An Effective Biometric Patient Identification System for Health Organizations

Eman Buhagiar, Clifford De Raffaele
Faculty of Science and Technology
Middlesex University
Malta
emails: buhagiareman@gmail.com, clifford.de.raffaele@gmail.com

Abstract— **Medical errors, such as patient misidentification, are the reason for around 2.6 million deaths per annum and around $42 billion in costs for health organizations in low to middle-income countries. While wristbands are the most common method for identifying patients, they can be easily misplaced and may contain missing or inaccurate information as this study shows. This may result in wrong medications and surgeries and in some instances, even preventable deaths along with liabilities for the health organizations. An in-depth literature review is conducted in this study and the current methods and process for identifying patients are also investigated, accompanied by a comparison of existing patient identification solutions, as well as issues and concerns about health data protection and privacy. Following this, the system requirements are determined through a qualitative analysis from a questionnaire distributed to different healthcare professionals. Subsequently, the effectiveness of biometric technology for patient identification through face recognition is examined. The paper finally proposes and evaluates a proof of concept with promising results for minimizing patient identification errors.**

Keywords-medical errors; health organizations; biometrics; patient identification; face recognition.

I. INTRODUCTION

Patient misidentification is a recognized worldwide problem faced by medical organizations of different types and sizes [1]–[3]. It is estimated that around 2.6 million people die each year, in just low to middle-income countries, due to medical errors [4], including errors of patient identification [5]. 9% of 7,600 (684) patient misidentification events captured in 181 different health organizations over the span of 32 months in the US led to patient harm, and in some cases, death [9]. Patient identification errors occur on different levels throughout the medical field. Various medical wards and units have been subject to such errors, including but not limited to, maternity wards, oncology centres, Intensive Care Units (ICU) and children's hospitals. In certain situations, such misidentification has led to severe consequences, one of which is the death of a patient [4][6]. According to the World Health Organization [4], between November 2003 and July 2005, the United Kingdom had 236 reported incidents related to missing wristbands or wristbands with incorrect information, the United States of America also had more than 100 similar cases reported from January 2000 to March 2003.

The National Patient Misidentification Report conducted by Ponemon Institute LLC in 2016 in the US [19] highlights the primary root causes of patient misidentification. The main three reasons include incorrect patient identification at the point of registration, time pressure when treating patients, and thirdly, lack of employee training and awareness. The report also outlines the health organization's financial impact, where the denial of claims costs the average healthcare organization $1.2 million a year. In a survey conducted by the same institute, seventy-six per cent (76%) of the respondents, who work in different types of organizations, such as large hospitals and small clinics, responded that biometrics at the patient registration point could reduce denied claims.

Patient misidentification may also lead to duplicate medical records that are time-consuming for organizations to manage and arrange [7]. An increase in insurance fraud for intentional misidentification may also be the cause of errors in patient identification. The National Health Care Anti-Fraud Association of the United States [8] estimates that the financial losses due to health care fraud are between 3-10% of the annual health care expenditure, which could lead to more than $300 billion a year. Moreover, according to the Medical Theft Alliance (MIFA), more than 2 million American citizens have been victims of medical identity theft, with cases rising each year [9].

This study analyses the effectiveness of using biometric technology for identifying patients by performing a literature review in Section II on the current problems caused by patient misidentification, followed by elucidating the process of identifying patients, current existing identification solutions, and the security and privacy issues and concerns regarding identifying patients. For the methodology in Section III, a list of system requirements is developed after distributing a questionnaire to a number of health professionals and analysing the responses. Once the requirements are documented, a system based on face recognition technology is proposed and designed in Section IV followed by its evaluation against a dataset in Section V. Finally, the results are analysed, and further improvements are suggested in Sections VI and VII.

II. LITERATURE REVIEW

Despite patient identification errors being preventable, many hospitals worldwide do not have patient identification systems implemented [13]. The first goal of The Joint Commission's National Patient Safety Goals (NPSG) for 2020 is to improve patient identification accuracy, both in hospitals and laboratories. Although the World Health Organization (WHO), the Emergency Care Research Institute (ECRI) [10], and other authors all promote the use of technology for

reducing errors in patient identification [4][10][11]. It was found by the same ECRI that technology itself was the actual cause in 15% of patient misidentification errors. One of the potential barriers to mitigating or reducing patient identification errors is the costs associated with implementing such solutions [3].

The National Patient Misidentification Report conducted by Ponemon Institute LLC in 2016 [19] determines the primary root causes of patient misidentification. The top three reasons included incorrect patient identification at the registration point of time, which may consist of placing an incorrect wristband, time pressure when treating patients, and lack of employee training and awareness. The report also outlines the health organisation's financial impact, mainly due to denial of claims, costing the average healthcare organization $1.2 million a year. Table I shows more detailed cost calculations. In a survey conducted by the same institute, seventy-six per cent (76%) of the respondents, who work in different types of organizations such as large hospitals and small clinics, responded that biometrics at the patient registration point could reduce denied claims. The report also outlined that sixty-nine per cent (69%) of the survey respondents spend more than thirty (30) minutes per shift contacting medical records or other departments to get critical information about their patients. Patient misidentification may also lead to duplicate medical records that are time-consuming for organizations to manage and fix [13]. It is therefore necessary to understand the process for patient identification in health organizations to determine any points where patient misidentification is likely to occur.

TABLE I. COST OF FAILED CLAIMS DUE TO PATIENT MISIDENTIFICATION

Cost of failed claims resulting from patient misidentification			
Step	Cost categories	Source	Average value*
A	Total billings (gross revenue) per year	AHA Financial Facts 2015	$164,300,000
B	Percentage of denied clams	Ponemon Institute survey	30.10%
C	Estimated value of denied claims per year	Calculation (A X B)	$49,454,300
D	Percentage of denied claims resulting from patient misidentification	Ponemon Institute survey	35.23%
E	Estimated value of denied claims resulting from patient misidentification	Calculation (C X D)	$17,422,750
F	Percentage of denials resulting from patient misidentification that are successfully appealed	Ponemon Institute benchmark	93.0%
G	Estimated value of denials resulting from patient misidentification that were not successfully appealed (or dropped)	Calculation (E X (1-F))	$1,219,592
*The amounts presented pertain to the average-sized registered hospital in the United States with 169 bed capacity.			

A. Patient Identification Process (PIP)

77% of wrong-patient incidents, identifying the patient was not described at all in the incident reports [14]. In a report conducted for the Australian Commission on Safety and Quality in Health Care [15], patient identification and profiling mark the beginning of a patient journey in a hospital (Figure 1). The report emphasises on the importance of providing the patient with a unique identifier that stays with the patient for the rest of the journey and other future journeys or visits. The Bay of Plenty District Health Board [16] recommends using at least three approved identifiers to identify a patient correctly. These include the patient's name, date of birth, and the National Health Index number, with the latter depending on the country's person identification system in place. A patient's bed or room number is not considered an approved identifier and should always be avoided [16], [17]. A patient's profile would include any information that can be used to confirm the patient's identity. The Australian Commission's same report [16] suggests that part of this information can be included in the wristband. It also recommends that the wristband (or a tag) should link to the patient's health record in the system.

