ONLINE VOTING DATABASE REQUIREMENTS

PROJECT DESCRIPTION:

The Online voting database requirement helps to create an efficient database system for managing the online voting system. The Online Voting System project develops a software application designed to manage the details of voters, candidates, elections, and voting results. It is a secure system that stores and retrieves data. The database includes tables for Voters, Candidates, Election Committees, and Political parties. Each table will represent the relevant attributes such as the Voters ID, Voter's name, Candidate's name, Voter's Address, Voter's phone number, Election type, Party name, and Party leader. This system also provides the Results table with attributes Results ID, Party ID, Candidate ID, District ID, and Votes count. The system provides functionalities like adding, updating, and counting records based on various criteria.

The Online Voting System is designed to provide an easy and secure way for voters to register, cast their votes, and view the election results. It helps election officials to manage the election process efficiently and accurately. The Voter Database System is designed to be user-friendly and accessible to all eligible voters. This system can include the user interface, voter eligibility verification, security, results reporting, and technical infrastructure. This system increases the number of voters and makes it easy for people to cast their votes and also improves the accuracy and speed of election results.

ENTITIES REQUIRED FOR THE ONLINE VOTING DATABASE SYSTEM:

Address: The Address entity in the Online Voting database represents the physical location where a voter resides. The purpose of storing the Address entity is to establish the geographical location and jurisdiction of the voter. This information is important for determining eligibility, verifying voter registration, and assigning the appropriate voting district. The list of attributes and their datatypes that can be associated with the Address entity are:

- DistrictID: NUMBER (10)
- Locality: VARCHAR2 (30)
- City: VARCHAR2 (30)

- State: VARCHAR2 (30)
- Zip: VARCHAR2 (30)

Voter_Table: In the context of the Online Voting database project, the "Voter_Table" represents a structured table that stores information about individual voters. It is a collection of records, where each record represents a unique voter and contains various attributes associated with that voter. It serves as a central repository for managing and organizing voter data and also enables efficient management of voter information, and ensures accurate tracking of voting activities within the online voting system. The list of attributes and their datatypes that can be associated with the Voter_Table entity are:

- AADHAAR: CHAR (15)
- FirstName: VARCHAR2 (30)
- LastName: VARCHAR2 (50)
- MotherName: VARCHAR2 (30)
- FatherName: VARCHAR2 (30)
- Sex: CHAR (7)
- Birthday: DATE
- Age: NUMBER (10)
- DistrictID: NUMBER (10)
- Phone: NUMBER (10)

Candidate_Type: In an online voting database, the "Candidate_Type" entity represents the various types or categories of candidates who are eligible to participate in an election. It helps classify candidates and provides relevant information about their candidacy. The Candidate_Type attribute represents the type of candidate as "Presidential candidate" or "Senate candidate". The list of attributes and their datatypes that can be associated with the Candidate_Type entity are:

- CandidateTypeID: NUMBER (10)
- CandidateType: VARCHAR2 (20)

Election_Table: The "Election_Table" entity in an online voting database represents a structured table that stores information about elections. The ElectionType attribute in this entity represents an election, such as a "Presidential election" or a "Local election". The list of attributes and their datatypes that can be associated with the Election_Table entity are:

- ElectionID: NUMBER (10)
- ElectionType: VARCHAR2(20)

Party_Table: The "Party_Table" entity represents a structured table that stores information about political parties participating in elections. It serves as a central repository for managing and organizing data related to different political parties within the online voting system. The Party_Table entity allows for efficient management and tracking of political parties, facilitates the presentation of party information to voters, and enables the association of candidates with their respective parties during elections within the online voting system. The list of attributes and their datatypes that can be associated with the Party_Table entity are:

- PartyID: NUMBER (10)
- PartyName: VARCHAR2(20)
- Symbol: VARCHAR2(20)
- PartyLeader: VARCHAR2(50)

User_Type: In an online voting database, the "User_Type" entity represents the different types or roles of users who interact with the system. It serves as a categorization or classification mechanism for managing and organizing user accounts and permissions within the online voting system. The list of attributes and their datatypes that can be associated with the User_Type entity are:

- UserTypeID: NUMBER (10)
- UserType: VARCHAR2 (20)

Candidate_Table: The "Candidate_Table" entity represents a structured table that stores information about individuals running as candidates in an election. The Candidate_Table entity allows for efficient management and tracking of candidates, facilitates the presentation of candidate information to voters, and enables the association of candidates with specific elections within the online voting system. It plays a crucial role in conducting fair and transparent elections by providing voters with information about the candidates running for office. The list of attributes and their datatypes that can be associated with the Candidate_Table entity are:

- CandidateID: NUMBER (10)
- AADHAAR: CHAR (15)
- CandidateTypeID: NUMBER (10)

- PartyID: NUMBER (10)
- ElectionID: NUMBER (10)
- DistrictID: NUMBER (10)

