The Mobile based Voting System

PRIMITIVE DESIGN REVIEW.

Faculty: Dr. Kavita Vemuri
Student mentors: Suhan Prabhu
Group Number: 6
Team Leader: Siddharth Bhat
Assistant Team Leader: Ganesh Vanahalli
Subgroup Leaders:
- ➔ Maintenance and Backend : Rohit Kumar Agarwal
- ➔ Statistics and Big Data Analysis : Samyak Agrawal
- ➔ User Interface and Architecture : Vashist Madiraju
- ➔ Security : Nitesh Gupta
- ➔ Awareness and Reaching Out : Kaushik Komallapalli

System Overview

- This project is to improve the Mobile Based Voting system proposed in 2009, integrating the system with new technological developments made so far which will make the system more efficient and user friendly.
- A majority of the country's youth does not vote as the election day generally clashes with the other commitments such as exams, college, work etc. In such cases, due to their laziness, the don't go and give excuses of long lines to cast vote, etc.. This mobile based system allows the people of the country to vote from the comfort of their homes, without the waiting and travelling period.
- Around 30% of the country's population possess or have access to a smartphone, most of these which have the usual Android or iOS operating systems. The people between 18 and 30 who are the youth of the country make up around 16-17% of the population, and most of them are not able to vote for various reasons (eg. Studying in a different state) .
- It would also allow the elderly who are unable to travel to vote, without discomfort.
- The implementation of this system would help increase the voter turnout also, which was only 60% in the most recent general elections.
- It would also allow the people who are unable to vote due to health conditions or climatic conditions or even fear of intimidation.
- Using social media awareness (benefits) of mobile based voting system are conveyed.

System Objective

- Our belief in democracy, our values of tolerance, fairness and justice all compel us to uphold the basic right given by DEMOCRACY, RIGHT TO VOTE to choose our leaders on our own and this is an attempt to make it more comfortable and secure.
- **The goal is to "Make a system that gives a citizen no excuse for not voting."**
- To analyze the current election system and suggest modern development of an mobile based voting system which will allow voters to cast their votes in a more convenient way.
- To develop a mobile based voting system that is transparent, reliable, tamper proof and that will provide a platform for voting.
- To reduce the usage of paper, which indeed is a way to **save trees**.
- Effective usage of social media so as to provide maximal amount of awareness on the new system.
- Greater speed and accuracy placing and tallying votes.
- Minimize the number of miscast votes and ensuring that the voter's genuine choice is recorded.
- Reduce the entire effort of setting up polling booths.
- To avoid the malpractices such as booth capturing.
- Our system also enhances the security and provides more mobility and convenience to voters.
- To allow the youth of the nation that fails to vote due to not being in their own ward to vote.
- To let all those physically disabled people, who due to their physical challenges can't make it to the polling booth, vote.

Operational Objectives

- To analyse the current election system and suggest modern development of an electronic online voting mobile application which will allow voters to cast their votes in a more convenient way.
- To design a mobile application prototype of a voting system for people with access to smartphones.
- To develop a mobile application voting system that is transparent, reliable, tamper-proof, secure, convenient and user friendly.

- Validating the system so that only eligible voters are allowed to vote.
- Improve the registration process by allowing voters to check their registration status prior to voting and centralizing registrational databases.
- Ensure that nobody's vote is counted more than once and discard the duplicate votes, if any.
- The system should ensure the privacy of the voter is not breached via any digital method while he is in the process of casting his vote.
- To ensure that all computations during the election are done in a reasonable amount of time and voters are not required to wait on other voters to complete the process.
- Test and review the system for usability and functionality.

System Design

Scope
- The current scope of the system doesn't include the entire nation.
- This is only for the people who own smartphone and are technically capable to install an application and complete the authorisation.
- According to the current statistics, ~30% of the people in India own a smartphone.
- Assuming on an average 2 people vote from a smartphone, our system will cover on an average ~60% of population.
- The scope of the system is limited to the people who have network access and people without the same are out of the scope of this system.
- It is limited to the people who are eligible to vote.
- The scope of the system however will expand with people having a more ready access to the smartphones and with setting up of more network stations.

Design Requirements
- The system requires the voters to have Voter ID/Aadhar card.
- The voter must possess/have access to a smartphone which runs on Android/iOS operating system.
- Good graphic designers to provide good pictorial representation wherever possible and necessary.
- Aadhar Database/ Voters list
- Stable Internet connection (preferably 3G or higher.)
- The government will ensure that sufficient network stations are set up in order to handle the traffic during the voting period.
- The public should be aware of the means and minimum/bare requirements required of the them to be eligible to vote in via this system.
- Good security protocols to ensure that the public trust and can safely exercise their right to vote an take part in fair elections.

Stakeholders
- Government
- Citizens
- ISPs

Design Characteristics

- Exporting and storage of election data which can be used for future analysis.
- Relinquishing the server when it faces a downfall.

- Elections results of all the constituencies and statistics of the elections are made public which can be used to study general trends or to improve accountability of the whole election process.
- Application interface which can be used to communicate all the details of the elections to the users.
- It is important to create awareness among the people whenever a new system arrives in society.
- Data encryption services so that our voting data is not accessible to mobile service provider.

System Organization

- The whole system is divided into five subsystems based on their expertise

  - **Maintenance and Backend** :- this subsystem handles the maintenance of the proxy servers and designs the architecture of the voting process.

  - **Statistics and Big Data Analysis** :- this subsystem processes the data that is acquired in this whole voting period and analyzes to give more information on how to make the system more efficient.

