UTM UNIVERSITI TEKNOLOGI MALAYSIA FACULTY OF COMPUTING UTM Johor Bahru

SECP1513: Technology Information System

Semester 01, 2024/2025

DESIGN THINKING PROJECT PROPOSAL

EYEDENTITY

PREPARED FOR: DR. MUHAMMAD IQBAL TARIQ BIN IDRIS

PREPARED BY: TECHTICIANS

Name	Matric No.
Kavivarthan A/L Mannivanan	A24CS0093
Muhammad Firdaus bin Md Lani	A24CS0132
Lim Bei En	A24CS5080
Phang Souh Xin	A24CS5051

Clients Name:

1. Koh Zi Qian (Student at UTM)
2. Nur Ilina binti Zikri (Educator at SM Imtiaz Ulul Albab Melaka)

Table of Contents

1. Introduction

Need (N)	● To replace the current student matric card since it presents several challenges in university environments. ● For instance, matric cards can easily be stolen. ● This increases the risk of unauthorized access and misuse of other's matric cards. ● Especially that matric cards serve various purposes, including access to facilities and functioning as debit cards for financial transactions.
Approach (A)	● Our proposed system, EYEDENTITY, introduces Iris scanning as the biometric that replaces the traditional card scanning. ● For registration, new users are required to scan their iris with the camera. Next, they will be required to scan their QR code from UTM Smart to link their personal information. ● The system will be installed at facilities that require access such as university entrance, laboratories and libraries. It ensures a secure and controlled environment for academic and research activities. ● Implement a dual-lane system at university entrance. This dual-lane system enhances security guard work efficiency and streamlines access management. ● Outside visitors must record their ID information at guardhouses to obtain a visitor pass and they are required to use a different lane.

Benefit (B)	● Iris patterns are unique for each individual. Thus, making it difficult to replicate and eliminate the risks of stolen matric cards. ● Provide convenience to students as they no longer need to carry a separate card which can prevent forgetfulness or loss. ● Only authorized individuals are granted access to enter permitted facilities. It reduces risks of unauthorized access and misuse of resources. ● The dual-lane system for access management lightens the workload of security personnel and reduces conjunction at university entry points.
Competitor (C)	● There are several similar biometric-based solutions available in the market such as fingerprint recognition systems and facial recognition systems. ● Fingerprint scanning can be replicated from surfaces and latent prints which will cause vulnerability towards spoofing. ● Facial recognition systems sometimes are less accurate in certain lighting conditions or with people wearing glasses or masks. ● Fingerprint and facial recognition systems pose a common weakness which is lower accuracy and consistency. Both biometrics will change overtime due to aging or injuries, affecting the accuracy of the readings.

2.1 Existing Systems

2.1.1 Current System

- Manual System: Student Matric Cards / Staff Cards

These cards serve the following **purposes**:

- **Identity Verification**: Students are required to present their physical matric cards at libraries, laboratories, and other specific facilities to gain access.
- **Payment Functionality**: Matric cards can function as debit cards for financial transactions.
- **Facility Access**: Used as a way of access control to allow only authorized staff to enter specific areas.

However, this system has the following **weaknesses**:

- Users often forget to bring or lose their matric cards which can cause inconvenience.
- Physical matric cards can be stolen or misused, leading to unauthorized access and security concerns.
- Physical damage on the card, especially on the chip will cause it to become unreadable by the system.
- The cards require plastics to be produced, which act as environmental waste.

2.1.2 Market-Available Systems

1. Fingerprint Recognition Systems

Strengths: Fingerprint recognition provides security and can be used for access control or payment verification, reducing the need for physical matric cards.

Weaknesses: Fingerprints can be easily copied and forged [3], posing a security risk, and are sensitive to issues like sweat or worn fingerprints.

2. Facial Recognition Systems

Strengths: Unlike passwords or fingerprint scanners, face recognition is contactless and does not require users to touch any device, making it fast and convenient.