User_Table: In an online voting database system, the "User_Table" entity represents a structured table that stores information about the users who interact with the system. The User_Table entity allows for efficient management and authentication of users within the online voting system. It enables user registration, login, and access control mechanisms, ensuring that users are properly identified and authenticated. The list of attributes and their datatypes that can be associated with the User_Table entity are:

- VoterID: NUMBER (10)
- Def_Password: VARCHAR2 (50)
- isActive: VARCHAR2 (10)
- AADHAAR: CHAR (15)
- UserTypeID: NUMBER (10)

Vote_Table: The "Vote_Table" entity represents a structured table that stores information about individual votes cast by voters in an election. The Vote_Table entity allows for efficient storage and retrieval of voting data, enabling the tallying of votes, auditing of the voting process, and generation of election results. It serves as the foundation for vote-related functionalities, such as verifying and validating votes, ensuring the integrity of the voting process, and enabling analysis of voting patterns and trends. The list of attributes and their datatypes that can be associated with the Vote_Table entity are:

- VoteID: VARCHAR2 (7)
- VoterID: VARCHAR2 (10)
- PartyID: NUMBER (10)
- CandidateID: NUMBER (10)
- DistrictID: NUMBER (10)
- Def_Password: VARCHAR2 (50)
- password_entered: VARCHAR2 (50)

Result: In an online voting database system, the "Result" entity represents the outcome or summary of an election. It stores information related to the final results and statistics of the voting process. The Result entity enables efficient storage and retrieval of election outcome

data, facilitating transparency, and providing a consolidated view of the result to the relevant stakeholders, such as voters, candidates, and election officials. It serves as a crucial component for analyzing historical election data, monitoring trends, and ensuring the integrity of the electoral process. The list of attributes and their datatypes that can be associated with the Result entity are:

- ResultID: NUMBER (10)
- CandidateID: NUMBER (10)
- PartyID: NUMBER (10)
- DistrictID: NUMBER (10)
- Vote_Count: NUMBER (10)

NON-FUNCTIONAL REQUIREMENTS:

1. Security:

Confidentiality: The system must ensure that voter identities and votes remain confidential and cannot be accessed or tampered with by unauthorized individuals.

Authentication: Robust mechanisms should be in place to verify the identity of voters and prevent impersonation or unauthorized access.

Data integrity: The system must maintain the integrity of votes and ensure they are not altered during transmission or storage**.**

Auditing: The system should have comprehensive auditing capabilities to track and record all activities related to voting and ensure transparency.

2. Reliability and Availability:

System availability: The online voting system should be accessible and operational for the entire duration of the voting process, including peak usage times.

Fault tolerance: The system should be designed to handle failures, such as hardware or network failures, without compromising the voting process.

Disaster recovery: Adequate backup and recovery mechanisms should be in place to ensure the system can be quickly restored in case of a disaster or data loss.

3. Performance:

Scalability: The system should be capable of handling a large number of simultaneous voters without experiencing significant degradation in performance.

Response time: The system should provide prompt response times to ensure a smooth and efficient voting experience for users.

Throughput: The system should support a high number of votes per unit of time to accommodate peak voting periods.

4. Usability:

User interface: The online voting system should have a user-friendly interface that is intuitive and easy to navigate, catering to users with varying levels of technical expertise.

Accessibility: The system should be accessible to individuals with disabilities, complying with accessibility standards and providing appropriate accommodations.

5. Compliance:

Legal and regulatory requirements: The system should adhere to all relevant laws, regulations, and standards governing elections and data protection.

Transparency: The system should provide transparency in terms of the voting process, ensuring that the process can be independently audited and verified.

RELATIONSHIP BETWEEN THE ENTITIES:

User Table and User Type:

The relationship between the user table and user type can be described as a one-to-one relationship. In the one-to-one relationship between the user table and user type entity, one user is associated with one user type, and one user type is linked to one user with a user type id. hence cardinality is 1:1.

Voter Table and User Table:

The relationship between the voter table and the user table can be described as a one-to-one relationship. In the one-to-one relationship between the voter table and user table entity, each voter is linked to the user table through Aadhar and gets only one voter id. Hence cardinality is 1:1.

User Table and Vote Table:

The relationship between the user table and the vote table can be described as a one-to-one relationship. In the one-to-one relationship between the user table and the vote table entity, each user gets only one vote id, and also each vote id is applicable to one user which is linked through the voter id. hence cardinality is 1:1.

Candidate Type and Candidate Table:

The relationship between the candidate type and candidate table entity can be described as a one-to-many relationship. In a one-to-many relationship between the candidate type and candidate table entity, each candidate type belongs to many candidates in the candidate table and each candidate can have one candidate type. hence cardinality is 1: M.

Address and Voter Table:

The relationship between the address and voter table entity can be described as a one-to-many relationship. In one-to-many relationships between the address and voter table entity, each address belongs to many voters in the voter table, and many voters can have one address. hence cardinality is 1: M.

Candidate Table and Result:

The relationship between the candidate table and the result can be described as a one-to-many relationship. In one-to-many relation between the candidate table and result entity, each candidate can get many results and also many results applicable to one candidate. hence cardinality is 1: M.