  - **User Interface and Architecture** :- this subsystem builds a GUI that is easier to use and efficient to carry out the voting process.

  - **Security** :- this subsystem handles the security issues regarding the system such as hacking, tampering of votes physically as well as on network.

  - **Awareness and Reaching Out** :- this subsystem plays a major role on educating the people about the system's advantages over existing voting systems.

- The subsystems are in constant interaction with each other to exchange information and making their subsystems more and more efficient hence making the system as a whole more efficient.

- Subsystem maintenance and backend is in interaction with security subsystem to design its way of data encryption so as to be compatible with security measures taken by security subsystem, it is in interaction with ui and architecture directly as the vote data is directly passed on from UI to backend subsystem.

- Subsystem statistics and big data analysis is in interaction with awareness and reaching out to collect participation data, also its in interaction with maintenance subsystem to know how many servers are deployed and other information to provide efficient measures. It takes population data from reaching out subsystem and analyzes number of servers needed as per the information given by backend subsystem and gives that number back to backend subsystem.

Subsystem 1: Maintenance and Backend

1.1. Introduction
1.1.1. Scope

- Setup and Maintenance of server infrastructure.
- Setup logging systems to notify stakeholders about the current server status.
- Adding new users and maintaining the user database.
- Storage of the votes polled. Maintaining the database securely.
- Verifying and allowing only authorised access to the servers.
- Maintenance of all other subsystems mainly Security and UI Architecture.

1.1.2. Purpose
- To set up the servers across the nation keeping in mind the traffic
- Ensure that the systems are genuine and have not been tampered with
- Ensure that the votes casted are stored properly and that there is no bug in the system
- Maintain the servers and keep updating it with the latest available features in consultation with the relevant sub-system
- Foresee problems that may occur and plan effectively to counter them.
- Being ready with effective backup plans in case of system failures on the D Day.

1.1.3. Overview
System maintenance is an ongoing activity, which covers a wide variety of activities, including removing program and design errors, updating documentation and test data and updating user support. For the purpose of convenience, maintenance may be categorized into three classes, namely:

- Corrective Maintenance: This type of maintenance implies removing errors in a program, which might have crept in the system due to faulty design or wrong assumptions. Thus, in corrective maintenance, processing or performance failures are repaired. For our mobile voting system, it is essential to evaluate the error log and fix these errors before the system could be exploited.

- Adaptive Maintenance: In adaptive maintenance, program functions are changed to enable the information system to satisfy the information needs of the user. This type of maintenance may become necessary because of organizational changes which may include:
    a) Change in the election commission's procedures,
    b) Change in election commission's objectives, goals, policies, etc.
    c) Change in forms,
    d) Change in information needs of election council.
    e) Change in system controls and security needs, etc.

- Perfective Maintenance: Perfective maintenance means adding new programs or modifying the existing programs to enhance the performance of the information system. This type of maintenance undertaken to respond to voter's additional needs. Outside changes are primarily environmental changes, which may in the absence of system maintenance, render the information system ineffective and inefficient. These environmental changes include:
    a) Changes in governmental policies, laws, etc.,
    b) Economic and competitive conditions, and
    c) New technology.

1.1.4.   System Characteristics

1.1.4.1 Physical characteristics

- This system's physical characteristics consist of the required hardware that is necessary to run servers. In general, our system will be a hardware heavy system. We will require access to powerful servers, with access to large network bandwidth at low latency. We require both of those characteristics to provide for a consistent experience for the voting system.
- The location of the system - Since this system will need to talk to the outside world: That is, the election committee's software and servers, it would be advantageous for this system to be co-located with the election servers. This will help for faster connections, as well as increased security for our system.
- Our system will need to be located at a center where there is access to uninterrupted electricity and internet. Otherwise, our servers will fail and will hamper the election process.
- It is advisable to make sure that the location is physically inaccessible to reduce any risk of terrorist attack.

1.1.4.2 Behavioural Characteristics

- Uptime: The system will guarantee a five nines uptime (a downtime of less that five minutes a year). Such reliability is essential for the voting process to be held.
- Bug-freeness: The system will ensure that all of its code is race condition free and crash free. We will ensure this is possible by rigorously checking our code using state-of-the-art model checkers and static analysis tools. We have considered using formally verified code, akin to the [DeepSpec](#) project, that aims to provide full correctness of hardware and software. This will enable us to fully trust the computations performed by our server.
- Fault tolerance: It is always possible that adversaries gain access to some of the network. Under such circumstances, our services will be written in a distributed style to make it harder for an adversary to control the entire system. Indeed, we shall use byzantine-resistant protocols to ensure that we minimise the chance of a hostile takeover.
- Data exchange: The system will allow for exporting and storage of data, to allow for analysis of the election to be performed later. This is necessary both to publish statistics and analyses about the elections. It also enable researchers to mine the data for information. It would also allow the detection of certain styles of voter fraud. Indeed, some research has gone into this, but it appears that high quality data is not available so far. We will be the first to publish such data and make it available for science.
- Openness: We will host all the code on an open source platform, to ensure community participation, as well as increased trust in our systems. We would like for our system to be adopted by other countries and trusted by our citizens. To this end, we wish to host our source-code on public version control. We are also considering using a blockchain-based model for voting, to ensure that a public ledger is present that records all votes that have been cast. Due to us storing data on a public ledger (ala blockchain), it will be tamper-proof.

