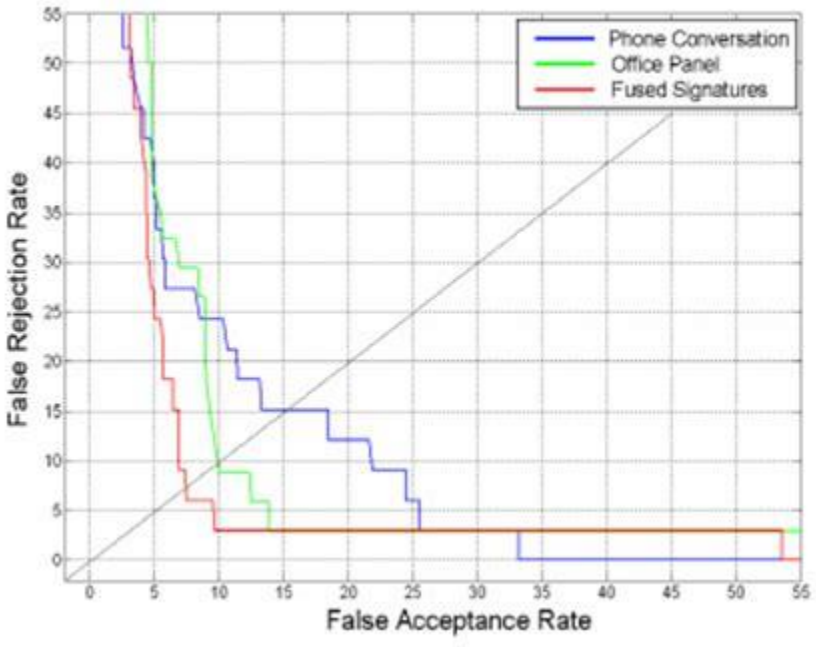



*Table 1 Detection Error Tradeoff (Source https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Ftse1.mm.bing.net%2Fth%3Fid%3DOIP.iCY3lTCHscSZW10dc5fMTAHaFa%26pid%3DApi&f=1)*

**Equal Error Rate (EER):**

This is the rate that occurs when FAR and FRR are equal it is usually used when there is a need for comparison. Using ROC there could be a clear method of identifying the accuracy. EER has an inverse relation with accuracy which means as the EER increases the accuracy decreases.

**Failure to Enroll Rate (FTE or FER):**

This happens when the sensors are not able to input the collected information to the system, it usually occurs when the information is invalidated because of lack of quality.

**Failure to Capture Rate (FTC)**: it is the rate of failure to acknowledge a valid input (Characteristics) from the sensor.

**Template capacity**: as the name indicates is the capacity (maximum) information that can be stored from the input of the sensor

# 3.7 Fingerprint Biometric security (FPBS)

"Fingerprint recognition is the process of comparing questioned and known friction skin ridge impressions from fingers or palms or even toes to determine if the impressions are from the same finger or palm." (14)

The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike, even two impressions recorded immediately after each other.

Fingerprint identification is the process of identifying and determining the origin of two friction ridge it is sometimes referred to as individualization. "A known print is the intentional recording of the friction ridges, usually with black printer's ink rolled across a contrasting white background, typically a white card. Friction ridges can also be recorded digitally using a technique called Live-**Scan**." (15)

. When there is a contact between friction ridges and a surface that is receptive to a print, material on the ridges, such as perspiration, oil, grease, ink, etc. can be transferred to the item. A Fingerprint Patterns is a process of analyzing a fingerprint to compare it against the features of a pattern collected. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. (16) The human skin has different structure as well as properties and knowing that is key to deploy a successful imaging technology.

The three basic patterns of fingerprint ridges are the **arch, loop**, and **whorl.** (17) · An **arch** is a created when there is a movement of finger pattern from both sides of the loop which forms an arch.

The **loop** is formed when a finger pattern looks like it is inserted from one side and exits from the same side forming a circle pattern. In the **whorl** pattern, is a type of pattern where a circular ridge is formed in the central part of the persons finger, this trait is sometimes shared with family members.

## 3.7.1 Preprocessing and Feature Extraction

"A fingerprint is composed of a pattern of interleaved ridges and valleys." (18) It has a flow which looks like its interloped but when observed closely its easier to pick up a parallel pattern.

**singularities** can be classified into three types: loop, delta, and whorl. (19)

**a)** the whorl singularity can be defined as two opposing loops. A minutia is formed because of the pattern that is created by the valleys and ridges. At the local level, the ridges and valleys pattern can exhibit a particular shape called minutia. There are two types of minutiae are considered as ridge endings and ridge bifurcation. Singularities at the global level are commonly used for fingerprint classification, which simplifies search and retrieval across a large database of fingerprint images.

**b)** The loop types of incorporates the core and delta singular points.

**c)** delta points are a result of "two landmarks of a fingerprint"

The gray scale representation of a fingerprint image is known to be unstable for fingerprint recognition most of the fingerprint matching algorithms use features which are extracted from the gray scale image.

If we expect that image, ridges and valley to flow smoothly in ideal conditions, there are factors that affect the quality of a fingerprint image: wetness or dryness of the skin, noise of the sensor, pressure on sensor, etc**.** (19)

Fingerprint segmentation consists of the separation of the fingerprint area (foreground) from the background (20) **.** This is useful to avoid subsequent extraction of fingerprint features in the background, which is too noisy. These techniques exploit the existence of an oriented periodical pattern in the foreground and a no oriented isotropic pattern in the background as mentioned above, the pattern of ridges and valleys exhibits several shapes called singularities. For the detection of singularities, most of the existing algorithms rely on the ridge orientation information. (18) .

# Fingerprint identification

Fingerprint identification uses two main assumptions which are called Invariance and **Singularity.**

**Invariance**: means having a characteristic that is not changing as time passes.

**Singularity**: means the fingerprint is unique and no two persons have the same pattern of fingerprint. (21)

**A. Image Capture or Image Acquisition stage**

This is the stage where the image will be collected, the image acquisition can take place in two main methods: online and offline. the size will be 260 by 300 pixels, and the offline fingerprint option uses ink and paper while the one that is online uses scans of the paper which produces an image.

**B. Image Pre-processing Stage**

On this stage the unwanted data (noise, reflection) is removed while enhancing the clarity of the ridge structure.
There are many steps for doing this process Image Segmentation, Binarization, Elimination of noise, smoothing and thinning**.** A detailed pre-processing is mentioned to remove false minutiae. Algorithms are used for features extractions. A fingerprint feature extraction program is to locate, measure and encode ridge endings and bifurcations in the fingerprint. (21)

C. **Matching stage**: -

On this stage the image that has been acquired will be compared to the previously collected features (templates) after which It will calculates the degree of similarity between the two.
Matching can be done in three methods: hierarchical approach, classification approach and Coding approaches (22). Using hierarchy comes at a cost as the accuracy will be affected even if there is high matching speed. Classification approaches assign a class to each biometric in a database by using coding approaches which uses one matching function to search entire databases. They are combining minutiae matching and image-based fingerprints verification methods

# 3.7.2 Fingerprint Sensing

We can classify scanners in to two main categories:

• **Multi-finger**: when using more than one finger at the same time which usually include the first four and are measured at the same time. there are three shots which will be enough to collect the 10 fingers. The segmentation of a single image containing four fingerprints into four separate single fingerprints is known as **slap segmentation** (23)**.**

• **Single finger**: only one finger at a time can be acquired; this type of scanner is most widely used in commercial and personal applications due to its small size, low cost, and simplicity of use. In the market there is a need for cheap and compact products to be used as a simple low-cost portable device.

# Live-Scan Fingerprint Sensing

This is one of the most important part of sensors which along many other forms the fingerprint image. Sensors could come in many forms they are optical, solid-state, and ultrasound (24) **.**

• **Solid-state or silicon sensors**: These consist of an array of pixels, each pixel being a sensor itself. After placing the finger on the silicon, we use four different methods to convert the ridges into electrical signals. These are: piezoelectric, capacitive, thermal, electric field (23) .

• **Optical:** The finger touches a glass prism and the prism is illuminated with diffused light. The light can be reflected at the valleys while it will be absorbed back in the ridges. "The reflected light is focused onto a CCD or CMOS sensor. Optical fingerprint sensors provide good image quality and large sensing area." (25)

• **Ultrasound**: The process involves capturing the signals from the fingerprint that has already echoed back. these types of scanners can capture images under hard conditions, but the size is usually large, and price is high.

# Optical Sensing

**Frustrated Total Internal Reflection (FTIR)**: this is the oldest and most commonly used live-scan acquisition technique .As the finger touches the top side of a glass/plastic prism, as the ridges are in contact with the prism the valleys will remain at a distance (25). They aren't usually deceived by using pictures or photographs as they are 3D finger surfaces.

Despite all that their unusual size makes them unusable for the public unlike optical fibers.

**Direct reading**: a direct reading device uses a high-quality camera to directly focus on the fingertip (23)**.** . Touchless acquisition may be perceived to be more hygienic and may overcome some problems of touch-based acquisition such as the nonlinear distortion caused by pressing the finger as a result there is a need for surface to be cleaned frequently.

# 3.7.3 Fingerprint Matching

One of the most difficult part of fingerprint biometric is Matching fingerprint as there are usually huge variability while using the same finger. The main factors are (26)**)**:

• **Displacement**: when scanning a single finger might be placed on different areas of the sensor which results in finger displacement which is around 2 mm (40 px, 500 dpi).

• **Rotation**: there is usually a finger rotation of ±20° vertically even if it is mounted with a finger guide in commercial scanners.

