PROJECT DESIGN PHASE – PART 1

Date	O4 November 2023
Team ID	NM2023TMID02239
Project Name	Electronic Voting Machine
Maximum Mark	4 Marks

Solution Architecture:

Designing a solution architecture for an electronic voting machine (EVM) involves several key components and considerations to ensure security, reliability, and accessibility. Below is a high-level outline of a typical solution architecture for an EVM system:

1. Voter Registration System:
    - Database to store voter information, including name, address, unique identifier, and other relevant details.
    - User interface for election officials to input and update voter information.
    - Authentication and authorization mechanisms to ensure only eligible voters can cast their votes.
2. Biometric Verification (Optional):
    - Biometric scanners (e.g., fingerprint, iris scan) for voter authentication.
    - Integration with the voter registration system to verify voter identity.
3. Ballot Configuration:
    - Database to store candidate and ballot information.
    - User interface for election administrators to define and configure the ballot.
4. Electronic Voting Machine (EVM):
    - Hardware component with a secure processor, display, input controls, and memory.
    - Software for managing the voting process, displaying the ballot, and recording votes securely.
5. Security Measures:
    - Encryption protocols for securing data in transit and at rest.
    - Secure boot process to ensure the integrity of the EVM software.
    - Tamper-proof seals and physical security measures to protect against physical tampering.
6. Network Infrastructure:

- Secure communication channels between EVMs, central servers, and other components.
- Firewalls, intrusion detection systems, and other security measures to protect against network-based attacks.

7. Central Server:
    - Database to store and manage election-related data, including vote counts and results.
    - Application logic for managing the election process, including vote counting and result aggregation.
    - Access controls and auditing mechanisms to ensure only authorized personnel can access sensitive data.
8. Audit Trail and Logging:
    - Logging mechanism to record all interactions with the system, including votes cast, system events, and administrative actions.
    - Audit trail for verifying the integrity of the election process.
9. Backup and Redundancy:
    - Regular data backups to ensure that no votes are lost in case of hardware failure or other unforeseen events.
    - Redundancy measures to ensure the system remains operational even if individual components fail.
10. Accessibility Features:
    - User interface considerations for accessibility, including options for visually impaired or physically challenged voters.
    - Multilingual support to accommodate diverse voter populations.
11. Testing and Certification:
    - Rigorous testing and certification processes to ensure the EVM system meets all security and reliability requirements.
12. Compliance and Legal Considerations:
    - Adherence to legal and regulatory requirements for electronic voting systems, including privacy, security, and accessibility standards.
13. Training and Support:
    - Training for election officials and support staff on how to use, maintain, and troubleshoot the EVM system.
14. Contingency Planning:

- Plans for handling unforeseen events, such as system failures, power outages, or cyberattacks, to ensure the integrity of the election process.

It's important to note that the specific implementation details may vary based on the jurisdiction, legal requirements, and available technology. Additionally, engaging with security experts, legal advisors, and experienced election officials is crucial in designing a robust and reliable EVM system.