1.2.   Requirements

- The initial requirements for maintenance are listed, although the requirements would continue to evolve during the development and operation of the system. Considerations include:

- Maximizing system availability to meet the operational requirements. This has to take into account the designed-in reliability and maintainability of the system and resources available.
- Preserving system operating potential through proper planning of system scheduled maintenance. This requires a reliability-centered maintenance strategy that incorporates preventive maintenance in order to preempt failures, thereby extending the mean time between corrective maintenance, as well as enhancing the availability of the system.
- Segmentation of maintenance activities for potential outsourcing of non-critical activities to approved maintenance subcontractors as to optimize scarce technical manpower resources and maintenance/repair turn-around times.
- Harnessing IT technology for maintenance management. This involves rigorous and systematic capturing and tracking of operating and maintenance activities to facilitate analysis and planning.

1.3. Objectives

- To ensure that the servers are up and running before the elections
- To ensure the integrity of the elections by having tamper-proof systems
- To ensure that only authentic users are able to use the app
- To maintain and store the election and votes database securely.
- To ensure that only authorised people get root access to the system. To put in place necessary checks for that.
- To maintain all the subsystems and keep them ready

1.4. Implementation

- **Disaster management :** Our primary servers will be managed by us, in a physically secure location. However, it is always possible that an attack or a disaster takes place which destroys or corrupts our primary servers. In such cases, we will have backup services that can be launched on demand, by using SaaS (software as a service) provides such as Amazon AWS, or google cloud computing, where we would have backup services available and ready.

- **Data management:** We wish to ensure that the election data cannot be compromised, while also ensuring openness of our data. This may seem paradoxical, but is not so. Indeed, bitcoin has managed to do the same for cryptocurrency.

    We will leverage the blockchain technology to associate each person with a digital anonymous globally unique ID (GUID). This GUID is encrypted and is only stored on the user's phone. This makes it less susceptible to large scale data-loss as would be the case if the data was stored in a centralised server. Indeed, apple phones provide for secure enclaves to store cryptographically secure information. We will ensure that we use the best cryptography technology possible.

We will make each vote add a node into the distributed ledger (Blockchain) of votes, thereby ensuring that an adversary is unable to tamper with the election data. This will be using the exact same principles as that of bitcoin / other blockchain providers.

- **Efficient data encoding :** Compressing the data size as much as possible to reduce the data usage so that even at very low net speed voting can be done. We will use standard techniques from coding theory to ensure that our data communication sizes are as small as possible. Most web servers now-a-days communicate with JSON, which is text based. While convenient, they are much larger than what a densely packed binary encoding of the same data would be. We will use Google's Protocol Buffers, a technology for serialising data which is available on all platforms for this purpose.

- **Congestion control:** We will ensure that our servers are fault and congestion tolerant. We shall naturally follow best practises and have caches and load balancers as the frontline to our servers. We shall also make use of content delivery networks such CloudFlare, which as a bonus also defend us from naive DDoS attacks.

- **Vote uniqueness:** We will need to ensure that each user is only able to cast one vote. In light of this, we will ensure that users that have registered for the e-voting service will not be allowed to vote at EVM's - their name will not be printed on the list of eligible voters at the voting booth. This will ensure that voters cannot "double vote" and abuse our system.
- **Anti vote-manipulation:** We will use machine learning to try and learn patterns of vote manipulation and collusion, to alert the authorities about such possibilities as the votes are being cast. There is some past literature on the topic, but no one has really tried such a system on a scale such as India (the world's *largest* democracy). Therefore, this would be a prime research project.
- **Software:** As mentioned before, we will first design the control flow of our server in a model checker such as TLA+, which is a specification tool to ensure that concurrent systems behave as expected.

  Next, we will ensure that our system behaves as expected by having a rigorous testing environment with unit and integration tests. However, this is definitely not enough. We will make sure to run our code through static analysis tools which help identify errors in programs by deeply analysing the source code. We will ensure that we run our code through a gauntlet of static analysis tools.

  In the end, we will run fuzz testing tools such as american fuzzy lop against the code that trace the assembly at runtime and try to abuse the code that it is running against.
- **Distributed system testing:** We will make use of industry best-practices when it comes to testing our distributed systems. Particularly, we will run Netflix's services called ChaosMonkey, which will arbitrarily always shut down some proportion of our servers during testing, to ensure that we can handle challenges like servers randomly failing during deployment. Si

1.5. Challenges

Challenges	Manageable / non manageable	Reason

Unpredicted traffic	Manageable	Collecting the information from subsystem statistics and big-data analysis and posting the acquired number of proxy servers to handle traffic.
Loss of data while transmission	Manageable	Using recent error correction codes, data retrieval techniques to reconstruct the data, if not possible in worst case conducting the elections again.
Implementing security and prevent system breaches	Manageable	Monitoring server health, making sure no attacks have taken place

1.6. References

- HomeAlone: Co-residency Detection in the Cloud via Side-Channel Analysis.
- This is probably require separate negotiations with Amazon / Google etc to provide machines themselves. Talk about possible problems, solutions.
- Hiding Routing information - David M. Goldschlag, Michael G. Reed, Paul F. Syverson.
- PProtecting SIP Proxy Servers from Ringing-Based Denial-of-Service Attacks - IEEE.

1.7. Use-Case Diagrams

Subsystem 2: Statistics and big data analysis

1. **Introduction**

    1.1. **Scope**
    - The sub-system will work towards analysing the elections in terms of statistics, numbers and data.
    - Sub-system is such that it can be used to better the whole process of digital voting via feedback on various components of the system.

    1.2. **Purpose**
    - This sub-system mainly deals with collecting relevant election statistics and deriving important conclusions from them.
    - The system also contributes towards enhancing the democratic setup of the country by releasing pre/post election data so that the people can make rational decisions.
    - To detect shortcomings of the e-voting system via the response of voters from different regions/classes and thus improving upon the reach of our system.