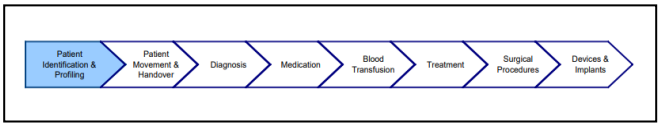

Figure 1. A patient journey in a hospital *[15]*

B. Identification Methods

While patient identification errors can be preventable [10], many hospitals worldwide do not have patient identification systems implemented [18]. The first goal of The Joint Commission's National Patient Safety Goals (NPSG) for 2020 is to improve patient identification accuracy, both in hospitals and laboratories [19]. Although many [10]–[12], [17], [18], [20] promote the use of technology for reducing errors in patient identification, it was found that technology itself was the actual cause in 15% of patient misidentification errors [10]. One of the potential barriers for mitigating or reducing patient identification errors is the costs associated with implementing such solutions [17].

1) Wristbands

Full implementation of a barcode-based Electronic Positive Patient and Specimen Identification (EPSID) system can result in a significant reduction in mislabeled specimens over three (3) years [21]. However, other studies identified wristbands as one of the leading causes of patient misidentification [22], [5]. The main issues are missing or wrong information and patients having more than one wristband. Implementing a simple wristbands system for patient identification is considered a low-cost practice for health organizations [23]. Since the simple wristbands with handwritten information on them are still prone to human error, the use of barcodes [23] or RFID [18] can reduce or mitigate patient identification errors.

Efficacy of a barcode wristband system on the prevention of medical errors indicated that the system can reduce some medical errors by an estimated 12.22% to 57.4% in different hospitals [24], [25], and medication error rate by 56% and by 47% in neonatal intensive care units [26], [27]. A barcode wristband system can help such organizations in saving

roughly $684,000 a year, from just denial of claims [28]. There are various standards and specifications for patient wristbands [15], [16], [29], [30]. The main specifications of a wristband include the size, colour, usability, method of identification, and information presentation while allowing for integrating technologies such as barcodes on the bands.

While wristbands are portable, relatively cheap, and generally easy to use, multiple problems can arise. One study concluded that 1 out of 84,000 barcode scans generated an incorrect patient identifier and as many as three (3) incorrect patient identifiers were outputted from a barcode [31]. Although this is a minimal number, these cases can still be fatal for a patient and costly for health organizations.

2) Palm Vein Pattern Recognition

Palm vein scanning is a widespread method of verifying and authenticating a user [32]. Given that each patient's palm vein pattern is unique and very stable over the person's lifetime, it makes this method the most commonly used successful technology for identifying people [33]. A palm vein scanner uses a near-infrared light wave to capture the user's vein pattern on the palm. In contrast with other recognition methods, palm veins have internal features making it almost impossible to reproduce with fake palms [34].

The stages of palm print authentication include acquiring the palm vein image, enhancement, extraction, matching, and authentication [32]. As for developing a palm vein pattern image, only specific blood flow patterns are considered for the sake of image clarity. The three methods for capturing vascular images are X-Rays, Ultrasonic Images (Ultrasound), and Infrared Imaging. The latter is the preferred method because of its non-invasive contactless, and nonharmful technique. While there are two types of Infrared technologies that can be used, Far-Infrared and Near-Infrared, the latter is used as it is less expensive to operate and is able to capture smaller veins, making it adequate for identification. However, Far-Infrared technology can capture thermal patterns that are unique even to identical twins [35].

While taking into consideration the accuracy of the palm vein scanning method, it is worth noting that this method is more costly when compared to the barcode wristband alternative. This is due to its unique software in addition to the installation and the implementation of the palm scanners. This form of method is also considered to be more intrusive for a patient as it may raise palm image storage security concerns. However, when compared to the fingerprint or face recognition methods, the palm vein scanners are favorable within this regard. Another issue worth considering is the matter of hygiene as when comparing methods, a noncontact method would be ideal, examples of this include barcode scanning and face recognition.

3) Ocular-based Identification

Two types of ocular-based identification technologies used to identify a person uniquely are iris and retinal scanning. The retina is the thin tissue located at the back of the eyeball, containing cells sensitive to light. It is composed of a complex structure of capillaries that supply the retina with blood and therefore, every person's retina is unique. Similar to palm vein pattern recognition, a retinal scan would map a person's retina's unique patterns. The iris is a thin circular structure behind the cornea of the eye, which is responsible for controlling the size of the pupils and, therefore, the amount of light reaching the retina. The complexity of the retina patterns makes it unique for every person. Unlike iris or palm vein scanning, retinal scanning uses camera technology with little infrared illumination to capture the retina's intricate structures' images.

Iris recognition method would be ideal in a health organization environment as it does not require proximity to a camera for a successful scan and uses safer low-energy infrared lighting. Moreover, retina scan accuracy may be affected by certain diseases [36] and iris scanning proved to be the most secure patient identification method in UCSD's Moore Cancer Center when implemented [37].

4) Face Recognition

Face recognition can be described as determining the identity of an individual based on the person's facial features. The challenge of facial recognition in its simplest form involves comparing two face images and deciphering if they are of the same person [38]. A more significant challenge arises when faces exhibit changes in appearance due to make-up, facial hair, and accessories, such as jewellery.

The process of identifying a face through a face recognition system is similar to that of iris recognition. The steps involved include acquiring the face image, the face detection, recognition, and identification [39]. During the face detection phase, an algorithm is used to do corrections, skin segmentation, and facial feature extraction from the digital face image. One of these algorithms is the Viola-Jones Algorithm, which is considered the first-ever real-time face detection system [40]. In the next stage of face recognition, the modified face image from the previous phase is classified to identify the person from a database. Different algorithms, which include FeedForward Neural Network (FFNN) [39], and Local Binary Pattern (LBP) [41] are used here as well.

One implementation of facial recognition with Microsoft Kinect v2 sensor for patient verification proved to be over 96% accurate [5]. However, each scan took around thirty (30) seconds to complete, a time frame that is unsatisfactory for a healthcare environment, but this can be classified as a limitation to the technology used, Microsoft Kinect v2, as other studies showed promising results in terms of performance, with time reduced to 100ms with the same level of accuracy [27][28].

C. Security and Privacy

The security and privacy areas in patient identification are habitually overlooked [29]. Privacy is also a significant concern for the patients themselves [46], and implementing a biometric system for improving patient identification accuracy is known to impose more privacy concerns for the patient [47].