• **Partial overlap**: This problem usually happens when there is a small sensor as it creates conditions for the finger to go outside the field of view.

• **Non-linear distortion**: it involves presenting a 3D shape of finger to a 2D sensor surface. Which will result in distortion on the same picture of the finger because of the occurrence of skin plasticity. a finger placement is correct when:

(i) The angle between the finger and the sensor becomes ninety degrees it will be ideal.
(ii) once the finger touches the sensor surface, the user does not apply traction or torsion, but the rest of the force will result in compression or stretching because of skin plasticity.

• **Pressure and skin condition**: the accuracy of the scan is highly dependent on the ridge which needs to be in a uniform contact with sensor surface.

• **Noise**: it usually comes from the residues left from previous fingerprint capture which originates from the fingerprint sensing system.

• **Feature extraction errors**: these errors are the results of feature extraction algorithms. An error can occur at any time during extraction. The method of introducing an aggressive enhancement algorithm results in inconsistent bias. A true minutia might not be detected if there is a low-quality image as it will produce spurious minutiae.

# Minutiae matching with pre-alignment

Embedding fingerprint alignment into the minutiae matching stage (as the methods presented in the previous section do), certainly leads to the design of robust algorithms, which are often able to operate with noisy and incomplete data (27) .

• **Absolute pre-alignment**: uses the position which will be the core point to translate (rotate) the fingerprint.

• **Relative pre-alignment**: the fingerprint retrieved will be compared with the once already collected and are stored in the templates. There will be a matching score with either a rejection or acceptance decision.

This variability is known as intraclass variability and is caused by several factors, including (28) :

a) displacement or rotation between different acquisitions

b) partial overlap

c) skin conditions (bruises, dirt, cut, etc.)

d) noise in the sensor

e) nonlinear distortion

# Solid-state sensors

In this type of sensors there is no need of optical as well as CMOS as the silicon can use array of pixels.

There are four technologies that is used for converting a fingerprint pattern in to electrical signals : thermal , capacitive , piezoelectric , electric field (23) .

• **Thermal**: they are maintained in high temperatures using an electric heating which will increase the temperature between the fingerprint and sensors. The temperature difference between fingerprint ridge and sensors will be produced by pyro-electric material which makes up the sensors.

• **Electric field**: This type of sensors requires the finger to be simultaneously in contact with both the sensor and the drive ring. Also referred to as RF imaging, the sensor consists of a drive ring that generates an RF (Radio Frequency) sinusoidal signal and a matrix of active antennas.

• **Piezoelectric**: These types of sensors work when an electrical signal is produced while mechanical stress is applied to them, it is made of dielectric material which encounter pressure from the finger, generates a small amount of electric current which are referred to as piezoelectric effect .the current that is generated is directly proportional to the pressure being applied by the finger .

# 3.8. Facial Biometric security (FBS)

Face recognition records the geometrical feature of an individual's face. Face recognition technique can be used for different purposes for our case it is implemented in airports, private companies as well as other government offices. This is a non-intrusive, cheap technology.

Face recognition is one of the most challenging biometric types for the researches around the world. Even though it has a lot of application it is very difficult to implement it as there is diversity in human face features.

Facial recognition is a biometric system which uses an individual's faces to identify the person or verify the person's identity. Facial recognition requires five steps to complete a process and check for a match.

A face recognition system has 3 modules (6) :

A) Image acquisition
B) Face Detection
C) Face Matching

## 3.8.1 Image acquisition

An image can be acquired in 3 main ways as the usual 2D photographs which everyone has at home, a 3D depth images and the last one is through a video.

Step1: **Acquiring image of the persons face**: which can be in two ways (29)

1) Digitally scan an existing photograph.

2) Acquire live image.

Step2: **Locating the image face from the image**: At this point a software is applied to locate the face in the image that was extracted.

Step3: **Analyzing the image that was collected** : it is measured by using is peaks and valleys; the middle part of the face usually known as the "golden triangle", the information collected are used for creating a face print.

Step4: **Comparing stage**: the face print which was created is used to compared to the other face prints already stored in the database.

Step5: **Matching stage**: This is the last stage where it will know if there is a possible match.

Facial recognition uses the distinctive features of the face which includes the upper outlines of the eye sockets, the areas surrounding the cheekbones, the sides of the mouth, and the location of the nose and eyes - to perform verification as well as identification.

Facial recognition technology shows results that closely matches to our search rather than a single match result.

The first step a software takes is to locate the face from the image that is provided. Then the facial characteristics are extracted. There are two main facial recognition techniques in use today: eigenfaces and facial metrics.

## A. Functions of Face Recognition (29)

**Facial pose estimation** measures the twist of the face by estimating the angle.

**Facial part detection**: identifying parts of the face for example the center of eyes, tip of nose, and corners of the jaws.

**Facial trait classification**: This is a type of classification that is based on age, appearance, gender, and other character.

**Face identification**: The process of identifying a person by matching them to a registered people.

## B. Statistical Face Recognition

This type of facial recognition is usually used in commercial applications. The first step is to find a facial pattern in the regular size. Human vision can find the face of a person even when the resolution of the image is 16x16 pixels. (6)

1) **Detection of face to be scanned**: The system will scan the whole image (top to bottom) to find a specific pattern.

2) **Facial pattern classification**: Facial patterns vary from person to person, and they also change according to the angle of the face and differences in lighting conditions or facial expressions. To balance the effect there is a necessity to formulate functions that allow discrimination between facial and non-facial images by applying statistical methods facial images.

## 3.8.2 Performance of Face Recognition

There were multiple steps taken to compare the precision(accuracy) of the different types of face recognition techniques from a large image database.

The first one being The Facial Recognition Technology (FERET) from 1993-1997 which was followed by Face Recognition Vendor Test (FRVT) 2002 that achieved 70% for the frontal pose under the normal light using a database that had 121589 images from 37437 subjects.

Another Face Recognition Vendor Test (FRVT) was performed in 2006 from the different scenarios the verification had 0.01 False Reject Rate (FRR) and 0.001 False Accept Rate (FAR) with high resolution. (6)

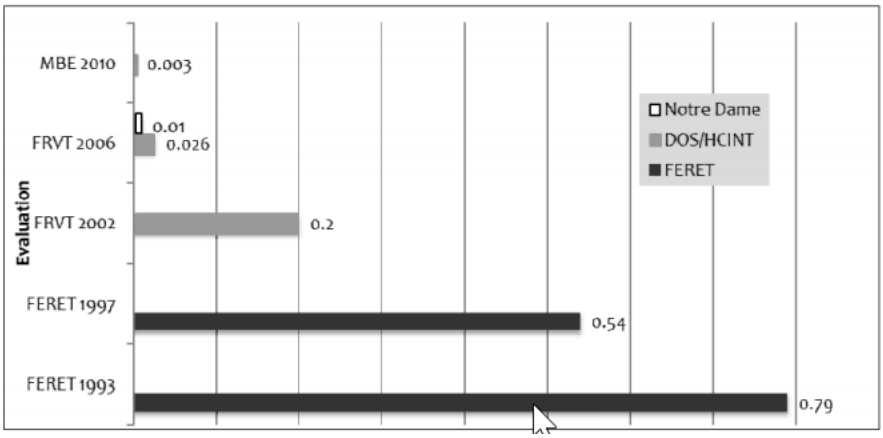



*Table 2 Face recognition accuracy (Source: (Anil K. Jain, 2011))*

## 3.8.3 Issues in Video-Based Face Recognition

### Image Resolution

At a distance the facial image is always at low resolution which will decrease the recognition strength as well as the performance for that reason it is advised to use high-definition camera which comes at a cost. The speed and the possible face detection will be decreased.

When using face recognition at a distance in most cases the face is out of focus which creates image blur which can be corrected to some extent using aperture lens. (30)

**Interlace** is a method of uncovering lines and rows of pixels from an image which will create a frame. Each field will contain the odd lines and the even lines of the image. This makes it difficult to find and recognize the face of the person. The solution for this problem is in the process of **de-interlacing** which has a side effect of lower resolution when the object is motion.

**Motion Blur** it occurs when the person or object is active, or the camera is shaking. Rapid exposures are used to correct the motion blur.

**Users' Heights**

Hight is one of the biggest problems when trying to use facial recognition system. It should be reflected in the designing process. There are two ways of acquiring the image that is by using a single large vision camera and using multiple cameras which have their own extraction methods (31)

**A, single large vision camera**

- will cover the user's height
- Fixed image aspect ratio 4:3 or 16:9
- Rotation of 90◦ for higher field of vision

**B, multiple cameras**

- the angles would at a different height
- the two main ways of processing the image is by merging the multi-images and using multi-images independently.
- If multi-images are used the visions of the cameras should be overlapped so that the face image is not cut into two images.

**Frontal Faces**

The best matching occurs when the face algorithm can find the frontal face. There should be a system that will lead the user to face the camera it should be handled in the design. The best way to attract the user's attention is by using different devices that will keep the attention of the user on the system so that frontal face image is collected. Use of a screen can be one of the ways by placing the camera below it the user will give all their attention without knowing that it exists. The user will sub-consciously watch the screen as it will have the same effect as a mirror. For better results the camera and the screen used should be kept close.

**High-Quality Images**

The quality of the image is dependent on two factors the clarity and exposure as it will need to meet some requirements. If the image is blur , it is the result of either loss of focus or the frequent movement of the person and sometimes the exposure is linked to background light .it can be captured with analog or digital camera that can have its own unique problems such as speed which affect the analog or have uneven edge because of locomotion when dealing with the digital one.

