*Software requirement specification*

Online voting system

Name: Susil Kumar K

Date: 15.03.2024

1. **Objectives and scope ………………………………………………………… 3**
2. **Project End Users …………………………………………………………….. 3**
3. **Features…………………………………………………………………………… 3**

3.1. Login to the system ………………………………………………………………………. 3

3.2. Authenticate via OTP …………………………………………………………………….. 4

3.3. View candidate details……………………………………………………………………. 4

3.4. Vote the candidate ………………………………………………………………………… 4

1. **External Interface Requirements**

4.1. User Interfaces………………………………………………………………………………..5

4.2. Hardware Interfaces…………………………………………………………………………5

4.3. Software Interface…………………………………………………………………………..6

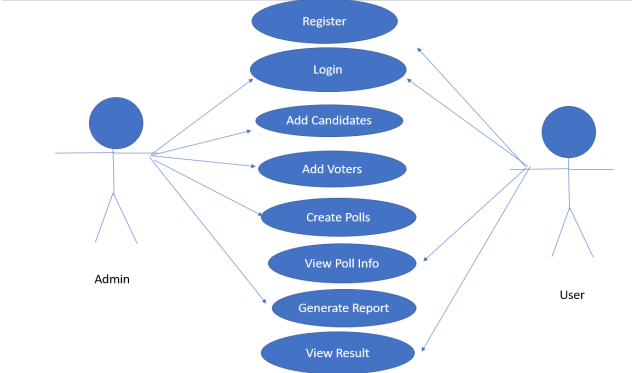
1. **Objective and Scope:**

The main objective of this online voting system is to give a seamless experience and to take the usual voting experience to the next level and make the voters vote with both security and comfort.

The scope of the online voting system includes the following features:

* For secure login it requires aadhar number, voter id, name as per the aadhar card.
* Aadhaar numbers and voter id would be saved encrypted on the database.
* For inclusivity there available ease navigation, for people who cant able see could able to navigate through dictation.
* There available different themes where we could switch between for better user interface
* Compared to the traditional way, this system has improved the counting process.

Below is the class diagram for online voting system,



1. **Project End Users:**

The people who are eligible to vote may use this system, as they could vote conveniently and securely.

1. **Features:**

**3.1 Login to the System:**

Every user should be authenticated through their name, aadhar and voter id and the user would receive an OTP to their phone numbers. By which they could login to the system. If he’s an admin he would be navigated to a separate page for managing elections, votings, voters etc.,

Validation for the system.

Name: It should only contain letters with a maximum of 20 characters.

Aadhar Number : It accepts only numbers upto 12 digits.

Voter Id: It accepts alphanumeric upto 10 characters.

**3.2 Authenticate via OTP:**

After verifying the credentials, a 7 digit otp number would be sent to the user for authentication, by which the user could login to the system.

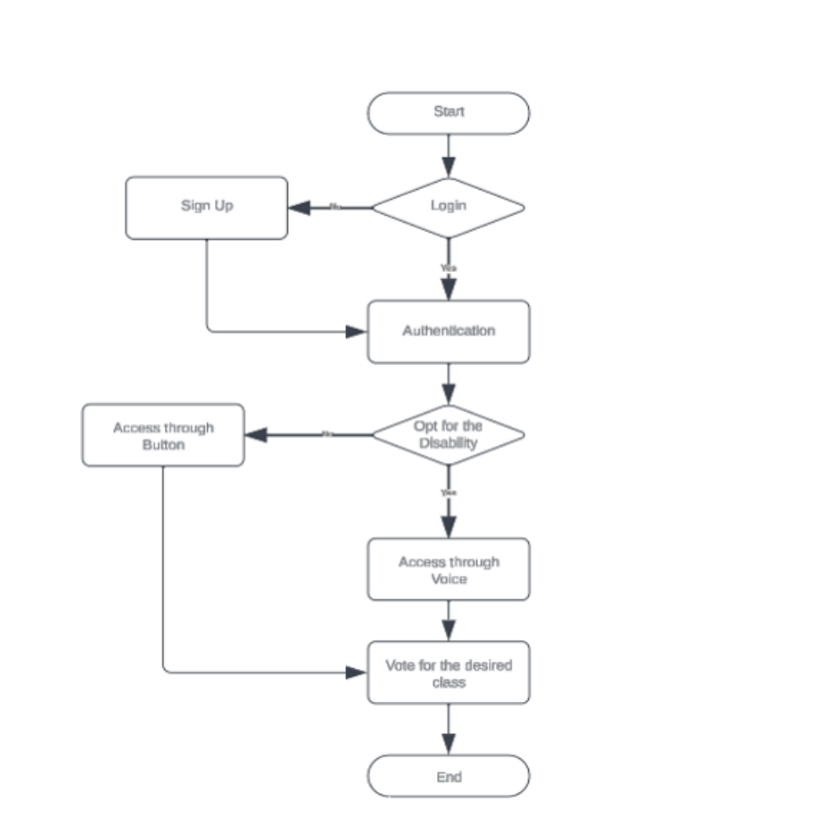
**3.3 View Candidate Details:**

At the voting process users were able to view the candidate details such as name, experience and any relevant details. The filters would be available for the user’s convenience as they would be able to find specific candidates easily.

**3.4 vote the candidate:**

For the voting process the user would be displayed with all the candidates information and they could select and vote for the desired one. For final review the user would be shown a dialog box to confirm with all the details of the selected candidate. After submission the window would automatically close.

The below flow chart best represents the flow of online voting system with the main functionalities.

****

1. **Other Nonfunctional Requirements**

**4.1. Performance Requirements:**

The software is expected to have reasonably short response time. It should be able to log-in and feed the voter with new pages on request with a response time of the order of a few seconds

**4.2. Safety Requirements:**

In order to prevent data loss in case of system failure, the result of votes that were polled till then have to be saved in the database, for the system to resume the counting process on reboot. • The EA should set up his system time appropriately for the election process to start at the correct time. • In case the EA detects any security lapse in the system, he should able to shut down the server and close all connections immediately while preserving the already polled votes.

**4.2. Security Requirements:**

The system should provide basic security features like password authentication and encrypted transactions. • All the passwords generated and communicated to the users should be stored in the server only in an encrypted form for login management to prevent misuse. • Serial attacks should be avoided by maintaining a minimum time gap between successive invalid log-in attempts.