Weaknesses: Several factors can degrade the accuracy of face recognition, including occlusion, low resolution, noise, illumination, pose variations, expressions, aging, and plastic surgery. [4]

2.2 Issues or Problems with Existing Systems

1. Security Concerns

- **Physical Matric Cards:**
  - Physical matric cards can be swapped and be replaced with other individual's information [1].
  - This will cause wrong identification when the tampered card is scanned.

- **Fingerprint Recognition Systems:**
  - Fingerprints can be spoofed from external surfaces, making them prone to duplication and unauthorized use.

- **Facial Recognition Systems:**
  - This system has a higher rejection rate when in a diverse or large population.
  - Images or videos of individuals can be spoofed to trick facial recognition systems, leading to unauthorized access.

2. Accuracy and Error Rates

- **Physical Matric Cards:**
    - If the chip on the card is damaged, the information may become unreadable or incorrectly read by the system, it can lead to access failure or incorrect identification.

- **Fingerprint Recognition Systems:**
    - Fingerprint recognition can be affected by sweat, dirt, scars, or fingertip wear, which may result in problems with accurate identification.

- **Facial Recognition Systems:**
    - The accuracy of facial recognition systems can be affected by factors like aging, partial occlusion, illumination, facial expressions, and so on. [4]
    - These factors can lead to misidentification, reducing the reliability of the system.

Table 1: Comparison of existing systems

Features	**Current Matric Card**	**Fingerprint Recognition Systems**	**Face Recognition Systems**	**Iris Recognition Systems** (Proposed System)
Identity Verification	Yes	Yes	Yes	Yes
Biometric Authentication	No	Yes	Yes	Yes
Ease of Use	Moderate	High	High	High
Security	Low	Moderate	Moderate	High
Accuracy	Low	Moderate	Moderate	High
Contactless Operation	No	No	Yes	Yes

3. **Proposed System**

EYEDENTITY, our proposed system, is a system which incorporates Iris scanning as a biometric data in the current attendance recording and security system in universities. The current system involves the use of matric cards for students and access cards for staff. The downside of this implementation is using cards itself. If a user forgets to bring along their card or misplaced it, they will have a hard time entering the university or certain areas. By using EYEDENTITY, it is now hassle free for the user as they now have to just carry themselves and scan their eyes to get entry permission.

Since Iris is a unique feature for each individual, no one can sabotage or manipulate the data involved, making it safer than the current system used [2]. This safety feature allows the use of EYEDENTITY to grant permission to certain individuals to enter specific buildings such as the laboratory and administrative buildings. Besides, by using EYEDENTITY, the use of matric cards and access cards can be avoided, which is cost-effective and reduces the amount of plastic used to create new cards annually.

Functionality

EYEDENTITY consists of two parts, registration and implementation. For registration, users are required to scan their Iris in the scanner attached to the registration scanner. Next, users are required to scan their QR code from UTM Smart to provide their personal information into our registration device in order to link their information with their respective Iris.

Our product, EYEDENTITY, will be placed at the entrance of a specific building or a secured room where users need to scan credentials in order to access them. The system will now process the Iris data and match with the existing data from the system in order to recognise the user and grant permission to enter. Using Iris data makes the system more secure as it is hard to replicate or sabotage as well as the Iris of each individual is unique.