**Feature Extraction and Matching**

The extracted image is dependent on the system that is used as there could be multiple method used. The registered facial images are inserted in a model such as AFM which connects

multiple different facial points. The ICP (Inductively Coupled Plasma) technique is unable to match this approach as these facial points are connected to each other rather than to a common one.

It is therefore possible to use ICP error for measuring the surface matches. there will be an assumption that the surface will be connected densely with the use of one-to-one mapping between facial surfaces.

A 3D coordinates of facial points of densely connected faces (point cloud feature), can be considered the simplest feature that is possible to use. The difference between the different facial points on the different surfaces are important as the geometrical features are dependent on it. The facial points are variable as it ranges between 19 and 73. (32).

# 4 PRACTICAL PART

This part of the thesis will be concerned about comparing the previously discussed biometric systems which are Facial and Fingerprint Biometric system. It will be done using the multicriteria analysis and comparing them with the specified factors which will be useful for individuals, private companies as well as the public sectors.

## 4.1 Selecting Biometric security systems

Choosing the best biometric system is one of the core steps to protect a companies and individuals can take to keep their information secure with that being said there was a need to compare these two commonly used systems as there was not that much independent assessments that described and investigated the different structures of each system . I have chosen two different Access control systems that were applied in different private companies as well as private homes by iSense Technologies Addis Ababa, Ethiopia. These systems were BioStation 2 (BS2-OEPW) and the FaceStation 2 (FS2-D) from the company Suprema HQ inc. The BioStation 2 (BS2-OEPW) is a Fingerprint biometric security device while FaceStation 2 (FS2-D) is a Facial Recognition biometric device , these systems helped formulate the results that led to a clear conclusion.

### 4.1.1 Overview of the company

Suprema HQ inc. is one of the best companies in the world covering the biggest market share in the EMEA region it offers biometric solutions related to security. It also offers access control monitoring devices for attendance and time. The company has exposure to different markets from the US to Asia as well as sectors such as transportation, Industrial and government this exposure helps it to connect with more than a billion people in the world. The company was established in 2000 and is based in Seongnam, South Korea.

The company uses a unique platform called Biostar which was developed by the company. Its first release was BioStar 1 which was replaced later by the second version called BioStar 2.

Biostar 2 is the web-based platform that uses Java Runtime and Database which will be used in this thesis as both BioStation 2 (BS2-OEPW) and FaceStation 2 (FS2-D) function on this platform and surprisingly it can be used simultaneously as well .

## 4.1.2 BioStar2

In order to use the platform, there is a need to install and connect to the server as it is for private use the same for the database.

| | |
|---|---|
| Max. Device | 1,000 |
| Multi-Door Control | Supported |
| Auto Reconnection to Serve | Direct & Server mode |
| USB Enrollment Device | BioMini, BioMini Plus 2, DUALi DE-620 |
| Max. Fingerprint per User | 10 |
| Max. Access Group per User | 16 |
| Max. Card per User | 8 |
| Web Server: HTTP 80 / HTTPS 443(Default) | API Server: 27017 (Default) |
| Database: Maria DB:3312(mysqld.exe) (Default)<br>ORACLE: 1521 (BioStar2.4.1)<br>MSSQL: 1433<br>T&A: 3000(HTTP)/ 3002(HTTPS) | Cloud: URL: api.biosar2.com /cloud.biostar2.com<br>52000(default) (nginx.exe *32)<br>V1 8790(App), 8791(doc) |
| Device Port: 51211 (default) | Filesharing: 445 |
| Web server: Nginx 9000 | Biostar2 Server: 51212 (biostar-server.exe) |
| RS-485 Protocol | OSDP Supported |

*Table 3 BioStar2 platform specifications (Source: https://www.supremainc.com/en/platform/hybrid-security-platform-biostar-2.asp)*

After installing the program, you will be able to see the following on your screen where you will be asked to log in with your credentials which will be provided by the company and must be replaced as soon as possible:

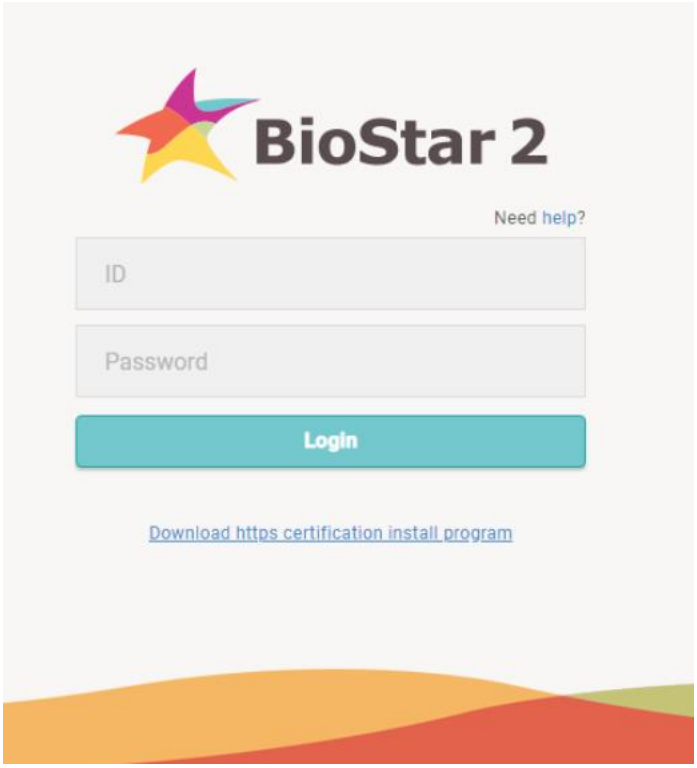



*Figure 3 Login page for BioStar2 (Source: own)*

The Dashboard will be visible from now own as the access is on the admin level. From here there will be multiple option to choose from accessing the registered users to changing the access control. This will be installed and configured by iSense Technology. Assembly of the devices will start from here as there is already a database (Maria DB:3312(mysqld.exe)) to connect too. There is an option to connect to MySQL server as well, but the process takes longer because it requires technical team to make sure the process goes smoothly.

This is where the device search starts as it was already assembled and is on site. On the Dashboard there will be a section called devices where server port and IP will be entered for each device (FaceStation2 and BioStation 2) then we can proceed to click on Apply.

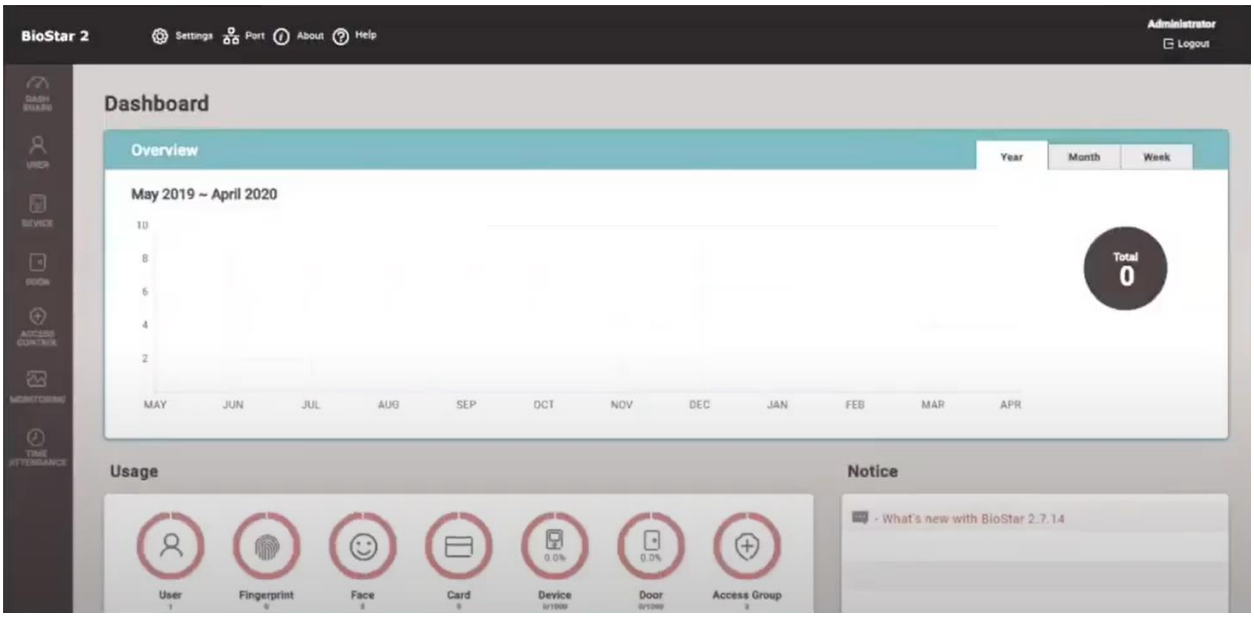



*Figure 4 BioStar2 Dashboard a single Admin user (Source: Suprema)*

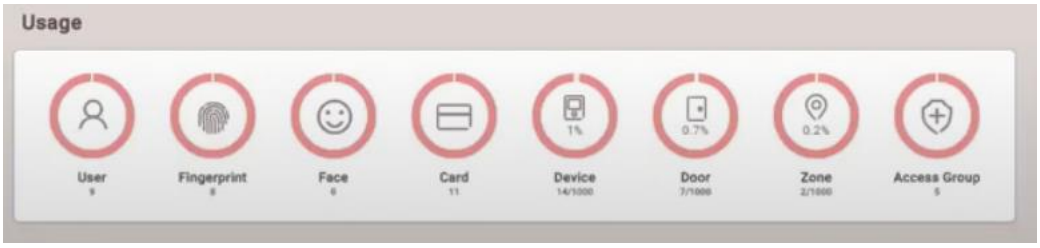



*Figure 5 BioStar 2 Usage section (Source: Suprema)*

### 4.1.3 Comparison Factors

The main factors for choosing biometric systems are stated below (6) these factors will be used to compare BioStation 2 and FaceStation 2 :

- Acceptability
- Performance
- Universality
- Uniqueness
- Permanence
- Measurability
- Circumvention

Note: It is worth to note that there are two extra factor (Aging and Cost) under consideration as it will have high effect on both systems.