1) Health and Data Breaches

According to a report issued by McAfee [48], a stolen health record would generally sell more than financial data on the black market. This is mainly because health data does not have that many established markets like financial data. Another study conducted by Infosec Institute (2015), shows that there was a 73% increase in cyberattacks between 2013 and 2014 targeted to healthcare organizations and that the average cost of a stolen health record amounted to $363 on the black market compared to $1 - $2 of the stolen credit card information. Health data breaches tripled in a year between 2017 and 2018 and there were over 15 million patient records breached in 2018 in the United States [49].

One of the most common causes of insider-related breaches is family member snooping [49], that is, healthcare workers spying on their family members. This cause amounted to around 67% of the breach cases, while the second most common type of breach was snooping on their co-workers, amounting to approximately 15% of the violations. Insiders, which are the healthcare workers, are also more likely to commit another breach after their first violation, as 51% of the offences are repeated.

2) Privacy

Storing and processing patients' personal and sensitive data calls for strict privacy protection measures to minimize patient privacy issues as much as possible. Biometrics privacy can be interlinked with personal privacy, given that our biometric information can uniquely identify us [50]. Various studies address different patient privacy concerns and implications [32][36]. In some cases where biometric technology is in place, patients refused to be subject to such technology due to privacy and confidentiality concerns [12]. Some biometric technologies proved to have a high acceptability rate, such as face recognition and voice recognition [5]. In contrast, others, such as iris and retina scanning [52], had a lower acceptability rate. Other studies however showed that biometric technologies are less or non-invasive than traditional methods of identification [5].

While there are no legislations covering the usage of biometric identification systems [53], and yet the right of privacy is considered a fundamental human right [54], safeguards must be set down for every step, from collection to retention of the data collected. Individuals must be given rights to access, correct and delete their data [50]. Furthermore, individuals should be assigned the ability to opt out, so biometric technologies should not be the only implementation for identification.

3. Security

Biometric technologies can help in identifying patients accurately and provide the right authorization and authentication or verification for accessing and amending medical records [38], [55]. The user asserts an identity for confirmation, and the biometric system confirms if the assertion is genuine. This process is generally used to prevent unauthorized access to a system or services. Verification can be explained formally using (1), where, given a claimed identity I and a query feature set x^A, the decision if (I, x^A) belongs to the 'genuine' or 'impostor' class needs to be taken. If x_I^E is the stored template that corresponds to the identity I, x^A is compared with x_I^E and a score s is matched, which measures the similarity between $x^A$and x^E, and η would be a predefined threshold.

$$(I, x^A) \in \begin{cases} genuine, \ if \ s \geq \eta, \\ impostor, if \ s < \eta, \end{cases} \quad (1)$$

However, biometric solutions can have their security flaws as well [41][42]. The biometric system's integrity is determined by its ability to guarantee non-repudiable authentication, that is, ensuring that a user who accesses a specific resource cannot later deny in using it. There are four major classes of security threats to biometric systems [6][26] and these are Denial of Service (DoS), Intrusion, Repudiation and Function Creep. Although it is much harder for an impostor to forge biometric traits than hacking traditional passwords, there are studies suggesting the use of multimodal biometric systems where multiple types of biometric features would be measured and compared, for example, fingerprints and face, for better accuracy [43][44].

The goal of this paper is to provide a proof of concept of the most favoured method of biometric patient identification determined through the methodology and evaluate its results against an already established dataset. Limitations and possible improvements are then suggested.

III. METHODOLOGY

A questionnaire was developed and distributed to professional healthcare participants using purposeful sampling, and its results are analysed. Consequently, requirements are determined, documented and validated using a House of Quality matrix and system designs are proposed.

A. Research Instrument

The questionnaire developed and conducted was sectioned into four (4) main sections:

- **Background Information** - gathering brief, non-personal information about the stakeholder, including their profession, roles, and practical experience.
- **The Problem** - capturing the stakeholder's awareness of patient misidentification and its consequences, globally and in the organization in which they practice in.
- **Their Process of Identifying a Patient in their Organization** – gathering information about the current process that health professionals use to identify patients. They were asked to explain the process briefly and what identifiers are used and at what point. They were also asked of awareness of any of the patient identification methods mentioned

earlier in this study and which of them are used in their organization, if any. Finally, they were asked to provide feedback on their current patient identification method, and if they think that it can be improved and on what aspects, such as accuracy, security and cost.

- **The Solution(s)** - participants were asked which patient identification methods they would implement in their organization, how would they prioritize them and why. They were also invited to prioritize the characteristics and the concerns of a biometric patient identification system in terms of security, accuracy, and efficiency.

B. Participants

Participants chosen that successfully answered all the questions which were provided to them amounted to nine (9), and these were staff nurses (2), an Accident and Emergency (A&E) nurse, a doctor, a general practitioner (GP), a urology surgeon, physiotherapists (2), and a speech-language pathologist. All the participants work in local health organizations in Malta. The GP owns, manages, and works in a small private healthcare clinic. The nurses, the doctor, and the urology surgeon work in a national hospital, while the physiotherapists and the speech-language pathologist work in smaller private healthcare organizations.

C. Results Analysis

All the respondents think that their current patient identification system works moderately well (67%) or very well (33%) (Fig. 2). Hence, participants were also asked to identify the vital positive characteristics of their current patient identification system, and these included the cost, where 58% rated it as very well, followed by ease of use and efficiency (17%), and patient's comfort in using it, where 30% of the participants classified it as very well, as shown in Figure 1. Security was the least rated, with 33% rating it as just slightly well. 25% of the respondents classified security as an aspect that needs to be improved in their current system, along with accuracy. Moreover, 89% of the participants said that, currently, it takes less than 15 seconds to identify a patient, with 33% of them stating that it even takes less than 5 seconds. Therefore, essential requirements that needed to remain there are the system's cost, ease of use, patient's comfort in using it, and efficiency (processing speed). On the other hand, other aspects that require improvements are security and accuracy.