4. References

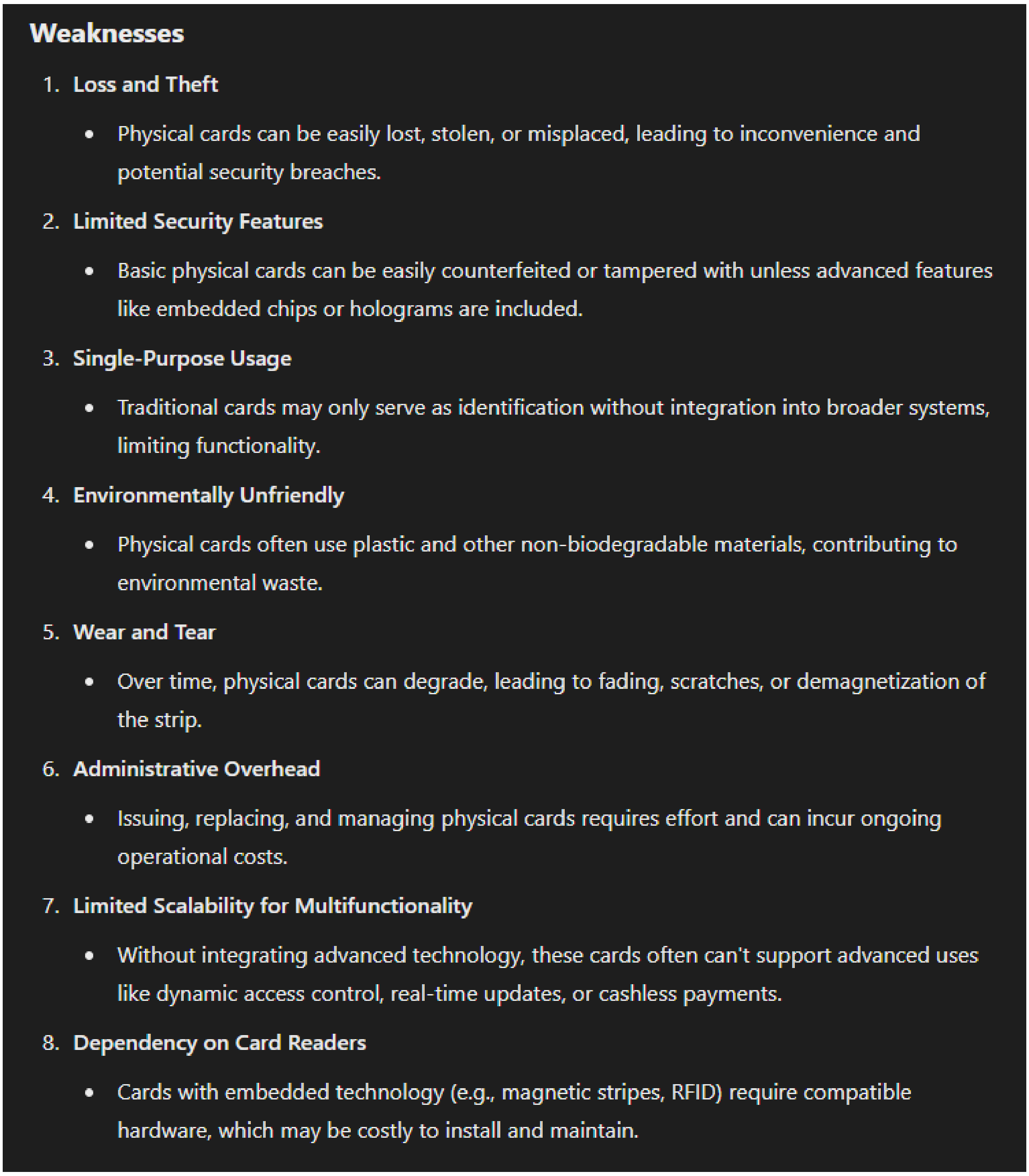
1. Williamson, A., Tsay, L., Kateeb, I. A., & Burton, L. (2013). "Solutions for RFID Smart Tagged Card Security Vulnerabilities." AASRI Procedia, 4, 282–287. https://doi.org/10.1016/j.aasri.2013.10.042

2. Daugman, J., Downing, C., Akande, O. N., & Abikoye, O. C. (2023). Ethnicity and Biometric Uniqueness: Iris Pattern Individuality in a West African database. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2309.06521

3. Kauba, C., Debiasi, L., & Uhl, A. (2020). Enabling fingerprint presentation attacks: fake fingerprint fabrication techniques and recognition performance. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2012.00606