# 4.2 Acceptability

The most important factor for selecting a biometric is acceptability as it will require consent from the users that's of course if it's not used by government and security apparatus.

According to (33) there will be a greater risk of privacy invasiveness when:

1. Users are not aware of the system's operation
2. If the user is offered option rather than making it mandatory
3. If the system is being applied to identify the user rather than verify
4. If there is a time bound rather than being fixed
5. When being used in private or public sector
6. when its applied in companies or government or for private use
7. private use of personal data rather than it being institutionalized
8. Personal storage of the user or general template database of biometric date
9. Private identifiable data storage rather than general data templates

For the case of BioStation 2 (BS2-OEPW) the users didn't have any objection as it was already in use by the government and immigration offices. The fingerprint was easily collected from the users except for some limited exception which was due to users having fingerprint loss and had to switch between multiple fingers. It was important to note that the users didn't have objection because of the small size of the company and the storage of the data which was in the same office rather than the usual large-scale application.

When it comes to FaceStation 2 (FS2-D) there was more hesitation as there was a need to register their faces. The acceptability decreased even more as the process took longer and as it got a bit complex during the first days the acceptability from the client company was also affected because of connection to the Wi-Fi which meant that it had more exposure. It was resolved by using a regular cable, the system was flexible as it could support 10/100/1000 Mbps.

The acceptability of these devices were very similar across many companies as there was a balance between curiosity and hesitation. The BioStation 2 had more acceptability as most of the people also used smart devices which came with Fingerprint biometric security of its on.

# 4.3. Performance

Under certain conditions the FaceStation 2 (FS2-D) performed very well as it had faster processing power and less difficulty for users after the initial stage of installation. The performance was better because this system also incorporated heat detection which was found useful now as there is COVID-19 restrictions that requires facemasks.

| Main Performance indicators | FaceStation 2 (FS2-D) (Facial) | BioStation 2 (BS2-OEPW) (Fingerprint) |
|---|---|---|
| | | |
| CPU | 1.4 GHz Quad Core | 1.0 GHz |
| Memory | 8GB Flash + 1GB RAM | 8GB Flash + 256 MB RAM |
| LCD Resolution | 800 x 480 | 2.8" QVGA Color LCD |
| Sound | 24 bit/Voice DSP (echo cancel) | 16-bit Hi-Fi |
| 1:1 (Maximum user) | 30,000 | 500,000 |
| 1: N (Maximum user) | 4,000 | 20,000 |
| 1:1 (Maximum Template) | 900,000 | 1,000,000 |
| 1: N (Maximum Template) | 120,000 | 40,000 |
| Text Log (Maximum) | 5,000,000 | 3,000,000 |
| Ethernet | 10/100/1000 Mbps | Not supported |
| power | Voltage: 24 VDC<br>Current: Max. 2.5 A | Voltage: DC 12V<br>Current: Max. 600 mA |
| Wi-Fi | Supported | Supported |
| Ingress Protection | Not Supported | IP65 |

*Table 4 Performance of BioStation 2 and FaceStation 2 (Source: https://www.supremainc.com/en/hardware/security-products-lineup.asp)*

It good to note that the ideal temperature, humidity, and RF range is the same for both systems. From the above table we can see that the performance of the facial system (FaceStation 2) was better as it handles more processes, but it also requires higher storage. If we take a look at the amount of users each system accepts it's the opposite as the difference is more than ten folds. For clients that are more concerned about the number of users (Large companies) it might not be a good idea to go for FaceStation 2 but performance wise FaceStation 2 had the upper hand.

# 4.4. Universality

Universality can be defined as the “quality or state of being universal (existing everywhere or involving everyone )” (34) . The owner of both of the devices is the same company as a result the distribution as well as placement is based on request, As long as the supply chain exists both of the devices will be available so the author chose to compare the given products based on its ability to involve everyone . This biggest obstacle when it comes to involvement is disability.

## 4.4.1 Disability

A disability could be many types but for this thesis there would be a concentration on hand and face as that will affect the biometric system that is being compared.

The largest numbers of disabilities are recorded in developing countries (34). Between the years of 2015 and 16 around 13.7% of people living in the rural part of Ethiopia had disabilities with the largest group being in the age range of 30 to 50 which can be considered as the working class (35) .

According to a report by World Health Organization the highest disability in Ethiopia were Leg or arm impairment (32%) , partial or total blindness (32%) and speech/ hearing impairment (19%) (36)

Types of Disability in Ethiopia

| Type of Disability | % of population |
|---|---|
| Blind | 0.1 |
| Difficulty seeing | 0.19 |
| Deaf | 0.03 |
| Difficulty hearing | 0.09 |
| Unable to speak | 0.013 |
| Deaf and Unable to speak | 0.05 |
| Non-functional Upper Limbs / Lower Limbs | 0.274 |

*Table 5 Disability in Ethiopia in population and cause (Source: Own calculation from latest Census 2007 data).*

With this results we can understand that the chance of having a user with hand disability is very high and the BioStation 2 (BS2-OEPW) (Fingerprint) is not inclusive considering the fact that there is no alternative solution without the use of a combined system. It should be clear that hand disability is not only bounded by losing a hand as it can also mean losing control over it

which can affect users. when it comes to FaceStation 2 the possibility of finding a person with face disability such as face burns is slim to none. To add to that FaceStation 2 supports disability as it allows flexibility as it can be adjusted for kids and people that are not able to stand or move freely.

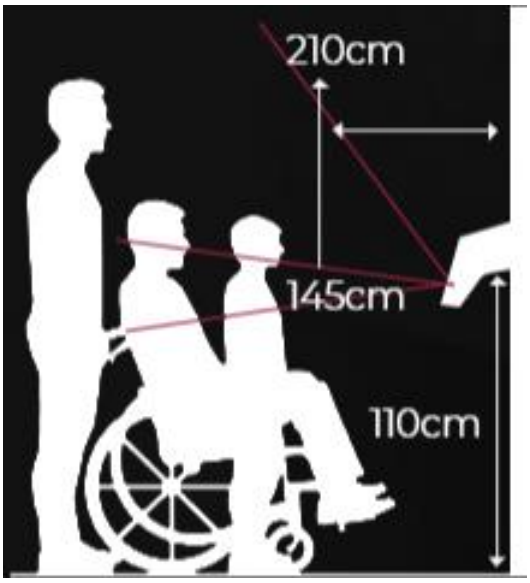



*Figure 6 FaceStation2 Options for Disability (Source: https://www.supremainc.com/en/hardware/face-recognition-terminal-facestation2.asp)*

# 4.5. Uniqueness

Uniqueness is a general character which describes all biometric systems including the two systems that we are comparing the difference will come when the question “how unique?” is asked. In order to understand the uniqueness of biometric systems there is a need to understand how each biometric differs from the other for this reason the author will be using a system that is used by forensic experts when handling fingerprint it is termed as ACEV (Analyze , Compare , Evaluate ,Verify ). (38)

*Figure 7 Different types of fingerprint (Source: www.scienceabc.com)*

In the above figure we can see two fingerprints the first one is the whorl and the second the loop these fingerprints were already analyzed as they were already taken off a scene but usually the steps included collecting the fingerprint using a powder and then inversing the fingerprint forming black and white format which then can be compared with each other. The figure clearly shows how different each pattern is even if it is the same finger type .

Comparison is done using technology or the human eye depending on who is doing the analysis. For this specific case the author used the eyes as there is a clear difference but usually if the fingerprint comes from the same type it is more difficult to tell with the naked eyes so for those cases there is a requirement to use a microscope or a verification software .

When it comes to Facial recognition the systems are fed the different Eigen faces from which it narrows down a specific person that is in the system.

*Figure 8 The average Eigen face from the vectors (Source: https://www.udacity.com/course/introduction-to-computer-vision--ud810)*

Unlike fingerprint biometrics the facial recognition systems are trained by feeding multiple pictures of the person so that it processes the pixel which will lead it to have a specific outcome that makes it highly dependent on the information that it is fed because of that some facial recognitions have some biases which lead to higher false verification (39) for our case that wont be a problem as FaceStation 2 will be enrolling a specific number of people in the company which will make the job easier .

Identifying an individual based on facial identification is more difficult as it requires a specific conditions to be adjusted in order to show best results according to a study by National Institute of Standards and Technology (38) the current technology is only able to differentiate twins under ideal conditions any manipulation of the controlled variable will lead to lower accuracy which will lead to a higher FAR . It found that the most important external conditions that needs to be controlled are the lighting in the room and expressions on the user faces.

It also explained that most systems can distinguish people in a crowd that are in public, but it had difficulty when it came to twins (not under ideal conditions). Facial expression had a large effect on the system rather than the age and gender. The algorithm performance was not as expected as it was below the base line. Under ideal condition it is possible to distinguish twins using facial recognition, but it is very challenging if it is not.