D. Requirements

One of the most commonly used methods to achieve a standard view of the relationship between customer requirements and product design is Quality Function Deployment (QFD) [60]. QFD is a product development methodology that gives importance to the customer's opinions throughout the development process. QFD was used in this study to determine the list of important requirements for the proposed system. Customer importance ratings for system requirements were calculated based on the results obtained

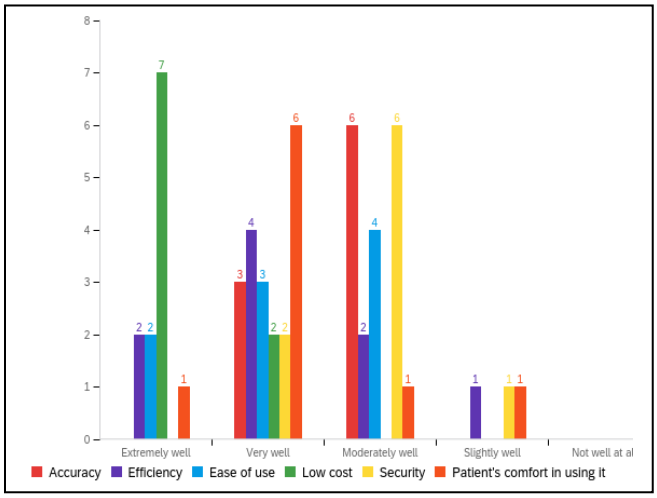

Figure 2. Question results for ranking aspects of the system

from the questionnaire distributed to health professionals in the order of Accuracy, Efficiency, Security, Ease of Use, Cost and Patient's Comfort. On the other hand, the requirements concluded from the previous section were listed on the other side of the matrix. The conditions that scored the highest importance ratings were found to be *Cost*, *Use of Secondary Identification Methods*, *Accuracy*, *Availability*, and *The Use of Alternative Non-Biometric Identification Methods*.

With the cost being the topmost essential requirement for the customer, any negative correlations related to this requirement should be addressed and ideally eliminated as soon as possible. Therefore, alternative non-biometric identification methods should be kept to a minimum and only used in cases where the patient refuses to use other biometric methods, for example. Patients will most probably opt for these alternative methods if they have trust concerns about the system, and hence the importance of *Transparency*. Each customer should be as transparent as possible to the patients about the biometric system, ensuring no physical harm will be done and securing their data safety while pointing out the benefits of such techniques for their own good. We must remember that using alternative non-biometric systems may negatively impact user training, the effort of operating the system, and identification accuracy.

IV. Design

High-level and low-level designs of the system and integration with the possible current systems are proposed. Furthermore, designs of the proposed mobile application are also portrayed together with data and process flows. Taking Systems Theory into perspective, the proposed system would have biometric information as an input and after biometric processing and communication with the Patient Medical Record System (MRS) or Database, outputs the patient information.

For patient identification, the app user needs to be authorised and authenticated. The app should display multiple authentication choices, including but not limited to Face

Recognition, Fingerprint Recognition, or a user account. Data collected at this stage is transferred securely to an internal API where it is processed. Through in-house or third-party APIs, if needed, roles and permissions are determined and set, and the user is then allowed to proceed and identify a patient on the app.

Provided the user is authenticated and authorized on the mobile application, the user can identify a patient, which has already been registered before, that is, the patient's biometric data required for identification has been securely stored on a database or service. After the patient has given consent and the biometric data is collected, such as a face photo, this data is sent through a secure and encrypted channel, such as HTTPS, to an internal API, which communicates to third party APIs, such as Microsoft Facial Recognition, and handles the identification and the fetching of patient information and medical records if needed to be sent back to the app so that vital patient information can be displayed.

The users can be provided with different options to authenticate themselves (Fig. 4a). Viable options include face or fingerprint recognition or a user account.

a) Face Recognition - A

A similar process used to identify patients through face biometrics can be used here to identify and authorize a user.

b) Fingerprint - B

Most of the modern smartphones are equipped with an inbuilt fingerprint sensor. This may be used to authenticate the user. However, this may require more development effort to implement.

c) User account - C

A user account is also another option, although less preferred since it is more time-consuming to develop and maintain. The integration of Microsoft Azure AD will help in improving performance if Microsoft Face Recognition is used for patient identification.

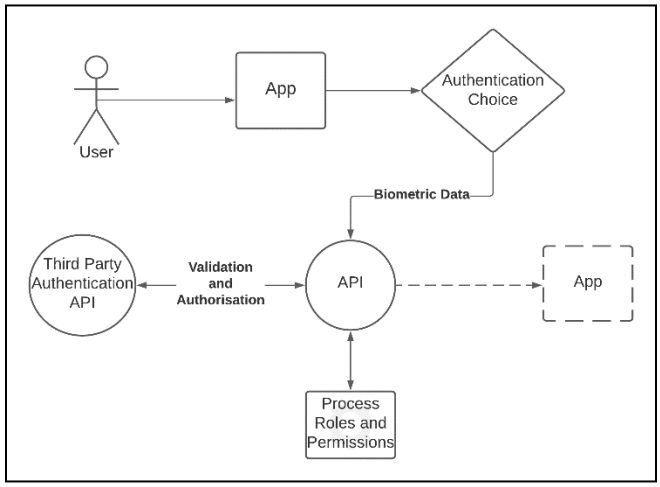

Figure 3. High-Level Authorisation Flow

Figure 3 shows the proposed flow of the mobile application used to identify patients by their face. Adopting two identifiers for identifying a patient, as suggested by the WHO [2], the first stage includes scanning the barcode or QR code printed on the wristband wearing the patient. The app should immediately display the camera preview after successful authentication, for the user to scan the barcode (Fig. 4b). The barcode should be recognised very quickly, and the Patient Identifier stored on the barcode or QR code is captured by the app. Once a barcode or QR code is successfully captured, the user should be prompted to capture the patient's biometric data. For this study, the method of face recognition using Microsoft Face Recognition is showcased. Therefore, the user is asked to take a photo of the patient's face, as straightforward as possible. The user should confirm the image taken for the identification process to initiate.

Upon identification completion, if succeeded, the user is prompted with a pop-up dialog asking to confirm the identification details, to ensure the identification and update biometrics or to scan again (Fig. 4c). Updating biometrics would send the last patient's face photo to Microsoft Face Recognition API and is added to the patient's list of faces for AI training.

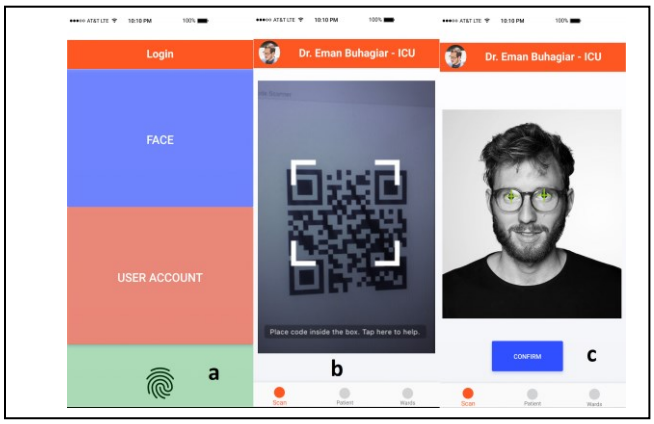

Figure 4. Proposed app system designs. a – Authentication, b – Barcode/QR code scanning, c – Identification confirmation

V. EVALUATION

The primary identification method of face recognition is implemented using Microsoft Cognitive Services and their Face API [61]. There are various reasons for opting for Microsoft Cognitive Services, and these reasons all cohere with the system requirements established earlier. Evaluation of the proposed system was divided into three stages:

A. Applicability

Microsoft Face API is a seamless, secure and an easy to integrate and operate API for face detection, emotion recognition, and identification. Microsoft Face API can be utilised in different scenarios, such as user authentication and counting people in a crowd.