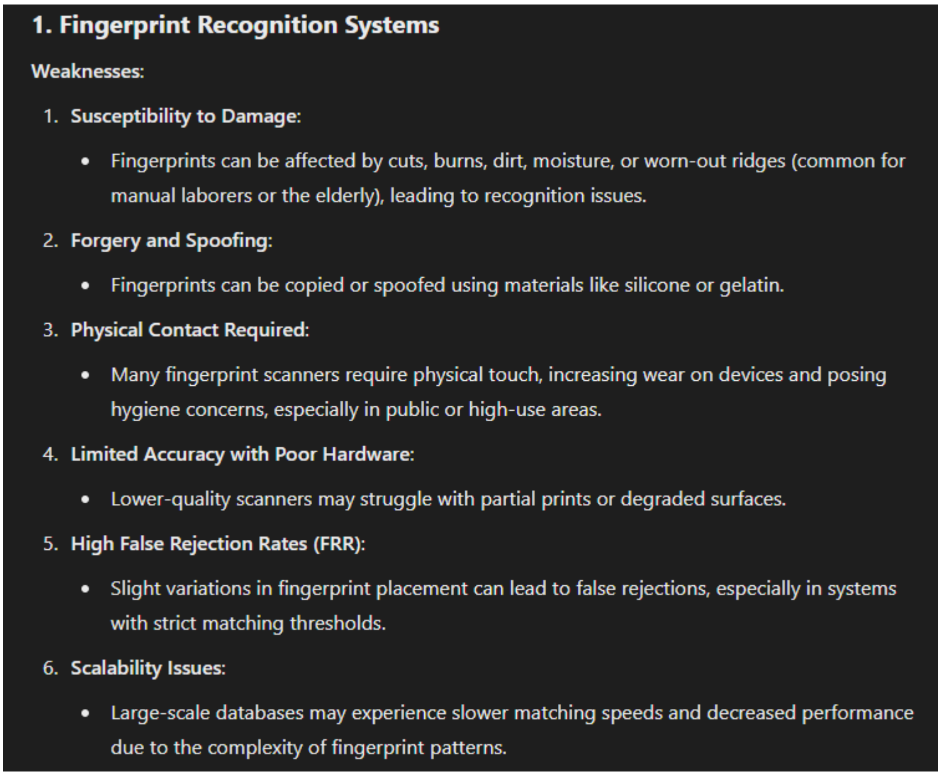
4. Susheela Dahiya. (2020, January). A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy. ResearchGate. https://www.researchgate.net/publication/337446642_A_Comprehensive_Review_on_Face_Recognition_Methods_and_Factors_Affecting_Facial_Recognition_Accuracy