In conclusion the uniqueness of each system is dependent on different condition that need to be met but from the above studies the fingerprint biometrics had less FAR even if it was from twins that had close features unlike the facial biometric that required the ideal condition for higher rejection rate .

# 4.6. Permanence

Permanence can be described as the stability of a system as measured by the effect of change of time on the performance of the biometric device. (40) There is a need for further research for this factor as it can be affected by multiple situations such as placement when BioStation2 was being used it was frequently placed outdoors which will expose it to dust as well as water moisture even if it has resistance to these exposures it will degrade more quickly than its counterpart . The FaceStation 2 was different as it was in a closed environment which was far from most the above particles, but one thing was certain as there were frequent misuse from employees of the companies which was solved by more training.

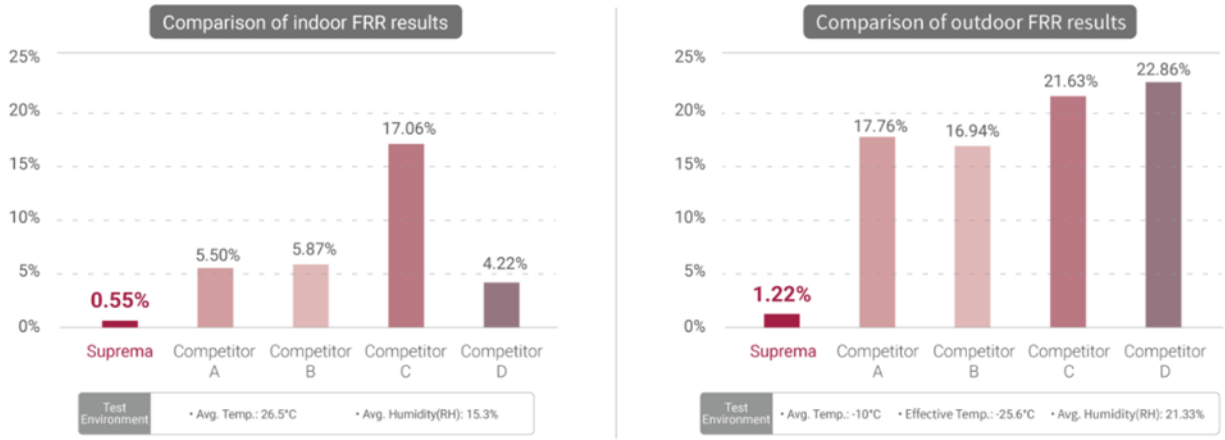



*Table 6 FRR of Suprema Fingerprint security for both outdoor and indoor installations (Source: https://www.supremainc.com/en/hardware/security-products-lineup.asp)*

| Biometric Traits | Test | Test Conditions | False Reject Rate | False Accept Rate |
|---|---|---|---|---|
| Fingerprint | FVC 2006 | Heterogenous population (manual workers and elderly people) | 4.2% | 0.1% |
| | FpVTE 2003 | U.S. government operational data | 0.6% | 0.1% |
| Face | FRVT 2006 | Controlled illumination | 0.8-1.6% | 0.1% |

*Table 7 Factors affecting biometric system selection regarding False reject and false accept rates (Source: (Anil K. Jain, 2011))*

The above tables shows that the FRR for BioStation 2 system which was tested for both indoor and outdoor scenarios it performed quite well even if the FRR had doubled as there was more exposure to the immediate environment its FRR was still below the standard . It is good to keep in mind that the result could vary based on the region as well. When it comes to Facestation 2 it had FRR of 1% that keeps it in the range which makes it 25% above the minimum standard that in return makes it more stable than BioStation 2 when considering results from the indoor but if we also consider the outdoors BioStation2 performs much better as there is a need to place it indoors as it is sensitive to its environment .

### 4.6.1 Aging effects

**Facial Biometrics**

FaceStation 2 could be considered as one of the most equipped systems when it comes to facial recognition but that doesn't make it exempt from the aging effect as it considers all the features a person has on their face. There are different ways of characterizing the different changes that can occur on the face due to age:

A, change in shape

B, loss or gain of weight

C, wrinkles

It is also important to mention that sagging of any part of the face (e.g. cheeks) can affect the systems of FaceStation2. As the type of biometric is new the aging effect has not been thoroughly studied because of that the database is not fully available.

Facial biometrics templates are greatly affected by aging as aging brings a significant change to everyone's face which will make it difficult for authenticating the user and there will be a need to modify the system to update the biometric templates.

**Fingerprint**

BioStation 2 can be affected by age as much as FaceStation 2 even if it doesn't look like it has direct relations. The changes occur rapidly from the age of 0 – 12 and stabilizes from 40 till 45 after which it starts to decrease which can be described as linear (35). As the gap between the samples increases there will be a high chance that there will be a performance loose .Aging affects the elasticity of the skin which will have a direct consequence on the scanner as it won't be firm contact. There could be multiple reasons for changes in the fingerprint, but the main reasons could be the exposure to injuries or damages as it will highly increase.

*Figure 9 Aging effect on fingerprint (Source: https://www.wired.com/magazine/wp-content/images/19-09/ff_indiaidb_f.jpg)*

To conclude the effect of aging on FaceStation is extremely high because of that the template needs to be updated frequently while for BioStation 2 the fingerprint wont degrade rapidly as the change usually takes 5 years to clearly observe and 10 years to be able to see a complete change so it goes without saying that fingerprint biometrics performs better with time as it is not dependent on peoples weight , beard or any other changes a user can go through in their day to day apart from accidents.

The permanence of the two systems could be affected by multiple factors for the two main once that have been described above the BioStation 2 had more resistance , flexibility and also adaptability in different environment which will make it the preferred option .

# 4.7. Measurability

Also referred to as collectability, the measurability of a biometric system can be understood as the ability of the given system to avoid or decrease user inconvenience. It can be found by measuring the FTA (Failure to Acquire) and FTE (Failure to Enroll).

Before starting the acquisition process it's important to add the devices (BioStation2, FaceStation 2) to the platform BioStar2. To do that we must follow these steps:

BioStar 2 > Devices > Search Devices > BioStation 2 / FaceStation 2 > Add > Ok

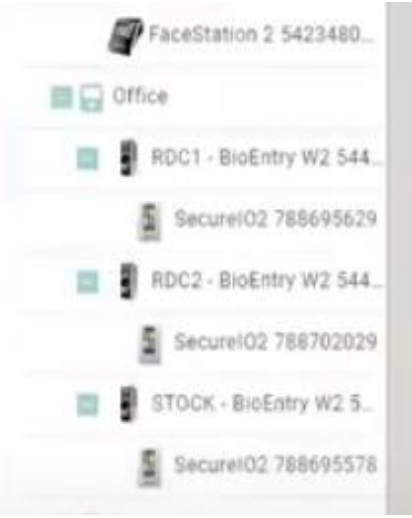



*Figure 10 Added devices on BioStar 2 (Source: Suprema)*

When looking at the fingerprint acquisition process it has become much easier throughout the years. A good example could be online sensors which have a very high capture rate even for high resolution images.

When it comes to deployment, both BioStation 2 and FaceStation 2 are new to most of the companies that used them as most were used to Pin Codes and cards . When the enrolment began the employees started getting registered using the BioStar 2 platform at first which was followed by each device. The BioStation 2 has some unique feature that makes it easy for collecting fingerprint data for example it has resistance to water, dust and moisture so choosing an ideal location isn't that important only requirement was a power supply and a Wi-Fi. Its flexibility is also reflected in the time it took to collect it as it takes less time and minimal supervision. It can be set up using the following steps:

Menu > User > Add User > Scan Finger > Verify (Option to continue with another finger)

| | |
|---|---|
| ID | |
| Name | |
| PIN | |
| Fingerprint | |
| Card | |
| User Level | |
| Start Date | |

*Table 8 BioStation 2 Enrolment process (Source: own)*

The enrolled fingerprint will be in the system and in BioStar 2 as the systems are synchronized. There is no need to keep a certain distance and body angle if the finger covers the scanner.

The enrolment is based on the availability of a clean finger with no injuries as the system might have difficulty reading it but there are other fingers that can be used unlike facial acquisition. There is also an opportunity to enroll using a smart phone that uses Android Lollipop 5 as the systems are as described above synchronized.

For FaceStation 2 the same process applies when it comes to the initial steps, but the later stages differ as registration will be facial.

Menu > User > Add User > Add ID > Register Face > Verify

The process of registration has 3 stages with each having 5 seconds recording:

1, Frontal face

2, Moving the face up and down

3, Moving face left and right

This makes it more difficult as each user needs to follow directions and stand still not to mention the need to control their bodies movement for the measurement to work user has to stand at least 40cm or at most 80cm from the scanner , have a stable facial expression (must not be changed) , eyes and eyebrows shouldn't be covered and most importantly people that wear glasses are registered twice once with the glass and the another without .

It has important benefits as well. If the company is to buy the extra thermal detector it helps solve the biggest problem post COVID-19 as it is able to scan users without the need for them to take off their masks while keeping their distance that is a big benefit as it combines both types of safety: Security and Health . If the Thermal camera is used there is an extra step to be taken as the FaceStation 2 will require the user to register a stable body temperature.