1) Face Detection

Face Detection can detect up to 100 faces in an image along with different attributes such as age, position, smile, emotion, facial hair, makeup and occlusions, such as masks and bandanas when a photo or image URL is passed as a parameter. No images are stored, but only the landmarks are stored, which cannot be used on their own to identify a person.

2) Face Recognition

Face Identification compares face landmarks previously stored on the API from adding faces to a person in a person group or large person group to an input image face landmarks. The API returns a confidence level (1-10) for the user to decide if the prediction is up to the user's expectations or not. The API also accepts a confidence threshold as a parameter to filter out results based on the user's preference for confidence. For example, in identifying patients, a confidence level below 80% (0.8) might not be acceptable, and therefore, a confidence threshold of 0.8 or greater should be passed.

3) Security

One of the most critical concerns addressed by health professionals in the questionnaire conducted for this study is the system's security. Microsoft ensures security by firstly not storing any actual face images on their servers, and secondly by encrypting any data stored using FIPS 140-2 compliant 256-bit AES encryption. FIPS 140-2 is a U.S. Government computer security standard used to approve cryptographic modules [62].

4) Cost

As for the cost of usage, the standard version allows for up to 10 transactions per second, with €0.506 per 1,000 transactions for 5 to 10 million transactions and €0.338 per 1,000 transactions for transactions amounting to more than 100 million. As for storage, €0.009 per 1,000 faces per month is charged. A transaction constitutes an API call, apart from the training calls where a transaction counts for every 1,000 images trained. Table II shows a detailed pricing scheme for Microsoft Face API.

TABLE II. MICROSOFT FACE API PRICING

Version	Transactions	Price
Free	20 per **minute**	30,000 transactions free per month
Standard	10 per **second**	0-1M transactions - €0.844*
		1M-5M transactions - €0.675*
		5M-100M transactions - €0.506*
		100M+ transactions - €0.338*
		€0.009 per 1,000 faces stored per month

5) Limitations

Like all other face recognition methods, there are some limitations that may hinder the system's accuracy. Various face occlusions, such as masks and makeup, or face injuries and ageing, may prevent face recognition algorithms from detecting or identifying a face. While many face recognition technologies cater for occlusions measurement when detecting a face, face masks during the COVID-19 pandemic impacted face recognition algorithms' overall accuracy [63]. Such a situation requires the need for alternative identification methods, such as retina recognition, to be available in the system.

Figure 5. Face image under different lighting conditions

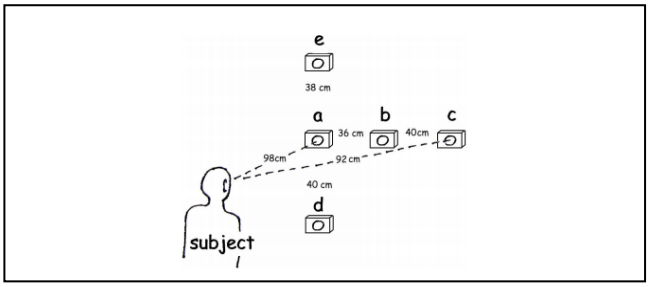

Figure 6. Angles of the camera from which the photos were taken [63]

B. Accuracy Evaluation

A dataset of multiple faces was used to evaluate a person's identification accuracy through Microsoft Face API. The dataset was introduced in an another study [64] to provide more diversity than the existing publicly available datasets regarding lighting, age, and ethnicity. The dataset consists of 3755 faces, totalling to 276 participants in all. Each participant has at least eight (8) face photos, each from a different angle or different lighting (Fig. 5, Fig. 6).

The image filenames have the form of i000qa-fn.jpg, where:

- i is the prefix of all files,
- 000 is the subject identification number,
- q is the lighting type, ranging from q to z,
- a is the camera angle, ranging from a to e,
- f for female or m for male,
- n for no glasses or g for with glasses.

This naming convention was used as wildcards in code during the evaluation process, as explained later on in this sub-chapter. This dataset was chosen to be used in this study as it fits nicely into healthcare scenarios for identifying different patients.

The following 'setup' process was adopted to evaluate the identification accuracy of Microsoft Face API:

1. A large person group with a name 'test' was created, and the returned *largePersonGroupId* was stored, to be used later to identify a face.
2. For each of the subjects in the dataset:

a. The subject was added to the large person group just created, and the identification number was used as the name (for example '000').

b. The face was added to the person using the first image file of the subject.

3. After all subjects are added, the large person group was trained by calling the train API endpoint.

Once all the subjects in the dataset were registered, the following identification process was conducted for each participant:

- The face was detected, and the *faceId* returned was stored.
- The face is identified, passing the *faceId* in the request body and the *largePersonGroupId* captured earlier when creating the group. If identified, a list of potential candidates should be returned, each with a *personId* and a confidence level.
- The person was identified and confirmed by getting the person in the large person group by the *personId* captured in the previous step. The person name and the file identification number were compared, and if these matched, identification was successful.

Figure 7 portraits the identification evaluation flow.

C. Performance Evaluation

The second stage of evaluation ensures that the second most crucial requirement established, efficiency is maintained throughout the identification process. For this, a simple mobile application was developed, simulating a patient's identification using two identifiers, a barcode and a face. Once this is done, the app prompts the user to take a photo of a face, and this is sent to Microsoft Face API upon confirmation for identification. Both the barcode key and the person identified from the API are compared, and if matched, a call to a database is made to fetch the records of the patient. The whole process was timed for efficiency evaluation.

