INTERACTION WITH FRONTEND

INTERACT WITH THE FRONTEND FOR ALL FUNCTIONALITIES

TEAM ID	NM2023TMID04400
PROJECT NAME	BIOMETRIC SECURITY SYSTEM FOR VOTING PLATFORM

EXISTING VOTING EQUIPMENT:

In the recent years, voting equipment which was widely adopted are may divided into five types.

1. **Paper-Based Voting**

- The voter gets a blank ballot and uses a marker to indicate the candidate heintends to vote for.
- However, this process may take a long time to get a hand count under the currentsystem.
- Paper ballot counting and recounting generates endless arguments about whether the marker print crosses inside the square/circle.

2. **Lever Voting Machine**

- Lever machine is peculiar equipment, and each lever is assigned for a corresponding candidate.
- The voter pulls the lever to poll for his favourite candidate.
- This kind of voting machine can count up the ballots automatically.
- Because its interface is not user-friendly enough, giving some training to voters is necessary.
- However, these machines are subject to malfunctions that can invalidate hundreds of votes.

3. **Punch Card**

- The voter uses metallic hole-punch

to punch a hole on the blank ballot.

- It can count votes automatically, but if the voter's perforation is

incomplete, the result is probably determined wrongfully.

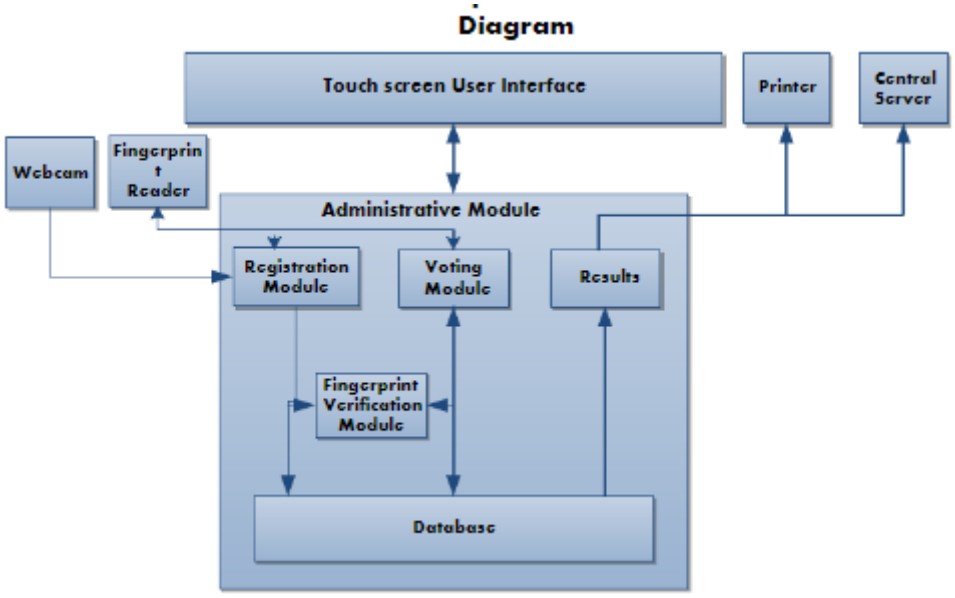
4. **Optical Voting Machine:**

- After each voter fills a circle corresponding to their favourite candidate on the blank ballot, this machine selects the darkest mark on each ballot for the vote then computes the total result.
- This kind of machine counts up ballots rapidly.
- However, if the voter fills over the circle, it will lead to the error result of optical-scan.

5. **Direct Recording Electronic (DRE) Voting Machine:**

- DRE integrates with a keyboard; touch screen, or buttons for the voter press to poll.
- Counting the votes is done very quickly.
- But the DREs are costly and they fail to prove that the vote stored in the machine is really what the voter saw and confirmed on the screen

PROPOSED DESIGN



HARDWARE IMPLEMENTATION: FINGERPRINT SCANNER

Fingerprint Scanner

Scan the Fingerprint image

Fingerprint Enhancement

Minutiea Extraction

Fingerprint Database

- The flow process, above summarizes clearly the implementation of the fingerprint scanner (DigitalPersona) we employed in this project.
- The Process involved is very simple.
- First, the chosen finger for example, the thumb is captured
- and extracted.
- The fingerprint template is then enrolled and store in a database.
- This primary process is done during the registration of eligible voters.
- After that, the chosen finger can be live scan

Facial recognition:

- A face analyzer is software that identifies or confirms a person's identity using their face.
- It works by identifying and measuring facial features in an image.
- Biometric security systems use facial recognition to uniquely identify individuals during user onboarding or logins as well as strengthen user authentication activity.
- Mobile and personal devices also commonly use face analyzer technology for device security.

Benefits of facial recognition:

- Some benefits of face recognition systems are as follows:

Efficient security:

- Facial recognition is a quick and efficient verification system.
- It is faster and more convenient compared to other biometric technologies like fingerprints or retina scans.
- There are also fewer touchpoints in facial recognition compared to entering passwords or PINs.
- It supports multifactor authentication for additional security verification.

Improved accuracy:

- Facial recognition is a more accurate way to identify individuals than simply using a mobile number, email address, mailing address, or IP address.
- For example, most exchange services, from stocks to cryptos, now rely on facial recognition to protect customers and their assets.

Easier integration:

- Face recognition technology is compatible and integrates easily with most security software.
- For example, smartphones with front-facing cameras have built-in support for facial recognition algorithms or software code.

Finge print or Face ID:

- Touch ID is currently more reliable than Face ID for some of the reasons which have been touched upon: Fingerprints are less subject to change than facial appearance.
- Fingerprint recognition doesn't depend on a specific camera angle.
- Fingerprint patterns are more unique than facial patterns

1. Software analyzes photos or videos of a face.
2. Software creates a map of a person's facial features.
3. Facial recognition systems compare the individual's facial signature to its database.
4. The facial recognition system determines whether or not the facial signature is a match to anything in its database.

- Facial recognition uses technology and biometrics — typically through AI — to identify human faces. It maps facial features from a photograph or video and then compares the information with a database of known faces to find a match.
- Facial recognition can help verify a person's identity but also raises privacy issues.