    1.3. **Overview**

- Big data is data sets that are so voluminous and complex that traditional data-processing application software are inadequate to deal with them. Some challenges in handling big data involve capturing data, data storage, data analysis, search, sharing, transfer, visualization, querying, updating, information privacy and data source.
- Some examples of data statistics that we could exploit to make interesting observations/inferences could be:
    - The number of voters who actually cast their vote.
    - Percentage of people who voted for the candidate of a particular religion only.
    - Region-wise ethnic and communal population distribution and the distribution of votes amongst candidates from various communal and ethnic backgrounds.

1.4. System Characteristics
- **Advantages**
    - Country's public can see the statistics and make their decisions for themselves.
    - The whole e-voting system can be improved upon based on collected data/feedback.
    - Participation of people can be quantified as well as general trends can be studied.
    - Improve accountability of the whole process.

- **Disadvantages**
    - Political parties can use big data analytics to manipulate the voters.
    - Data analytics generally requires a lot of human, technological and monetary resources.
    - Published data can be tampered/manipulated to mislead people.
- **Case Studies**
    - Some case studies related to the use of statistics and big data analytics in the field of politics and especially the election process.
    - *2012 US presidential elections:*

        Analytics played a bigger and more important role in the election than just predicting the outcome. Analytics was an integral part of the 2012 political campaign. In recent elections, Republican and Democratic campaigns have employed data-driven analytics and social-media data to stay ahead of the competition, but the Democrats clearly had the

competitive advantage in the 2012 presidential. During the six months leading up to the election, the Obama team launched a full-scale and all-front campaign, leveraging Web, mobile, TV, call, social media and analytics to directly micro-target potential voters and donors with tailored messages. Compared to previous presidential campaigns in 2004 and 2008, the 2012 campaign was going digital and analytical across all channels. The Obama campaign management hired a multi-disciplinary team of statisticians, predictive modelers, data-mining experts, mathematicians, software programmers and quantitative analysts. It eventually built an entire analytics department five times as large as that of its 2008 campaign which proved out to be an important factor of Obama's victory.

- *India Case Study:*

  India's very own Narendra Modi is considered to be one of the most technology and social media-savvy politicians in the world! Prime Minister Modi has no less than 10k followers on Twitter, 32 million likes on Facebook & 440 million views on Google+. In 2014 elections, the BJP party won the elections in India with the help of open-source digital tools that put them directly in touch with their voters. Most of the metrics to do that were achieved using data mining and data analytics to dig into the plethora of social media activities. This is how digitalized and data driven election campaigning and post/pre election analysis is slowly paving it's way into the Indian political scene also.

2. Requirements

2.1. System Entities

- Ideation for proposing methods for conventional voting system with mobile voting.
- NGO's and government survey bodies.
- Voters of the country.

2.2. Subsystem Mission

- Find new trends in elections by looking at data from different domains and different sections of the same domain.
- Find out the sections of the society and regions of the country where people are not using the application and provide that data to the advertising subsystem.
- To make sure that the proposed solutions are consistent and compatible with other subsystems .

- To propose a maintainable and efficient Data collection system and optimize on the current methods of data collection .

3. **Objectives**
    3.1.   **Pre-Mission Phase Objectives:**
    - The pre-mission phase involves gathering relevant data from surveys conducted over the years by government as well as independent NGO's.
    - Build up the required software to support and handle the huge amount of data and different types of data.

    3.2.   **Mission Phase Objectives:**
    - Live update of data as soon as its available.
    - Changing statistics based on the inflowing data during the time of elections .

    3.3.   **Post-Mission Phase Objectives:**
    - Analyse the collected data and help other subsystems handle it and obtain useful conclusions from it .
    - Identifying the shortcomings of the subsystems and working on them , also optimize the current processes and useful data generation methods.
    - Conduct surveys around the country to collect more data and target important areas based on the current data.
    - Release the data which can be made public so that media and people can utilize it in decision making and discussions.

4. **Implementation**
    4.1.   **System Reliability**
    - The reliability of this system depends on the Data Collection Phase. This system simply interprets the data collected to provide trends in voting in different areas.
    - The different kinds of data is collected after the elections which helps the Political Parties as well. The data can help them to know in which areas they got more support and in which constituencies support for them is less so that they can focus more on that constituency in the next elections.
    - Also, manual human verification is done to ensure that the data collected is viable.
    - The trends in the result were compared with the result of the elections conducted on paper to check that it follows the same trends and thus prove our system more reliable.

    4.2.   **System Maintainability:**
    - The advancement in the mobile devices the wireless sensor network and web technologies that has given rise to the new applications which makes the voting process very easy and efficient.
    - Large database is needed due to large scalability of our system. And the data stored can be used as an input in case of any issues and the system will look at solutions for each of the issues and then combine them in an appropriate manner.
    - If suppose the system faces a new problem that is not among the list of existing problems as suggested by the previous system, solutions for that issue will have to

be manually determined and given to the system for future reference. It will then repeat the same process of obtaining solutions for each of the individual problems and then finding an appropriate solution by finding a blend of the known solutions (of the individual problems).

- If there is any new data which may either be a new problem faced by or due to the machinery or any part of the system or a new solution for a specific problem, the system is updated immediately and the results will therefore be accordingly modified.

4.3.   System Availability:

- The system is a simple Android Mobile application and so the system is easily available with all the people using Smartphones.
- The system can however be used only in the areas where data network is available.