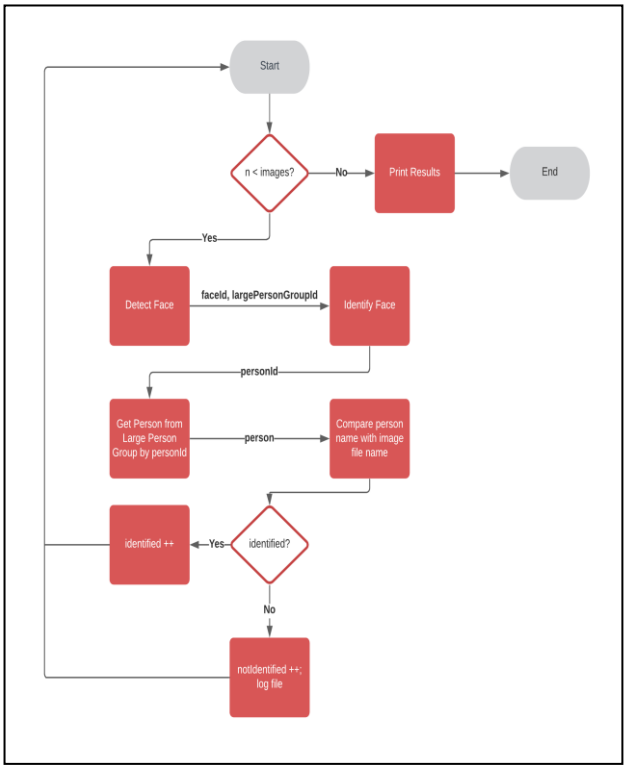

Figure 7. Identification Evaluation Flowchart

VI. Results and Discussion

The results of the previously explained evaluation processes are analysed and discussed in detail. There are specific scenarios where the system performed very well, but there are others in which accuracy was challenged, and possible improvements are suggested for these cases.

A. Accuracy of Face Recognition

There were eight (8) types of datasets that were used to assess the accuracy of the proposed system (Fig. 7). These will be referenced as *a*, *b*, *c*, *d*, *e* and *qa*, *rb*, *sb*. *a* – *e* represent the different angles of the camera from which the photo was taken, while *q*, *r* and *s* represent the amount of light exposed to the face, with $s > r > q$.

The thresholds used for evaluating the accuracy of the system ranged from 0.97 to 0.92. Anything above the threshold of 0.97 resulted in less than 80% accuracy, which is not considered safe enough for such a critical system. On the other hand, any threshold below 0.92 always resulted in 100% accuracy in all scenarios tested.

1) Case 1 – Camera Angles

In the first case, the first set of faces *qa*, that is, photos taken from in front of the person (*a*) and with lighting set *q*, was added to the API and trained. After that, all the other photos from the remaining angles were tested for identification against different thresholds.

As seen in Table III, the accuracy results obtained by training just *qa* were always above 88% for 276 photos. It can be noted that angles *b* and *c* resulted in less accuracy than angles *d* and *e*. Therefore, side angles seem to be less accurate than front angles. Angles *c* and *d* provided the same accuracy results, while angle *d* proved to be the best angle for obtaining accurate results.

TABLE III. CASE 1 RESULTS

Thr. / Sc.	0.97	0.96	0.95	0.94
b	88.04	98.55	99.28	100.00
c	88.04	98.55	99.28	100.00
d	99.28	100.00	100.00	100.00
e	93.48	97.83	98.91	100.00

n = 276

2) Case 2 – Lighting

In the second case, with trained set *qa*, all the other remaining photos with r and s lighting exposed to them were tested for identification with different thresholds.

In this case, accuracy suffered much more when different lighting was used on the person's face. As shown in Table IV, the accuracy went down to 43.96% and 39.56% from 88.04 and above 99% from the previous case. This indicates that lighting has a significant effect on identifying a person from their face, and a less threshold of 0.92 compared to 0.94 had to be used for achieving 100% accuracy on the 91 photos tested. Lighting set *r* performed better than set *s* significantly. Significant changes were also noted when the threshold was changed each time by 0.01, with accuracy changes of more than 30% in some cases.

Since this case resulted in low accuracy results in some scenarios, set *ra* was added to the API and trained, and set *sb* was tested again. The same angle of the previously trained set was used (*a*) for consistency. This was done to note the difference in accuracy and the effectiveness of training. Table IV shows the accuracy results of set *rb* when tested, while sets *qa* and *ra* are trained already.

Accuracy improved significantly for set *sb* when *ra* was added and then trained. With 0.97 as the threshold, accuracy improved by more than 24% and by more than 17% for the 0.96 threshold (Table V). This shows that dataset training provided by Microsoft Face API does improve identification accuracy.

B. Integration Efficiency Test

For this case, a simple mobile application was developed to showcase the use of the proposed system by the users. The app communicates with a custom developed API hosted on Microsoft Azure, which then communicates to Microsoft Face API and a database with records of patients, also hosted on Microsoft Azure. The process took between 5 to 7 seconds when timed in code, with full-bar Wi-Fi connectivity, to detect and identify the face through the API, and to get the patient's allergies and conditions list from a sample database. This result coheres with the efficiency requirement established earlier for identification to take not more than 15 seconds and ideally not more than 5 seconds.

TABLE IV. CASE 2 RESULTS

Thr. / Sc.	0.97	0.96	0.95	0.94	0.93	0.92
rb	43.96	73.63	90.11	96.70	100.00	100.00
sb	39.56	64.84	82.42	93.41	98.54	100.00

n = 91 (photos 000 - 090)

TABLE V. CASE 3 RESULTS

Thr. / Sc	0.97	0.96	0.95	0.94	0.93
sb	64.84	82.42	92.31	96.70	100.00

n = 91 (photos 000 - 090)

VII. CONCLUSION AND FUTURE WORK

We recognise that patient misidentification is a known global problem in various healthcare organizations, and it can lead to further complications to the patients and the organizations themselves. While biometric technology is applied in multiple sectors, such as authentication and security, payroll, and banking, there are fewer studies on the application of biometric technology for positive patient identification. This study conducted a questionnaire among different health professionals to determine the top concerns for implementing a biometric system in healthcare. These included security, accuracy, cost, and patient cooperation. While most of the participants were aware of some of the biometric methods for patient identification, none of them has ever made use of any of them but would consider in doing so, given a better accuracy rate and robust security. The quantitative analysis obtained from the questionnaire helped in determining and prioritising the proposed system requirements, although a further study can be conducted with a more extensive questionnaire and more participants.

For the proof of concept, this study evaluated the implementation of face recognition biometric technology for identifying patients, as this was the most preferred biometric

method chosen by the questionnaire participants. Microsoft Face API was used as the third-party provider for identifying faces, and the proposed system was evaluated against its accuracy and efficiency, among other requirements determined. While results were promising with over 80% accuracy in most cases, this technology seemed to lack in identifying faces with occlusions, such as different lighting. When more than one face photo from different angles and different lighting are registered and trained, accuracy was improved significantly.

As for future works, the system needs to be evaluated against a larger dataset with a larger variety of face occlusions to mimic real-case scenarios in health organizations. Further studies on the security aspects of the system are also important to be conducted to minimise the risks of malicious attacks on the system and gain more confidence from the system users.

REFERENCES

[1] E. Buhagiar and C. De Raffaele, "An Effective Biometric Patient Identification System for Health Organizations," in eTELEMED 2021, The Thirteenth International Conference on eHealth, Telemedicine, and Social Medicine, 2021, pp. 62–70, doi: 978-1-61208-872-3.

[2] E. Buhagiar, "Implementing an Effective Biometric Patient Identification System in a Health Organization," Middlesex University Malta, 2021.