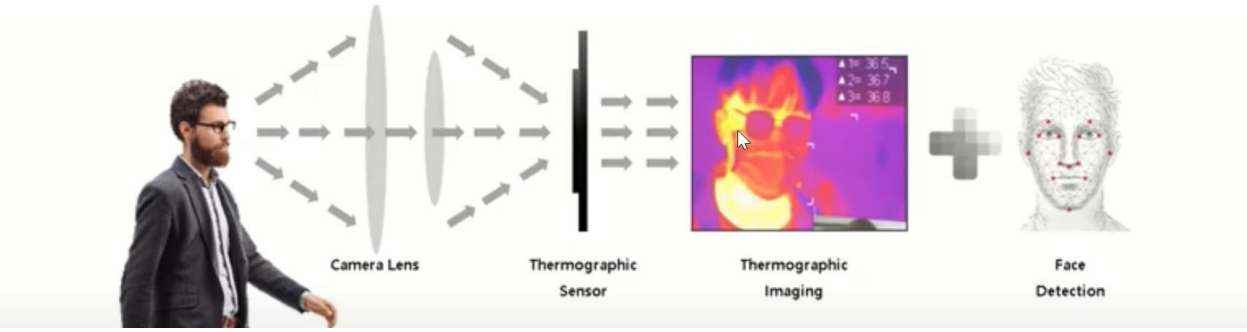



*Figure 11 Thermal detection (Source: https://www.egress-sys.co.uk/facestation-2-thermal-camera/)*

FaceStation 2 has multiple requirements to receive usable image, these are the parameters that needs to be adjusted depending on the conditions an example could be the different angles, lighting, camera-user distance. The results could easily be manipulated by shifting any of the above. The best system at this time is the 3D sensors (used by FaceStation 2) which solves most of the problems that the 2D had such as aging. This process showed that skin reflectance had the greatest effect to the FaceStation 2 sensor.

In conclusion measurability (collectability) of a biometric is highly dependent on data acquisition process and from the above experience the fingerprint biometric acquisition is easily performed even if the type of sensors aren't found in everyday commercial use it is possible to say it can be frequently used in the coming years but when it comes to facial biometric acquisition it can be difficult as there is a need to control different factors that can easily change the results for both controlled and uncontrolled environment as a result the user will be affected .

# 4.8. Circumvention (Attack scenarios)

To understand the systems weakness, it's important to see the whole process with that being said the figure below shows the configuration of FaceStation 2.

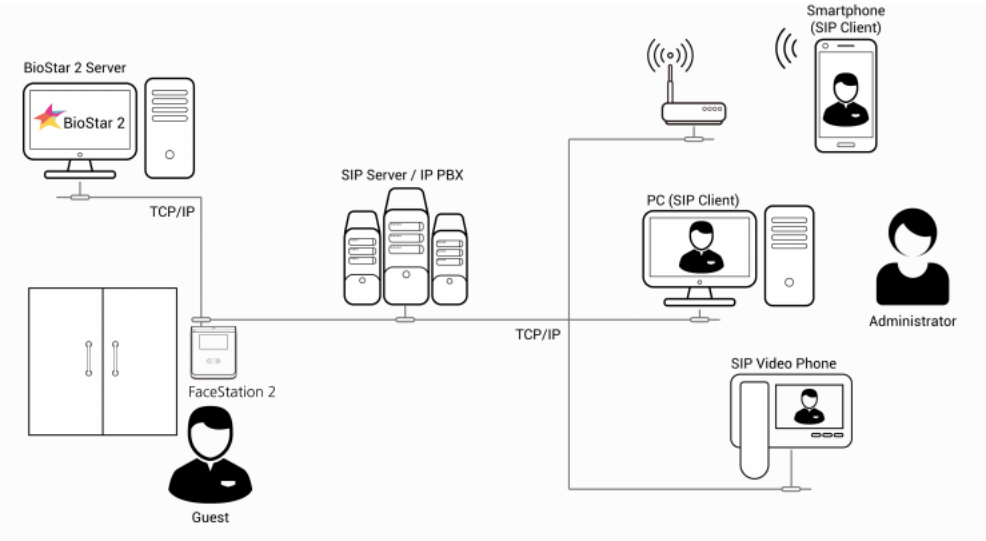



*Figure 12 FaceStation 2 configuration (Source: https://www.supremainc.com/en/hardware/face-recognition-terminal-facestation2.asp)*

The above system only shows the main idea as the real design starts from the dashboard where the administrator will have control over each specific device. when adding the different devices there is an option to set a "trigger and action" as action reaction option where each information will be permitted. Depending on the set up it can sound an alarm when it senses spoofing , forced entry , high temperature ( if thermal camera is installed ) or it can go as far as denying access to disability which can be used for good as it could be a construction site . The design makes it difficult to use the usual tricks to get access the anti-passback, anti-tailgating and the unique Live face detection (Infrared) are some of its features. The system is all in one location since the only way of enrolling a user is on site the system doesn't give a lot of flexibility for attackers to get access. When looking at the BioStation 2 the situation becomes different as it allows enrolment from the user's phone which makes it easier to attack. The most difficult part is finding an access to the platform for this case BioStar 2 which is solved as the user is only required to find the phone and password or pin. Even if it won't be easy the portability of a phone will allow the attacker enough time to try multiple times and use different substance. The action can be completed if the user was to enroll himself in the system as the person can have his on access to the company weather, he chooses fingerprint, chip, or even mobile NFS. There is a Bluetooth option as well which increases its vulnerability .

The usual method of placing a transparent plastic on the sensor won't work as it is placed in the compound rather than public surrounding not to mention the refraction that will occur because of the tendency of the material that will be placed .

The author has done multiple fake finger spoofing penetration testing which was not successful as the sensor security of BioStation 2 was strong but the vulnerability of the phones fingerprint biometrics are dependent on the type the client decides to use . A hacker in this day and age can use multiple materials in order to gain access using the phones .

Another method could be to use the data in the BioStation 2 itself as explained previously the systems are synchronized and as a result the information will be stored in the BioStation 2 rather than being the usual receiver. There is an external feature which will guarantee data safety if unplugging the ethernet cable possibly occurs actions such as enrolment can still continue . For this case it means that there is data on the device which is unprotected and the only layer of protection will be the pin which most companies forget or choose not to change

There are multiple vulnerabilities in a Fingerprint biometric system but for this scenario there will be a concentration on spoofing (Sensor attack) as it is one of the easiest to attack and difficult to defend. There is also away to get access from non-cooperative person as it was done by Jan Krissler (starbug) as he was able to use a photograph of Germany's Defense Minister's fingerprint and make a clone in order to get access to the phone. It should be noted that it was from 3,4,5,6 and 7 meters in order to get the full image. Without the need of contact or even presence (pictures taken by professional photographer) and by using household materials. 60% of the dummies were able to be authenticated. This goes to prove that the cooperation is not really needed for an attacker to be able to access the mobile device . (43)

The FaceStation 2 had more resistance as even printed pictures were not being authenticated as it uses infrared technology . Over all it was easier in order to try or even plan ways of finding access from BioStation 2 but for FaceStation 2 it was much harder at least for everyday people to try to get access.

# 4.9 Cost Comparison

The price of each device differs based on location and distributers as it is not sold directly by the company itself. Both devices have multiple capabilities which makes their use very wide because of this reason the prices below will only reflect on the Access control system and their accessories as they don't function independently. It is worth noting that the prices are based on the conversion rate of Ethiopian Birr to United State Dollars at the time, as the products are importing the prices are set based on the taxes and logistics costs. The prices could be reduced or increased depending on the specific case such as large acquisition of a specific product or when the installation is for large companies that require a lot of hardware. The overall expense comes from labor and the product itself.

| | **Installation 1** | **Installation 2** |
|---|---|---|
| **BioStation 2** | 1300$ | - |
| **FaceStation 2** | - | 1450$ |
| **Secure I/O Reader (Single Door)** | 110 $ | 110 $ |
| **Secure I/O Reader (Multiple Door)** | 429 $ | 429 $ |
| **Software License (BioStar 2) 6-20 Doors MSRP** | 370$ | 370$ |
| **Assembly/Installation fee (per door)** | 150 $ | 200$ |
| **Regular Maintenance (Monthly)** | 100 $ | 100 $ |
| **BioMini Plus 2** | 134 $ | 134 $ |
| **Total** | 2593$ | 2793$ |

*Table 9 Actual cost of BioStation 2 and FaceStation 2 installation in Addis Ababa, Ethiopia 2020 (Source: iSense Technology and other Distributors)*

(Notice : The prices were originally provided in Ethiopian Birr and the author converted the prices back to USD using https://www.xe.com/currencyconverter/ based on 2021 rate)

As the table above shows on average it was cheaper to use BioStation 2 as it required less fees for installation and others. The result was an average from the distributers that sell them as it is becoming a competitive market. These fees are only for the specified number of users as the license fee is higher for more users. The installation costs for larger buildings require more manpower and also products which in return creates a steep price difference.

# 5. Result

## Multi criterial analysis

From the information gathered above we will be analyzing the results by using a simple Multi Criterial Analysis. A table containing the 8 factors was created and made the decision making much easier. we will be using a simple "x" to indicate which one was found to perform better in each of the factors.

The factors are

**Acceptability** – Which will indicate the acceptance of the system in the immediate environment we plan to implement the system.