5.   Table of Challenges

Challenges	Manageable / non manageable	Reason
Collection of very large dataset	Manageable	Population of the country
Making app available and usable in rural areas	Manageable	Enhancing the network facilities in rural areas
Inability of people to use mobile and the application	Manageable	Illiteracy and Lack of awareness and exposure.

6.   References:

6.1.   https://theaims.ac.in/resources/vote-for-analytics-how-predictive-analytics-impacts-elections.html

7.   Use-Case Diagrams

<u>**Subsystem 3: Application Development and UI Architecture**</u>

1. **Introduction**
    1.1. **Scope**
        - This subsystem will look at the User Interface (hence forward referred to as UI) architecture of the system.
        - Focus of this subsystem is to make UI easy to use, attractive, efficient and responsive .
        - This subsystem will try to make a standard interface design which is 'right' for each type of user.
        - This subsystem is not fully independent, it has to coordinate with the other subsystem Backend and Maintenance.
    1.2. **Purpose**
        - This system will target a vast variety of users, so we need to make classification of types of users and try to understand their goals and requirements.
        - We can set some parameters for defining user ability like :
            1. Levels of ability e.g. novice, advanced beginner, competent user, proficient user,expert(dreyfus)
            2. Levels of usage (constant, regular, occasional)
            3. Familiarity with task set (this is one sort of ability, but quite different from that implied by (1), which is slanted towards technical ability)
            4. Degree of usage of similar or dissimilar hardware/software.
            5. User age and status profile.
            6. User group's task value perception (particularly relevant to the introduction of new technology).

1.3. Overview

- The User Interface (UI) design of a mobile app is associated with its look and feel that means that how your app is going to be interacting with its users.The design of the app should be made by comprehending mind of end users.
- In our case the end users are general public all over India, so the design should be simple such that a common man is able to use the app.
- As the system is based on smartphones, it'll encourage the "Tech Savvy" youth of the country to come out and vote to voice their opinion, which has been missing in recent elections.

1.4. System Characteristics

- **Intuitive and consistent design**

    For an interface to be easily useable and navigable, the controls and information must be laid out in an intuitive and consistent fashion. Your users are probably well acquainted with many other interfaces, and you should be too if you want to achieve a level of familiarity for your users. Coming out with an entirely new layout might sound like a highly rewarding, paradigm-breaking project, but for all practical purposes, if you want users to feel at home then follow the path of your predecessors! Logic of usability should play a big part in the design process: features that are the most frequently used should be the most prominent in the UI and controls should be consistent so that users know how to repeat their actions.

- **Clarity**

    If a user is not able to understand his or her way around your interface, all the time you spent perfecting the software's functionality is rendered useless. Both in terms of visual hierarchy and content, there should be absolutely no ambiguity over the way your interface operates.

- **High responsivity**

    For a user to enjoy using your interface, it cannot feel as if the interface is lagging to keep up with their mouse clicking and keyboard tapping. If the interface fails keep up with the demands of the user, this will significantly diminish their experience and can result in frustration, particularly when trying to perform basic tasks.

- **Maintainability**

    Call it flexibility if you wish - a UI should have the capacity for updates to be installed and changes to be integrated without causing a conflict of interest. For instance, you may need to add an additional feature to the software, if your interface is so convoluted that there is no space to draw attention to this feature without compromising something else or appearing unaesthetic, then this signifies a flaw in design.

- **Attractiveness**

    A pretty look cannot make up for a poor design. But pleasant colour scheme can go a long way in making the user feel more at home when using your interface. Again, the aesthetics you choose for your interface must be appropriate for the particular user - so perhaps some market research is required to determine exactly what your users are looking for. Good aesthetics give the product character and soul.

- **Conciseness**

    Clarity in a user interface is great, however, the design should not be over-clarifying. It is easy to add definitions and explanations, but every time you do that you add mass. Your interface grows. Add too many explanations and your users will have to spend too much time reading through them, it would be tough for the common person who is using the app. For example to use a particular feature instead of explaining in one sentence you are explaining in 3 , that makes your UI not concise.

- **Forgiving**

    A forgiving interface is one that can save your users from costly mistakes. For example, if someone deletes an important piece of information, can they easily retrieve it or undo this action? If by chance someone navigates to a broken or nonexistent page on the app,then they shouldn't be greeted with a cryptic error instead they should get a helpful list of alternative destinations.

2. **Requirements**
    2.1. Every user must have Aadhar card for voting.
    2.2. Android or iOS (Most common Mobile Operating system in Smartphones) phone should be available to each user i.e . atleast one within every household to ensure easy access to app. Android and iOS provide variety of pre-built UI components such as structured layout objects and UI controls that allow you to build the graphical user interface for your app.
    2.3. Aadhar Database (Used by government for linking bank accounts)
    2.4. State/Central government (i.e the governing body) will create servers for voting process (proxy).
    2.5. Stable internet connection, preferably 3G or higher.
    2.6. Some market research required to determine exactly what your users are looking for and what type of things are users familiar with.
    2.7. Good UI designers.
    2.8. The memory of the phone should be higher than 2Gb so that it doesn't hangs while voting.
    2.9. Good UI specifications are needed which takes into account the data and context of the user within the application. This will be done while consulting the Awareness and Statistics subsystems.

3. **Objectives**

    3.1. To maximize the turnout of voting.

    3.2. To ensure that users want to vote and have ease of access to vote.

3.3. To ensure that people with disabilities or limitations don't face difficulty in voting. The disabilities may include the person being Blind, Physically handicapped, Deaf, Illiterate, etc.

4. Implementation

4.1. Design
- This system is designed to ensure that all the citizens of the country with access to a smartphone are able to access the application and are able to correctly identify and vote for their chosen party/candidate.
- This is done while consulting the Security subsystem and is done with complete coordination to avoid any loopholes and glitches in the Application.