[3] S. Kelly, "The patient misidentification crisis," Health Manag. Technol., pp. 12–14, 2016.

[4] WHO, "WHO calls for urgent action to reduce patient harm in healthcare," Saudi Med. J., vol. 40, no. 10, pp. 1075–1076, 2019, Accessed: Apr. 18, 2021. [Online]. Available: https://www.who.int/news/item/13-09-2019-who-calls-for-urgent-action-to-reduce-patient-harm-in-healthcare.

[5] G. Lippi, L. Chiozza, C. Mattiuzzi, and M. Plebani, "Patient and Sample Identification. out of the Maze?," J. Med. Biochem., vol. 36, no. 2, pp. 107–112, 2017, doi: 10.1515/jomb-2017-0003.

[6] M. Jonas, S. Solangasenathirajan, and D. Hett, "Patient Identification, A Review of the Use of Biometrics in the ICU," 2014, pp. 679–688.

[7] T. H. Tase, E. R. S. Quadrado, and D. M. R. Tronchin, "Evaluation of the risk of misidentification of women in a public maternity hospital," Rev. Bras. Enferm., vol. 71, no. 1, pp. 120–125, 2018, doi: 10.1590/0034-7167-2017-0134.

[8] NHCAA, "The Challenge of Health Care Fraud - The NHCAA," 2015. https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx (accessed Aug. 04, 2020).

[9] Ponemon Institute, "Fifth Annual Study on Medical Identity Theft," no. February, 2015, [Online]. Available: http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

[10] ECRI Institute, "Patient identification errors," 2016. doi: 10.1016/j.enfcli.2011.07.006.

[11] M. A. Yahiro, "Biometrics Solutions in e-Health Security," Spine (Phila. Pa. 1976)., vol. 19, no. Supplement, pp. 2274S-2278S, 2015, doi: 10.1097/00007632-199410151-00004.

[12] N. Anne et al., "Feasibility and acceptability of an iris biometric system for unique patient identification in routine HIV services in Kenya," Int. J. Med. Inform., vol. 133, no. September 2019, p. 104006, 2020, doi: 10.1016/j.ijmedinf.2019.104006.

[13] M. A. McClellan, "Duplicate medical records: a survey of Twin Cities healthcare organizations.," AMIA Annu. Symp. Proc., vol. 2009, pp. 421–425, 2009.

[14] M. Härkänen, M. Tiainen, and K. Haatainen, "Wrong-patient incidents during medication administrations," Journal of Clinical Nursing, vol. 27, no. 3–4. pp. 715–724, 2018, doi: 10.1111/jocn.14021.

[15] S. Allworth, P. Lapsley, J. Kelly, D. Martin, and V. J. Kelly, "Technology Solutions to Patient Misidentification Report of Review Final," no. October, 2008.

[16] Bay of Plenty District Health Board, "Patient Identifiction Standards," p. 50061, 2016.

[17] World Health Organization, "Patient Identification," J. Nurs. Care Qual., vol. 1, no. 2, 2007, doi: 10.1097/00001786-200301000-00010.

[18] A. Aguilar, W. Van Der Putten, and G. Maguire, "Positive Patient Identification using RFID and Wireless Networks," Undefined, 2006.

[19] The Joint Comission, "National Patient Safety Goals Effective July 2020 for the Hospital Program Goal," Jt. Com., no. July, p. 14, 2020, [Online]. Available: https://www.jointcommission.org/-/media/tjc/documents/standards/national-patient-safety-goals/2020/npsg_chapter_hap_jul2020.pdf.

[20] S. Kelly, "The patient misidentifi cation crisis," Health Manag. Technol., pp. 12–14, 2016.

[21] P. D. Hain et al., "An intervention to decrease patient identification band errors in a Children's Hospital," Qual. Saf. Heal. Care, vol. 19, no. 3, pp. 244–247, 2010, doi: 10.1136/qshc.2008.030288.

[22] S. W. Renner, "Wristband Errors in Small Hospitals," vol. 28, no. 3, 1997.

[23] L. V. Hoffmeister and G. M. S. S. De Moura, "Use of identification wristbands among patients receiving inpatient treatment in a teaching hospital," Rev. Lat. Am. Enfermagem, vol. 23, no. 1, pp. 36–43, 2015, doi: 10.1590/0104-1169.0144.2522.

[24] M. Khammarnia, A. Kassani, and M. Eslahi, "The efficacy of patients' wristband bar-code on prevention of medical errors: A meta-analysis study," Appl. Clin. Inform., vol. 6, no. 4, pp. 716–727, 2015, doi: 10.4338/ACI-2015-06-R-0077.

[25] B. Wegerbauer, “Can barcoded wristbands improve patient safety ?,” no. January, pp. 1–5, 2007.

[26] N. Dwibedi et al., “Effect of bar-code-assisted medication administration on nurses’ activities in an intensive care unit: A time-motion study,” Am. J. Heal. Pharm., vol. 68, no. 11, pp. 1026–1031, 2011, doi: 10.2146/ajhp100382.

[27] F. H. Morriss et al., “Effectiveness of a Barcode Medication Administration System in Reducing Preventable Adverse Drug Events in a Neonatal Intensive Care Unit: A Prospective Cohort Study,” J. Pediatr., vol. 154, no. 3, 2009, doi: 10.1016/j.jpeds.2008.08.025.

[28] Ponemon Institute LLC, “2016 National Patient Misidentification Report Independently conducted by Ponemon Institute LLC Sponsored by Imprivata,” no. December, 2016.

[29] Australian Commission for Safety and Quality in Health Care, “Specifications for a standard patient identification band,” pp. 3–4, 2007, [Online]. Available: http://www.safetyandquality.gov.au/wp-content/uploads/2012/02/FactSheet-PatID-Band.pdf.

[30] The Joint Commission, “Patient identification policy,” Patient Saf. Solut., vol. 1, no. May, pp. 1–26, 2011.

[31] M. L. Snyder, A. Carter, K. Jenkins, and C. R. Fantz, “Patient misidentifications caused by errors in standard bar code technology,” Clin. Chem., vol. 56, no. 10, pp. 1554–1560, 2010, doi: 10.1373/clinchem.2010.150094.

[32] O. Akinsowon, B. Alese, and O. Adewale, “Infrared Capture of Palm-Vein Blood Vessel Patterns for Human Authentication,” J. Internet Technol. Secur. Trans., vol. 3, no. 1, pp. 203–209, 2014, doi: 10.20533/jitst.2046.3723.2014.0027.

[33] Imprivata, “Improving Patient Care with Positive Patient Identification - White Papers - HealthITAnalytics,” 2015.