Party Table and Candidate Table:

The relationship between the party table and candidate table entity can be described as one to many relationships. This relationship implies that many candidates belong to one party, but a party can have multiple candidates representing it. hence cardinality is 1: M.

Election Table and Candidate Table:

The relationship between the election table and the candidate table entity can be described as a one-to-many relationship. In the one-to-many relationship between the election table and the candidate table entity, many candidates can participate in one election. hence cardinality is 1:M.

Vote Table and Candidate Table:

The relationship between the vote table and the candidate table entity can be described as a many-to-one relationship. In a many-to-one relationship between the vote table and the candidate table entity, each voter can vote for each candidate also each candidate can request votes from many voters. hence cardinality is M:1.

User Table and Election Table:

The relationship between the user table and the election table can be described as a many-to-many relationship. In many-to-many relationships between the user table and election table entity, each user can vote in many elections and many elections can be participated by many users. hence cardinality is M: M.

Candidate Table and Address:

The relationship between the candidate table and the address entity can be described as a many-to-many relationship. In a many-to-many relationship between the candidate table and address entity, many candidates can participate in many addresses, hence cardinality is M: M.

RISKS:

Data Breaches:

Protecting the voter database from unauthorized access is crucial. Implement robust security measures such as encryption, strong access controls, and regular security audits.

Unauthorized Access:

Implement authentication mechanisms to ensure only eligible voters can access the system. Consider using multi-factor authentication (e.g., combining passwords with SMS verification codes) to enhance security.

Data Integrity:

Prevent unauthorized modifications or tampering of the database. Implement measures like digital signatures or hash functions to verify the integrity of the stored data.

Denial of Service (DoS) Attacks:

Online voting systems can be vulnerable to DoS attacks that can disrupt the availability of the system. Implement measures like rate limiting, traffic monitoring, and redundancy to mitigate these risks.

Insider Threats:

Protect the database from internal threats such as malicious employees or administrators. Implement strict access controls, regular monitoring, and auditing to detect and prevent unauthorized activities.

Voter Privacy:

Ensure that voter information remains confidential. Apply data anonymization techniques whenever possible, and strictly adhere to privacy regulations and policies.

ASSUMPTIONS:

When making assumptions about a database for online voting, it's important to consider various factors and requirements. Here are some assumptions that can be made:

Security:

The database should be designed with robust security measures to protect the integrity, confidentiality, and availability of the voting data. It should implement strong encryption, access controls, and regular security audits to prevent unauthorized access and tampering.

Reliability:

The database should be highly reliable and capable of handling a large volume of concurrent transactions. It should have built-in redundancy and backup mechanisms to ensure data availability in case of hardware or software failures.

Scalability:

The database should be scalable to accommodate a potentially high number of voters and concurrent transactions during peak periods. It should be able to handle the increased load without sacrificing performance or data consistency.

Data Integrity:

The database should ensure the integrity of the voting data, preventing any unauthorized modifications or tampering. Implementing mechanisms such as transaction logs, checksums, and data validation techniques can help maintain data integrity.

Data Privacy:

The database should adhere to strict privacy regulations and protect the personally identifiable information (PII) of voters. It should follow best practices for data anonymization and pseudonymization to ensure the privacy of individuals participating in the voting process.

Backup and Recovery:

The database should have regular backups and a well-defined recovery strategy to minimize the risk of data loss. This includes implementing processes for periodic backups, off-site storage, and restoration procedures in case of a disaster.

Auditability:

The database should support comprehensive auditing capabilities to enable traceability and accountability. It should log all relevant activities, such as user access, data modifications, and system changes, to facilitate post-election audits and investigations if required.

Compliance:

The database should comply with relevant legal and regulatory requirements for online voting, such as data protection laws, election regulations, and privacy regulations. It should ensure transparency and maintain an audit trail to demonstrate compliance.

Accessibility:

The database should be designed to provide accessibility for all eligible voters, including those with disabilities. It should support adaptive technologies and provide alternative voting methods if needed.

Disaster Recovery:

The database should have a robust disaster recovery plan in place, including off-site data backups, redundant infrastructure, and failover mechanisms. This ensures that voting data can be recovered and the system can resume operations in the event of a catastrophic event or system failure.

These assumptions provide a general framework for designing a database for online voting. However, it's important to consult with experts in the field and consider specific legal and regulatory requirements to ensure a secure and reliable online voting system.

CONCLUSION:

The online voting system includes all aspects of conducting secure and transparent voting using online technology. Data collection, management, and security are important aspects of an online voting system. The system helps to provide all the needs of the election commission and the voters. This system ensures the accuracy and integrity of the voting results and maintains the privacy and anonymity of the voters.

EQUALLY CONTRIBUTED BY

1. LOHITH V (TL)
2. NAGA VINEETHA POLINA
3. V.K. KARTHIK
4. PALADUGU VINOD
5. VISHNUPRIYA G
6. YUGANDHAR P
7. VINISHA J