4.2. Accessing the Application
- The person will need to open the application.
- The person will first be displayed with a screen where they will have to choose between two options, choosing whether they they are literate or illiterate. This will be done pictorially and in a non-demeaning way to ensure no one is offended, but so that the distinction between the two is evident.
- Then the person is displayed with a screen from which they will get to choose the language they want to access the app in.
- Blind Voters may use the help of a person they trust to help in verification, and vote.

4.3. Verification and Authentication
- The person then is required to enter their Aadhar credentials/Voter ID credentials(current system allows for either) for basic authentication of person. They are then sent an OTP (One-Time Password) for confirmation to their registered phone number (Aadhar credentials).
- The OTP will be auto-detected by the Application, and incase it isn't due to special circumstances (Like voter not in possession of registered phone number), the voter will have the option to fill it in manually.
- The auto detection is to increase the ease of usage of the app, but mainly also to help the blind users who are unable to fill in the OTP.
- The voter then proceeds to the voting portal.

4.4. Identification of Candidate
- The screen which is displayed here depends on the Aadhar credentials (Disabilities are listed) and the mode (literate/Illiterate) which the voter has selected.
- If a person is Blind or needs vocal options read to them, the Application reads the options out loud (in the language of their choice)for the person and requires them to reply vocally with a number corresponding to their choice. It is confirmed once before moving on. This allows them to vote independently without the help of anyone and allows them to exercise their vote to secrecy of their vote.
- For people who are not visually impaired or disabled in a manner due to which they need vocal guidance, the app displays the party's logo along with the candidate's name and photo. This ensures that both literate and illiterate voters are able to uniquely identify the candidate.

4.5. Confirmation
- After the person has chosen their candidate they are asked to confirm their choice, in case of a mistake. If it is confirmed then the vote is confirmed and sent to a secure outbox, which uploads the vote when the server is active, else holds it till server is active.
- In case the vote is not confirmed, the screen goes back to the Candidate screen mentioned in section 4.4.
- The voter is then automatically logged out after the vote is sent to the the outbox and the Application settings are then refreshed after changing the status of the previous voter to DONE, preventing duplication of votes.

5. Table of Challenges
- **5.1.** The main challenges faced are listed with possible solutions in the table below:
  - Physically Disabled Voters
  - Illiterate Voters
  - Mentally Disabled Voters
  - Loss of connection to server

Table representing challenges:

Challenges	Manageable / Unmanageable	Solution / Reason
Physically Disabled Voters: - Amputees - Blind/ Visually challenged - Deaf - Blind & Deaf	- Yes - Yes (With some compromises) - Yes - No	- Through Vocal guidance/ can access app normally - Through Vocal guidance and help of a second person - Do not face any problems due to disability in this regard. - Not possible to make generalised app which will allow them complete freedom.
Illiterate Voters	- Yes(To some extent assuming person can at least write their name and copy credentials from cards if once taught)	- Through pictorial representation. This can be achieved with the help of good graphical advisory team, and is done regularly in many places like plane safety manual etc.
Mentally Disabled Voters	- No	- Can not help the voter if they are not able to make proper choice and not mentally well.
Loss of connection to server	- Yes	- Solved by sending vote to secure outbox for storage until secure connection to server is established

Table will be different with compounded disabilities as it would not be possible to make a generalised app while including them, which would not cause inconvenience to other users.

6.   References

6.1.   http://usabilitypost.com/2009/04/15/8-characteristics-of-successful-user-interfaces/
6.2.   http://www.it.bton.ac.uk/staff/lp22/CS133/usergroups.html

7.   Use-Case Diagrams

<u>**Subsystem 4: Security**</u>

1. **Introduction**
    1.1. **Scope -**
    - This subsystem will look at the major areas which are most prone to the attacks.
    - The data collected will be within the past 1-2 year.
    - The system will take care of all the major problems/attacks that have happened on already deployed Electronic Voting systems.
    - This subsystem is limited to the people who are eligible to vote and have access to smartphones and are technically capable of using the application.
    - With constant and active efforts of the Awareness and the Reaching out team, the scope of the system will expand as people who're passionate about voting and are unable to do so because they're not in their voting ward will get an incentive to buy a cheap smart phone and download the application as it'll let them vote.

    1.2. **Purpose -**
    - The system is not foolproof and vulnerable to security and software problems , it can be hacked as compared to the manual voting done. This subsystem handles all such problems.
    - It focuses on providing Network security as well as social security.
    - Network security : Network security aims to provide security to avoid loss/manipulation of the votes along the network.
    - Social security : Social security means avoiding social threats that might lead to vote tampering like people bullying other people to take their phone and cast vote or people stealing/borrowing phones to cast votes.

    1.3. **Overview -**
    - Cyber threats are evolving everyday thus increasing the need to develop and tighten security measures to ensure the protection of everyone using the cyberspace. Increasing use of cyber space throughout the world coupled with globalization has increased the complexity of cyber threats. Cyber security threats continue to escalate in frequency and variation.
    - This has led to major security assaults all over the world some of which has been documented below.
    - Attacks (threats):
        - Denial of Service in internet voting system:It can affect the internet voting system in two different ways of denial of service attacks
            - Hacker may able to change the network connection of the targeted web server with junk data that clogs the network and prevents the user or voter by accessing the web server and casting his vote.
            - In the second attack the hacker may put irrelevant resources with useless task on the election web server so that the server is busy. As the server is busy it may be unable to respond to the legitimate

voters. This type of attack may mostly be done on the last day of the election, as most of the electorate may plan to cast their vote on the last day.

