Project Design Phase – part 2

Determine The Requirements

TEAM ID	NM2023TMID04400
PROJECT NAME	BIOMETRIC SECURITY SYSTEM FOR VOTING PLATFORM

User Requirements :

- User shall read and understand the vote title and option.
- User shall make a choice for the vote.
- User shall use fingerprint to authenticate.

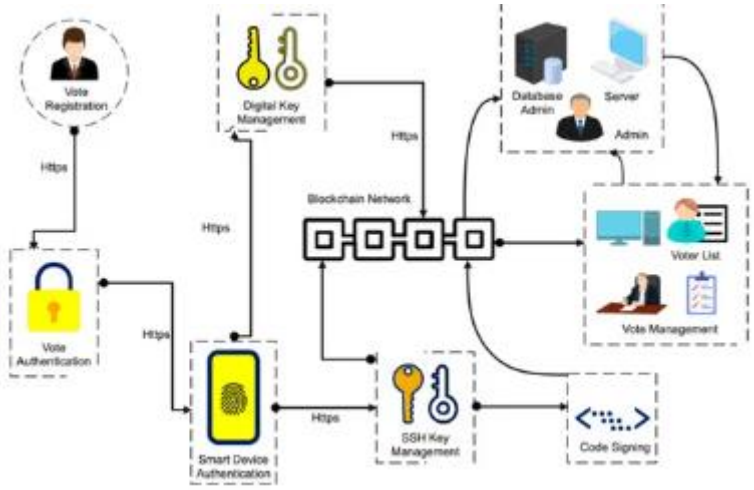
- The functional requirement of this project will be the system need to provide basic function of voting system such as create voting event, vote, calculate result, show result.
- Moreover, the system shall be able to authenticate the user identity when user try to login and fingerprint biometric authentication when submitting vote.
- In addition, the user's phone number is required when register, after that the system should send a one-time code to user's phone by SMS message.
- The non-functional requirement of this system will be the security of the system and the fairness of voting should be secure.
- The system of this project will be using biometric to achieve it. Besides, the mobility is also one of the non-functional requirements of this project.

- This is because the system needs to provide user to use it anywhere and anytime.

- Not only that, but the system should also have good performance to perform any function with only using low usage.

- This can make the application can run on more devices.

Paper Title	Author's Name, Years	Technique Used	Advantage	Disadvantage
Mobile Voting Using Finger Print Authentication	Jumb, Martin, Figer & Rebello 2015	OTP, Minutiae Algorithm	Inexpensive, Less time consuming, Wide acceptance, Better secure	Cannot recognize poor quality fingerprint images
Secured E-voting System Using Two-factor Biometric Authentication	Komatineni & Lingala n.d.	Eigen face recognition algorithm, Minutiae algorithm	Two choices for authentication, Less time consuming	High cost, more data to store
E-Voting System Using Visual Cryptography & Secure Multi-party Computation	Naidu, Kharat, Teckade, Mendhe & Magade n.d.	Secret sharing algorithm, Minutia extraction	More secure	Unavailable when one share of data lost.



Security Requirements :

1. **Voter Authenticity:**

   Ensure that the voter must identify himself (with respect to the registration database) to be entitled to vote. If voting other than at his home precinct, the voter may be asked to show some legal identification document.

2. **Registration:**

   The voter registration shall be done in person only. However, the computerized registration database shall be made available to polling-booths all around the nation.

3. Voter Anonymity:

Ensure that votes must not be associated with voter identity.

4. System Integrity:

Ensure that the system cannot be re-configured during operation.

5. Data Integrity:

Ensure that each vote is recorded as intended and cannot be tampered with in any manner, once recorded (i.e., votes should not be modified, forged or deleted without detection).

6. Secrecy / Privacy:

No one should be able to determine how any individual voted.

7. Non-coercibility and No Vote-selling:

Voters should not be able to prove to others how they voted (which would facilitate vote selling or coercion).

8. Reliability:

Election systems should work robustly, without loss of any votes, even in the face of numerous failures, including failures of voting machines and total loss of network communication. The system shall be developed in a manner that ensures there is no malicious code or bugs.

9. Availability:

Ensure that system is protected against accidental and malicious denial of service attacks. Also, setup redundant communication paths so that availability is ensured.

10. System Disclosability:

The core of the system, especially the vote-casting equipment, shall be opensource, so that it can allow external inspection and auditing.

11. Simplicity:

The system shall be designed to be extremely simple, as complexity is the enemy of security.

12. Testing and Certification:

The system should be tested by experts with respect to all of the security considerations, so that election officials have the confidence that the system meets the necessary criteria.

13. System Accountability:

Ensure that system operations are logged and audited.

14. Personnel Integrity:

Those developing and operating the voting system should have unquestionable records of behavior.

15. Operator Authentication and Control:

Ensure that those operating and administering the system are authenticated and have strictly controlled functional access on the system.

16. Distribution of Authority:

The administrative authority shall not rest with a single entity. The authority shall be distributed among multiple administrators, who are known not to collude among themselves (e.g., different political parties).