**Performance** – It will indicate the accuracy of the system when being implemented.

**Universality** – This will be describing how easily the system can found and its availability for all type of users .

**Cost** – The actual cost of deploying the devices

**Uniqueness** – Shows how unique the specific biometric trait really is.

**Permanence** – The ability for the accuracy to stay the same as time changes.

**Measurability** – The Ability to easily measure the biometric trait of individuals.

**Circumvention** – The ability to resist attacks from unknown intruder.

| | **Acceptability** | **Performance** | **Universality** | **Cost** | **Uniqueness** | **Circumvention** | **Permanence** | **Measurability** |
|---|---|---|---|---|---|---|---|---|
| **Fingerprint biometric system** | X | | | X | X | | X | X |
| **Facial biometric system** | | X | X | | | X | | |

*Table 1 Multi criterial analysis of Result collected (Source: own)*

We can clearly see a difference in both above systems as fingerprint dominates in most of the factors. This will answer the questions that were left unanswered when this thesis was started. It

shows that spending a lot of money on facial biometric system is pointless at this time as it will have more side effects then benefits. In public use the facial biometric will have higher FMR than fingerprint which will result in higher miss match which at the end will affect public safety.

# 6. Conclusion

The aim of my thesis was to compare the safety standards of Fingerprint and Face Recognition Biometric system as they are the main biometric system that are in use today. An analysis was conducted on the advantage and disadvantage of each system in the scope of the devices (BioStation 2 and FaceStation 2). Products of Suprema HQ inc. were chosen as their applications were in both private and public sector. The theoretical part included a review of different literatures on how the Fingerprint and Facial biometrics function and what makes them unique and the practical part compared the chosen devices (BioStation 2 (BS2-OEPW) and the FaceStation 2 (FS2-D)) against 8 key factors which resulted in a clear answer.

The thesis explored and included effects such as aging as well as privacy concerns on the users as most researches don't include these factors for comparing biometrics. The results clearly showed the BioStation 2 fingerprint biometric system were more than 60% better than FaceStation 2 from the overall results. Even if fingerprint was found to have a better outcome the safety issue was better answered by FaceStation 2 as finding access was very difficult.

In conclusion using BioStation 2 fingerprint biometric was found to be a better solution for the security concerns that we are having in this day and age as it answered most of the concerning factors that were raised as a result the author believes it's the best option for use at this time. The safety weakness that was described in this thesis can easily be answered by assigning a person to look after the processes which can easily be used by private or government offices .

The opinions that have been included in this thesis are the authors own and doesn't reflect the official company (iSense Technology, Suprema HQ inc.) stance or policy on this matter.

## Bibliography

1. *Biometric Recognition: Security and Privacy Concerns.* **S. Prabhakar, S. Pankanti and A. K. Jain.** 2, Armonk : IEEE Security & Privacy, 2003, Vol. 1.

2. *The Permanence of Finger-Print Patterns.* **Faulds, Henry.** 2464, s.l. : Nature, 1917, Vol. 98. 10.1038/098388c0.

3. *FUNDAMENTALS OF BIOMETRIC AUTHENTICATION TECHNOLOGIES.* **WAYMAN, JAMES L.** 1, s.l. : International Journal of Image and Graphics, 2001, Vol. 1. 10.1142/S0219467801000074.

4. *Biometrics Verification: a Literature Survey.* **Mir A.H, Rubab, S and Jhat, Z. A.** 2, s.l. : Journal of Computing and ICT Research, 2011, Vol. 5.

5. **National Research Council, Division on Engineering and Physical Sciences, Computer Science and Telecommunications Board, Whither Biometrics Committee.** *Biometric Recognition: Challenges and Opportunities.* 2010. 0309142075, 9780309142076.

6. **Anil K. Jain, Arun A. Ross , Karthik Nandakumar.** *Introduction to Biometrics.* New York : Springer New York Dordrecht Heidelberg London, 2011. 978-0-387-77325-4.

7. *Security issues of Internet-based biometric authentication systems:.* **Zeitza, Christian.** Vigo : Signal and Communications Processing Dpt., Univ. of Vigo, 2005.

8. **Chao, Gao.** *Study on Privacy Protection and Anonymous Communication in Peer-to-Peer Networks.* Huangshi : IEEE, 2009. 978-0-7695-3843-3.

9. *A Multi-Biometric Template Security: An Application of Code-Based Cryptosystem.* **Ajay Sharma, Deo Brat Ojha.** Ghaziabad : Research Scholar Singhania University, 2011.

10. **ISO.** Information technology (Vocabularies). 1, 2015.

11. —. Condition monitoring and diagnostics of machine systems. 1, 2003.

12. *THEORETICAL STATISTICAL CORRELATION FOR BIOMETRIC IDENTIFICATION.* **Schuckers, Michael E.** New York : Center for Identification Technology Research (CITeR), 2008.

13. *A Survey on Multimodal Biometric.* **Sakshi Kalra, Anil Lamba.** 2, Haryana : International Journal of Computer Science and Information Technologies, 2014, Vol. 5.

14. *Improving Delaunay Technique for Fingerprint Recognition.* **Ankita, Iqbaldeep Kaur.** 1, s.l. : International Journal of Computer Science Issues, 2015, Vol. 12. 1694-0784 .

15. *Multi-Biometric Approaches to Face and Fingerprint.* **Dr Shubhangi D C, Manohar Bali.** 5, Gulbarga : International Journal of Engineering Research & Technology, 2012, Vol. 1. 2278-0181.

16. *A Method for fingerprint authentication for ATM based banking application* . **S.Koteswari, Dr.P.John Paul , V.Pradeep kumar , A.B.S.R.Manoha.** 9, Andhra Pradesh : International Journal of Computer Science and Information Security, 2011, Vol. 9.

17. *Study of Fingerprint Patterns in Relationship with Blood group and Gendera Statistical Review.* **Desai Bhavana, Jaiswal Ruch , Tiwari Prakash , Kalyan J.L.** 1, Karnataka : Research Journal of Forensic Sciences, 2013, Vol. 1.

18. *Fingerprint Recognition.* **Fernando Alonso-Fernandez, (in alphabetical order) Josef Bigun, Julian Fierrez, Hartwig Fronthaler, Klaus Kollreider, and Javier Ortega-Garcia.** Madrid : BioSecure Multimodal Evaluation Campaign, 2008.

19. *Biometrics and Fingerprint Payment Technology Computer Science & Technology.* **Priya, S.Padma.** 1, s.l. : International Journal of Advanced Research in, 2017, Vol. 5.

20. *Fingerprint Segmentation Algorithms: A Literature.* **Rohan Nimkar, Agya Mishra.** 5, Jabalpur : International Journal of Computer Applications, 2014, Vol. 95.

21. *Overview of Fingerprint Recognition System.* **Mouad M.H. Ali, Vivek Hilal Mahale , Pravin Yannawar , Ashok Gaikwad.** Tamil Nadu : International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016. 10.1109/ICEEOT.2016.7754902.

22. *Fingerprint Recognition and its Advanced.* **Soukhya S M, Sonu G , L Karthik Narayan.** 04, Bangalore : International Journal of Engineering Research & Technology (IJERT), 2020, Vol. 9.

23. **Davide Maltoni, Dario Maio , Anil K. Jain , Salil Prabhakar.** *Handbook of Fingerprint Recognition.* s.l. : Springer Professional Computing, 2009. 978-0387954318.

24. *Vulnerabilities and Performance Analysis over Fingerprint Biometric Authentication Network.* **Edward Guillen, Lina Alfonso, Karina Martinez and Marcela Mejia.** San Francisco : Proceedings of the World Congress on Engineering and Computer Science, 2012, Vol. 2.

25. *Performance of fingerprint quality measures depending on sensor technology.* **Fernando Alonso-Fernandez, Fabio Roli , Gian Luca Marcialis.** 1, s.l. : Journal of Electronic Imaging, 2008, Vol. 17. 10.1117/1.2895876.

26. **Alejandro Chau Chau, Carlos Pon Soto.** *Hybrid Algorithm for Fingerprint Matching Using Delaunay Triangulation and Local Binary Patterns.* s.l. : Springer, 2011. 978-3-642-25084-2.

27. *Minutia based partial fingerprint recognition.* **Jea, Tsai-Yang.** s.l. : University of Buffalo, 2005.

28. *Guide to Biometric Reference Systems and Performance Evaluation.* **Bernadette Dorizzi, Gerard Chollet , Dijana Petrovska-Delacrétaz.** s.l. : Springer, 2009. 978-1-84800-291-3.

29. *Biometrics and Face Recognition Techniques.* **Bhatia, R.** 5, Haryana : International Journal of Advanced Research in Computer Science and Software Engineering, 2013, Vol. 3.

30. **Ao M., Yi D., Lei Z., Li S.Z.** *Face Recognition at a Distance: System Issues.* London : Springer, 2009. 978-1-84882-384-6.

31. *Video-based face recognition: A survey.* **Huafeng Wang, Y. Wang , Y. Cao.** s.l. : World Academy of Science, Engineering and Technology , 2011.

32. *Three-Dimensional Model Based Face Recognition.* **Xiaoguang Lu, Dirk Colbry, and Anil K. Jain.** Michigan : Department of Computer Science & Engineering, 2005. 10.1007/11527923_104.

33. **Samir Nanavati, Michael Thieme , Raj Nanavati.** *Biometrics: Identity Verification in a Networked World.* s.l. : Wiley, 2007. 978-0471099451.

34. **Organization, World Health.** *World Report on Disability.* s.l. : World Health Organization, 2011.

35. **Kulkarni, Vani S.** *Rural Poverty and Disability in Ethiopia.* s.l. : Global Development Institute, 2020.

36. **Organization, Wold Health.** *Disability in Ethiopia: the scope of the problem* .

37. **Anil K.Jain, Salil Prabhakar , Sharath Pankanti.** *On the similarity of identical twin fingerprints.* NY : Science Direct , 2002. Vol. 35.