- ○ Domain name service (DNS) attack:
  - ■ Attacks against the Domain name service route traffic to an attacker instead of to the legitimate vote service.

- ○ Viruses or Malicious Software:
  - ■ There is a threat of introducing any malicious software onto the internet voting server before or on the Election Day by any communication link or email and also if huge number of PCs (personal computers) connected to the internet voting server, then any PC which is infected with virus, there might be more number of chances to spread the viruses to the voting server. This may change the confidentiality and integrity of the vote or even the vote may be changed without the knowledge of the voter before it is transmitted to the voting server.

- ○ Hacking
  - ■ If the links of the voting system is changed or hacked then the voter may face difficulty in casting his/her vote, which may change the confidentiality and integrity of the vote.

- ○ Authentication Threats
  - ■ One of the main feature of our voting system is to link with Aadhar. This gives rise to many Cross site attacks such as CSRF attacks, XSS attacks, Cross site timing attacks.
- ○ Documented problems with electronic voting across the world:
  - ■ In Australia, during the New South Wales state election in 2015, there were several reports that over 66,000 electronic votes could have been compromised. Although the iVote (remote electronic voting system in New South Wales) website is secure, security specialist believe that a third party website was able to attack the system. This was the first time a major vulnerability was discovered in the middle of an ongoing poll.
  - ■ In Netherlands, on October 30, 2006, the Dutch Minister of the Interior withdrew the license of 1187 voting machines from manufacturer Sdu NV, about 10% of the total number to be used, because it was proven by the General Intelligence and Security Service that one could eavesdrop on voting from up to 40 meters.
  - ■ In United States, in 2010, graduate students from the University of Michigan hacked into the District of Columbia online voting systems during an online voting mock test run and changed all the cast ballots to cater to their preferred candidates. This voting system was being tested for military voters and overseas citizens, allowing them to vote on the Web, and was scheduled to run later that year. It only took the hackers, a team of computer scientists, thirty-six hours to find the list of the government's passwords and break into the system.

- Thus, there is a need for installation of better security measures to prevent the occurrence of these threats and for systems like the mobile based voting system which decides the future of the country, decides which party come to power it becomes essentially important to have preventive measures relative to the security of the system to prevent hackers or competing parties from tampering with the votes caste by the voters and thus altering the results of the overall elections.

1.4. System Characteristics

- Scalability: With the growth of population use of internet based voting system continues to increase so expansion in terms of coverage and capacity as needed- Should provide protection against huge traffic (Denial of Service attacks)
- Data Loss Prevention : Stops sensitive information from being revealed lets you stay in control what information is sent out.
- Application Control: Impedes unauthorized executables from functioning on your protected application (used for voting).
- Prevention as much as on real time protection against well known and new threats.
- To establish rules and measures to use against attacks over the Internet.

2. Requirements
2.1. Aadhar Card for each voter.
2.2. Phone (preferable android, ios, etc as operating system)
2.3. Aadhar Database (Used by government for linking bank accounts)
2.4. State government will create servers for voting process(proxy)
2.5. Stable internet connection
2.6. Ballot Server for counting

3. Objectives
3.1. Network security
- Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- It contains the workflow of how the user will use the API to vote
- It also explains the protocol required for interaction between different parties
- It involves the authorization of access to data in a network, which is controlled by the network administrator.

3.2. Social security
- Social security consists of the practices adopted to avoid social threats to fair voting process like social bullying, phone theft etc.
- It contains our proposed solutions to overcome these problems.
- These problems however can't be solved completely and this solutions only avoid them to some extent.
- To ensure accuracy and precision in voting to report the will of voters, to make every vote count.

4. Implementation
4.1. Network security

- **Workflow**
  - In this proposed system
    - Initially the voters should have to provide their Aadhar number to authenticate themselves and establish their user-ids. This constraint is imposed to ensure that only the genuine person is allowed to vote in the elections.
    - Our main focus is on the session OTP that is provided to the voter during the process of casting a vote. The OTP is nothing but a One-Time Password that is required to continue with the process of voting and this makes the system secure and free from misuse by an external party.
    - Election committee or administrator can authenticate and validate the voter as well as candidate.
    - Voter will caste his/her vote to the appropriate candidate according to their background information provided through the registered account.
    - Result will be displayed on the prescribed date and time

- **Protocol**
  - This system provides for three roles, namely, the signer (aadhar database), the recipient (the voter), the proxies(the state government), voting center and the bulletin(central government). The operation proceeds through four phases, namely, initiation, verification, voting and counting.

- **Initialization**

  - Step 1. The system first generates the required parameters(public key and private keys using the aadhar number for OTP) for each voter using blind

signature. In a blind signature scheme, a signee could get a message's digital signature signed by a signer without revealing any information about the message.

- ○ Step 2. The public keys are passed on to various proxies(State government).

- **Verification:**

  - ○ Step 3a. The voter gets authenticated with the Aadhar database using his Aadhar number. Then the proxy examines whether the registrant is a legal voter; if so, he or she distributes a certificate to the voter.(Check workflow pt 1,2,3)

  - ○ Step 3b. The proxy publishes the certificate of the voter to the bulletin.

  - ○ Step 3c. Meanwhile the voter checks whether he or she has registered successfully via the bulletin.

- **Voting:**

  - ○ Step 4. The voter chooses a candidate.

  - ○ Step 5a. The voter casts his or her ballot and sends it to the voting center.

  - ○ Step 5b. The voting center publishes a message about the ballot from the voter to the bulletin.