[34] H. Setiawan and E. M. Yuniarno, “Biometric Recognition Based on Palm Vein Image Using Learning Vector Quantization,” Proc. 2017 5th Int. Conf. Instrumentation, Commun. Inf. Technol. Biomed. Eng. ICICI-BME 2017, no. June, pp. 95–99, 2018, doi: 10.1109/ICICI-BME.2017.8537770.

[35] D. C.Lakshmi, A.Kandaswamy, and C.Vimal, “Protection of Patient Identity and Privacy Using Vascular Biometrics,” Int. J. Secur., vol. 4, 2010.

[36] M. D. Abràmoff, M. K. Garvin, and M. Sonka, “Retinal Imaging and Image Analysis,” IEEE Rev Biomed Eng, pp. 169–208, 2010, doi: 10.1109/RBME.2010.2084567.Retinal.

[37] B. N. Haile, “The Eyes Have It : Iris Biometrics Safely Identify UCSD Patients for Radiation Oncology Treatment,” 2010.

[38] A. K. Jain, A. A. Ross, and K. Nandakumar, Introduction to Biometrics. Boston, MA: Springer US, 2011.

[39] A. Gurel, C., & Erden, “Design of a Face Recognition System,” 15th Int. Conf. Mach. Des. Prod., vol. 1, no. 2012, 2012.

[40] Y.-Q. Wang, “An Analysis of the Viola-Jones Face Detection Algorithm,” Image Process. Line, vol. 4, pp. 128–148, 2014, doi: 10.5201/ipol.2014.104.

[41] S. M. Bah and F. Ming, “An improved face recognition algorithm and its application in attendance management system,” Array, vol. 5, no. November 2019, p. 100014, 2020, doi: 10.1016/j.array.2019.100014.

[42] R. Ranjan et al., “A Fast and Accurate System for Face Detection, Identification, and Verification,” IEEE Trans. Biometrics, Behav. Identity Sci., vol. 1, no. 2, pp. 82–96, 2019, doi: 10.1109/tbiom.2019.2908436.

[43] S. Anila and N. Devarajan, “Simple and Fast Face Detection System Based on Edges,” Researchgate.Net, no. May, 2010, [Online]. Available: https://www.researchgate.net/profile/Anila_Satish/publication/225292501_Simple_and_Fast_Face_Detection_System_Based_on_Edges/links/09e414fd75a23d2c1b000000.pdf.

[44] Hembroff, G. C., Wang, X., and Muftic, S., “Providing an Additional Factor for Patient Identification Based on Digital Fingerprint,” *2nd {USENIX} Workshop on Health Security and Privacy (HealthSec 11)*, 2011.

[45] E. B. Heinlein, “Medical records security,” Comput. Secur., vol. 15, no. 2, pp. 100–102, 1996, doi: 10.1016/0167-4048(96)89322-9.

[46] P. Houston, “Research Responses to Patient Privacy Concerns,” 2017.

[47] C. L. Parks and K. L. Monson, “Automated Facial Recognition of Computed Tomography-Derived Facial Images: Patient Privacy Implications,” J. Digit. Imaging, vol. 30, no. 2, pp. 204–214, 2017, doi: 10.1007/s10278-016-9932-7.

[48] C. Beek, C. McFarland, and R. Samani, “Health Warning Report,” 2018.

[49] Protenus Inc., “Protenus 2019 Breach Barometer,” pp. 1–21, 2019, [Online]. Available: https://email.protenus.com/hubfs/Breach_Barometer/2018/2019 Breach Barometer Annual Report.pdf.

[50] C. U. Ebelogu, O. Adelaiye, and F. Silas, “Privacy Concerns in Biometrics,” no. July, 2019.

[51] D. Birnbaum, K. Gretsinger, M. G. Antonio, E. Loewen, and P. Lacroix, “Revisiting public health informatics: patient privacy concerns,” Int. J. Heal. Gov., vol. 23, no. 2, pp. 149–159, 2018, doi: 10.1108/IJHG-11-2017-0058.

[52] N. Dahiya and C. Kant, “Biometrics security concerns,” Proc. - 2012 2nd Int. Conf. Adv. Comput. Commun. Technol. ACCT 2012, pp. 297–302, 2012, doi: 10.1109/ACCT.2012.36.

[53] R. Gellman, “Privacy and Biometric ID Systems : An Approach Using Fair Information CGD Policy Paper 028

August 2013," Cent. Glob. Dev., no. August, 2013.

[54] A. Puri, "Privacy is a fundamental human right," pp. 1–3, 2013.

[55] A. Dandashi and W. Karam, "Biometrics security and experiments on face recognition algorithms," 2012 IEEE Symp. Comput. Intell. Secur. Def. Appl. CISDA 2012, 2012, doi: 10.1109/CISDA.2012.6291532.

[56] S. O. Olatinwo, O. Shoewu, and O. O. Omitola, "Iris Recognition Technology : Implementation , Application , and Security," Pacific J. Sci. Technol., vol. 14, no. 2, pp. 228–233, 2013.

[57] J. C. Mazura, K. Juluru, J. J. Chen, T. A. Morgan, M. John, and E. L. Siegel, "Facial recognition software success rates for the identification of 3D surface reconstructed facial images: Implications for patient privacy and security," J. Digit. Imaging, vol. 25, no. 3, pp. 347–351, 2012, doi: 10.1007/s10278-011-9429-3.

[58] K. Sasidhar, V. L. Kakulapati, K. Ramakrishna, and K. KailasaRao, "Multimodal Biometric Systems - Study to Improve Accuracy and Performance," Int. J. Comput. Sci. Eng. Surv., vol. 1, no. 2, pp. 54–61, 2010, doi: 10.5121/ijcses.2010.1205.

[59] W. Dahea, "Multimodal biometric system : A review Multimodal biometric system : A review," no. November, pp. 25–31, 2018, doi: 10.13140/RG.2.2.34056.65287.

[60] R. J. Hauser, A. Griffin, L. R. Klein, M. G. Katz, and P. S. Gaskin, "Quality function deployment," 2010, doi: 10.4271/870272.

[61] Microsoft, "Facial Recognition | Microsoft Azure," 2020. https://azure.microsoft.com/en-us/services/cognitive-services/face/ (accessed Dec. 08, 2020).

[62] FIPS 140-2, "FIPS 140-2 Change Notices (12-03-2002) Federal Information Processing Standards Publication (Supercedes FIPS PUB 140-1," FIPS PUB 140-2, 2001.

[63] M. Ngan, P. Grother, and K. Hanaoka, "Ongoing Face Recognition Vendor Test (FRVT) - Part 6A: Face recognition accuracy with masks using pre-COVID-19 algorithms," 2020.

[64] S. Milborrow, J. Morkel, and F. Nicolls, "The MUCT Landmarked Face Database," Proc. Pattern Recognit. Assoc. South Africa, pp. 32–34, 2010.