38. *Facial Recognition of Identical Twins* . **Matthew T. Pruitt, Jason M. Grant, Jeffrey R. Paone, Patrick J. Flynn , Richard W. Vorder Bruegge.** VA : Digital Evidence Laboratory, Federal Bureau of Investigation , University of Notre Dame, 2011.

39. *Double Trouble: Differentiating Identical Twins by Face Recognition.* **Jeffrey R. Paone, Patrick J. Flynn , P. Jonathon Philips , Kevin W. Bowyer , Richard W. Vorder Bruegge, Patrick J. Grother,.** 2, s.l. : IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2014, Vol. 9.

40. *Biometric Permanence: Definition and Robust Calculation.* **John Harvey, John Campbell , Stephen Elliott and Michael Brockly , Andy Adler.** Ottawa : Dept. of Systems and Computer Engineering, 2017.

41. *Implementation of Easy Fingerprint Image Authentication with Traditional Euclidean and Singular Value Decomposition Algorithms* . **M. James Stephen*, P.V.G.D Prasad Reddy.** 2, Visakhapatnam : Int. J. Advance. Soft Comput. Appl (ICSRS), 2011, Vol. 3. 2074-8523.

42. *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems.* **C. M. Cook, J. J. Howard, Y. B. Sirotin, J. L. Tipton and A. R. Vemury.** 1, s.l. : IEEE Transactions on Biometrics, Behavior, and Identity Science, 2019, Vol. 1. 10.1109/TBIOM.2019.2897801.

43. *Ich sehe, also bin ich ... Du.* **Krissler, Jan.** s.l. : Chaos Communication Congress, 2014.

44. *Introduction to Biometrics.* **Jain, Anil K., Ross, Arun A., Nandakumar, Karthik.** s.l. : springer, 2011. 978-0-387-77326-1.

45. *Biometric recognition: security and privacy concerns.* **Salil Prabhakar, Sharath Pankanti , Anil K. Jain.** s.l. : IEEE SECURITY & PRIVACY, 2003.

46. *Usability Evaluation Model for Biometric System considering Privacy Concern Based on MCDM Model.* **Junhyoung Oh, Ukjin Lee , Kyungho Lee.** seoul : Security and Communication Networks, 2019. 10.1155/2019/8715264.

47. *FRVT 2006 and ICE 2006.* **P. Jonathon Phillips, W. Todd Scruggs , Alice J. O'Toole , Patrick J. Flynn , Kevin W. , Cathy L. Schott , Matthew Sharpe.** MD : National Institute of Standards and Technology Gaithersburg, MD 20899, 2007.

48. *Security and Accuracy of Fingerprint-Based Biometrics: A Review.* **Wencheng Yang, Song Wang , Jiankun Hu , Guanglou Zheng and Craig Valli.** Canberra : Security Research Institute, Edith Cowan University, 2019.

49. *Biometrics: Accessibility challenge or opportunity?* **Ramon Blanco-Gonzalo, Chiara Lunerti,Raul Sanchez-Reillo,Richard Michael Guest.** s.l. : Blanco-Gonzalo, 2018. 10.1371/journal.pone.0194111.

50. *Facial Biometric Templates and Aging : Problems and Challenges for Artificial.* **Lanitis, Andreas.** Lemesos : Department of Multimedia and Graphic Arts , Cyprus University of Technology, 2009.

51. *A survey of the effects of aging on biometric identity verification.* **Lanitis, Andreas.** 1, Lemesos : International Journal of Biometrics , 2010, Vol. 2. 10.1504/IJBM.2010.030415.

52. *Ongoing Face Recognition Vendor Test (FRVT) Part 6B: Face recognition accuracy with face masks using post-COVID-19 algorithms.* **Mei Ngan, Patrick Grother , Kayee Hanaoka.** s.l. : National Institute of Standards and Technology , U.S. Department of Commerce , 2020.

53. *Is your biometric system robust to morphing attacks?* **M. Gomez-Barrero, C. Rathgeb, U. Scherhag and C. Busch.** Coventry : IEEE, 2017, Vol. 5. 10.1109/IWBF.2017.7935079.

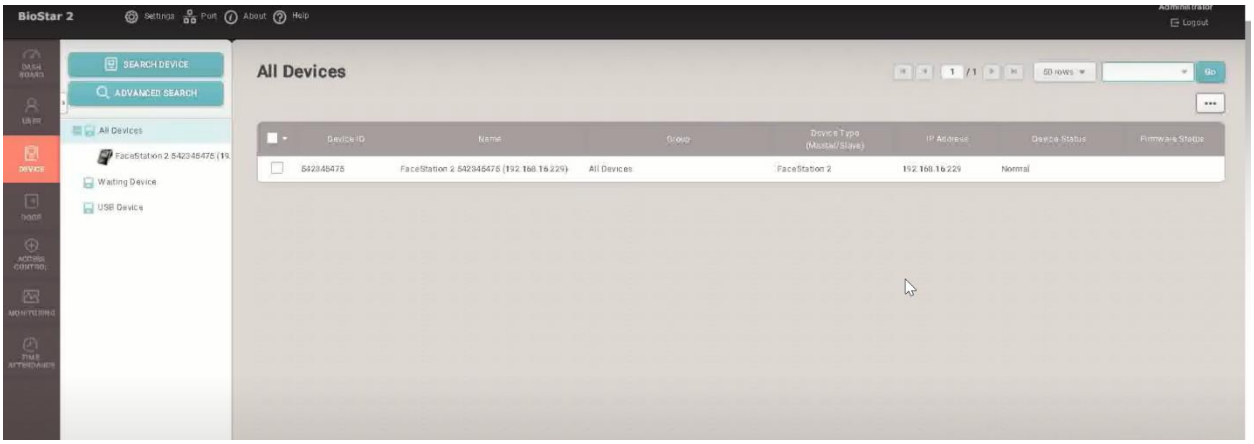
54. *Analysis of the attack potential in low cost spoofing of fingerprints.* **Goicoechea-Telleria, J. Liu-Jimenez, H. Quiros-Sandoval and R. Sanchez-Reillo.** Madrid : International Carnahan Conference on Security Technology (ICCST), 2017. 10.1109/CCST.2017.8167798.

55. *A Review of Facial Biometrics Security for Smart Devices.* **Mary Grace Galterio, Simi Angelic Shavit and Thaier Hayajneh.** New York : Fordham Center for Cybersecurity, 2018. 10.3390.

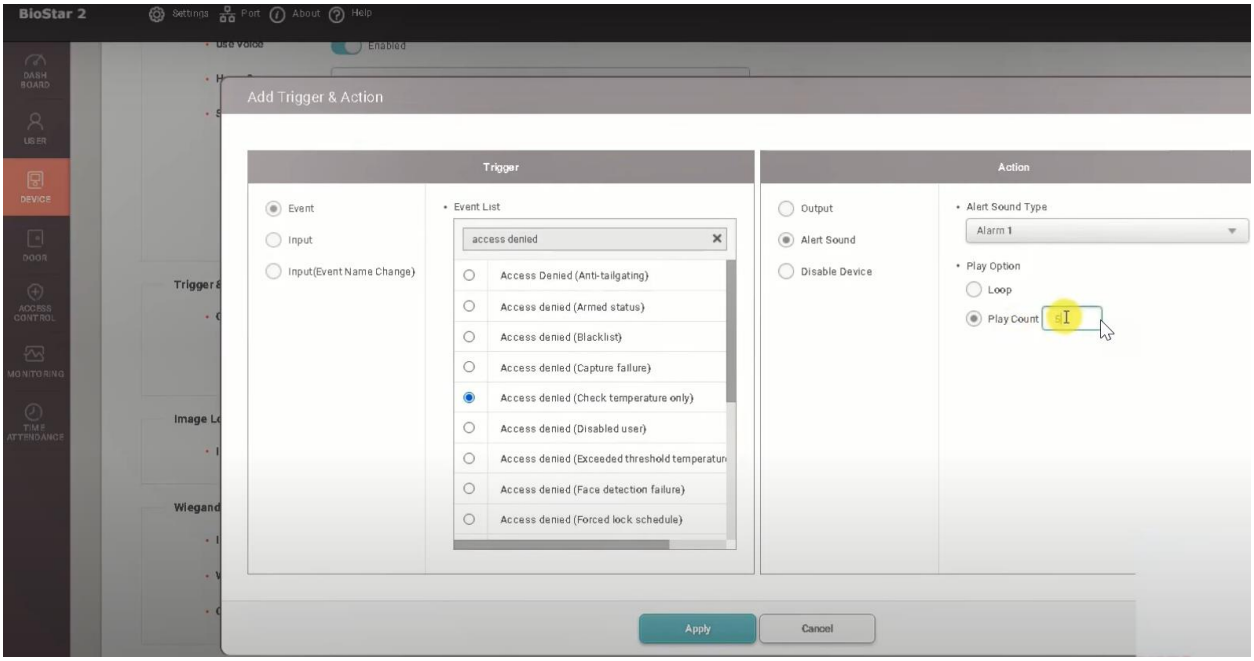
56. **Diane W. Braza MD, Jennifer N. Yacub Martin MD.** *Essentials of Physical Medicine and Rehabilitation.* s.l. : Science Direct, 2020. 978-0-323-54947-9.

# Appendix


1, The figure above shows a picture of an assembled FaceStation 2 and BioStation 2 with the Secure I/O Reader (Single and Multi-user) included (Source: Suprema)




2, The figure above shows the added device in the BioStar 2 dashboard (Source: Company)




3, The Figure shows an option to control a user by adding a condition in Trigger & Action for maximum security (Source: Suprema).