5. Appendices



Weaknesses

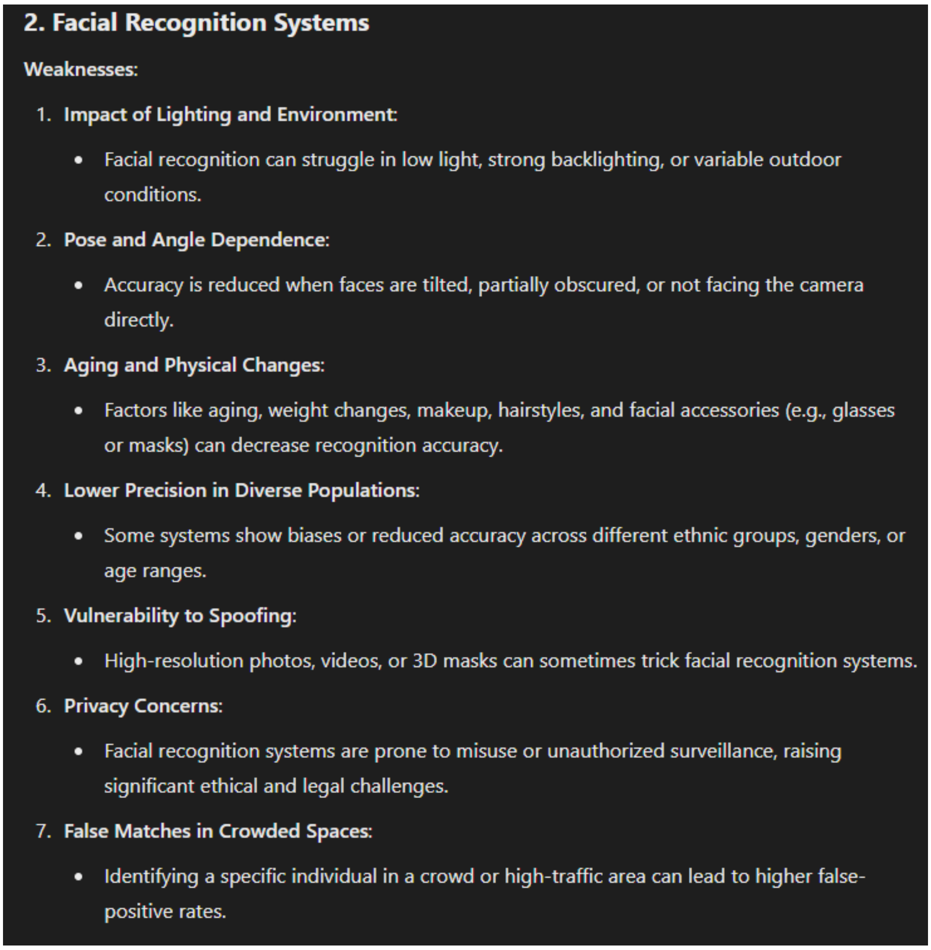
1. **Loss and Theft**
   - Physical cards can be easily lost, stolen, or misplaced, leading to inconvenience and potential security breaches.
2. **Limited Security Features**
   - Basic physical cards can be easily counterfeited or tampered with unless advanced features like embedded chips or holograms are included.
3. **Single-Purpose Usage**
   - Traditional cards may only serve as identification without integration into broader systems, limiting functionality.
4. **Environmentally Unfriendly**
   - Physical cards often use plastic and other non-biodegradable materials, contributing to environmental waste.
5. **Wear and Tear**
   - Over time, physical cards can degrade, leading to fading, scratches, or demagnetization of the strip.
6. **Administrative Overhead**
   - Issuing, replacing, and managing physical cards requires effort and can incur ongoing operational costs.
7. **Limited Scalability for Multifunctionality**
   - Without integrating advanced technology, these cards often can't support advanced uses like dynamic access control, real-time updates, or cashless payments.
8. **Dependency on Card Readers**
   - Cards with embedded technology (e.g., magnetic stripes, RFID) require compatible hardware, which may be costly to install and maintain.



1. Fingerprint Recognition Systems

Weaknesses:

1. **Susceptibility to Damage:**
   - Fingerprints can be affected by cuts, burns, dirt, moisture, or worn-out ridges (common for manual laborers or the elderly), leading to recognition issues.
2. **Forgery and Spoofing:**
   - Fingerprints can be copied or spoofed using materials like silicone or gelatin.
3. **Physical Contact Required:**
   - Many fingerprint scanners require physical touch, increasing wear on devices and posing hygiene concerns, especially in public or high-use areas.
4. **Limited Accuracy with Poor Hardware:**
   - Lower-quality scanners may struggle with partial prints or degraded surfaces.
5. **High False Rejection Rates (FRR):**
   - Slight variations in fingerprint placement can lead to false rejections, especially in systems with strict matching thresholds.
6. **Scalability Issues:**
   - Large-scale databases may experience slower matching speeds and decreased performance due to the complexity of fingerprint patterns.



2. Facial Recognition Systems

Weaknesses:

1. **Impact of Lighting and Environment:**
   - Facial recognition can struggle in low light, strong backlighting, or variable outdoor conditions.
2. **Pose and Angle Dependence:**
   - Accuracy is reduced when faces are tilted, partially obscured, or not facing the camera directly.
3. **Aging and Physical Changes:**
   - Factors like aging, weight changes, makeup, hairstyles, and facial accessories (e.g., glasses or masks) can decrease recognition accuracy.
4. **Lower Precision in Diverse Populations:**
   - Some systems show biases or reduced accuracy across different ethnic groups, genders, or age ranges.
5. **Vulnerability to Spoofing:**
   - High-resolution photos, videos, or 3D masks can sometimes trick facial recognition systems.
6. **Privacy Concerns:**
   - Facial recognition systems are prone to misuse or unauthorized surveillance, raising significant ethical and legal challenges.
7. **False Matches in Crowded Spaces:**
   - Identifying a specific individual in a crowd or high-traffic area can lead to higher false-positive rates.

https://chatgpt.com/share/678fa17b-14f4-800e-b32c-e4ad2910a66e