  - ○ Step 5c. Every voter can confirm whether his or her ballot has been received by the voting center; if not, he or she can resend the ballot.

  - ○

- **Counting**

  - ○ Step 6a. At the end of the voting period, the proxy creator forwards the decrypting key to the voting canter, and the voting center starts to verify and count the ballots.

  - ○ Step 6b. The voting center publishes the voting result to the bulletin, where everyone can verify and count all ballots.

- **Social security**

  - ○ Phone theft - To avoid this problem of phone thievery, what we aim to provide is a theft report portal, where you can enter your aadhar card number and voting for that aadhar card will be disabled. This will ensure

that people can't just go about stealing phones in order to cast multiple votes. (How feasible is alternate phone number?)
  ○ Social bullying - How far this problem can be solved still remains a question. However, to avoid as much bullying as possible, in addition to the above solutions proposed to provide network security, we will ensure that each session expires in a given time which then results in a user requesting to log in again, and hence to some extent might reduce a person bullying a person to log in and then hand him the phone.

5. **Challenges**
  5.1. **Digital divide**
    ● e-Voting system leads to a financial divide in the sense, that rich people who can afford and buy the technologies will be able to vote while the comparatively less affluent voters who may not be able to afford the technical devices won't be able to vote. Apart from that people who involve more in net banking facilities etc. are more used to using apps for every function. On the other hand, some financially strong people who even though are able to afford the device might not be very comfortable with this system if they haven't used the app based systems for rest of their jobs.
  5.2. **Privacy**
    ● This challenge is currently being legislated worldwide. We need to balance privacy with the need to gather information that can help address security breaches or fraud, while complying with associated legislation.

  5.3. **State-sponsored espionage**
    ● This challenge highlights the need to protect critical data from politically or financially motivated threats. Critical data includes the information needed to run network attached infrastructure and drive innovative solutions.

  5.4. **Social bullying**
    ● Even though we tried to provide a solution for the problem of social bullying, the extent to which that solution solves the problem is definitely not 100%. Implementation of time

Challenges	Manageable/Unmanageable	Solution/Reason
Digital Divide	Unmanageable	The fact that there exists a difference in the price of a smartphone and a normal phone in the market which leads to the digital divide is beyond the scope of the our subsystem and in fact the entire system. Hence, this challenge remains a challenge.
Privacy	Manageable	Secured connections, encrypted votes to prevent hackers from eavesdropping and tampering with the connection
State-sponsored espionage	Manageable (to most extent)	Having a strong security infrastructure to protect the system

		from such threats.
Social Bullying	Manageable (to some extent)	● Provide network security ● Limited window for voting

6.   References

6.1. Electronic voting (wikipedia)
https://en.wikipedia.org/wiki/Electronic_voting#Documented_problems_with_electronic_voting
6.2. Sandeep Mudana (University of Auckland)
https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/sr.pdf

Subsystem 5: Awareness and Reaching Out

1. **Introduction**

1.1 Scope
- The subsystem is only limited to the people who are eligible to vote
- The subsystem makes sure that the percentage of population voting is maximized after using this system.

1.2 Purpose
- As the name of the subsystem itself justifies, the system strives to provide awareness to the people to get adapted and habituated to the current digital world's mobile based voting system.
- To achieve this, the subsystem uses different mediums which enhances the way to reach required target
- This also operates on the time and cost constraints which is an important factor in the current days busy world.

1.3 Overview
- To understand the importance of voting using mobile and convenience of voting
- Make them believe in the security of their vote.

2. Characteristics
- The subsystem will have the following characteristics:
- Proper motivation and volunteering for people to attract more users to use the new system.
- More people to get adopted to the current digital world by proper campaigning on how to use the app and enable users to vote efficiently.
- Time efficiency : Saving a lot of time by not standing in long queues, going to polling booths and getting stuck in traffic. Also fast way to get election results.
- Cost efficiency : No manpower needed and no maintenance costs of the polling booth.
- Increase in the percentage of votes so as to form an efficient democratic government. (As more people vote, the accurate the government formed is)

- More people coverage. Examples:-
  - Many lazy people can't go to polling booths and give their vote. In spite of the vast effort involved in transport, they do ignore.
  - Not all would be free enough to go to their home town and give vote. Not being free include need for job leave, 18+ aged students having examinations at that time etc.
  - In that way, this system can also cover such people.

3. Requirements
- A supportive and engaged community to create awareness among the people.
- Good interactions among different communities
- Finding the person towards whom people will be receptive(Socially influential people).
- Conducting campaigns in the form of advertising and radio.
- The preparation and distribution of communication materials containing key messages on Elections (posters, brochures, ...
- Campaigning people should be able to properly communicate with the local people in their respective regional languages.
- Present the information in the languages of each state.

4. Objectives
- Picking the effective social media to spread about the system.
- To sensitize the voters about the importance of participation in an election process to ensure responsive,accountable and democratically elected government.
- To persuade minorities, the homeless, disabled persons, and many others who lack access to the vote for a variety of reasons including poverty, illiteracy, intimidation, or unfair election processes to participate in the election process
- To ensure that people understand their right as voters and exercise that right with full knowledge and responsibility.
- To impart knowledge on voting procedure.
- To ensure that climate or location does not hinder casting of the vote.
- To make the system comfortable from user's side by reducing the effort needed by users. Examples:-
  - Huge rush involved in the public transport which users need to reach the election venues.
  - Elections generally take place in May, the duration of peak summer. In such unfavourable climatic situations also people have to adjust with the environment standing in the long queues. As a result of long exposure, it may lead to sun-stroke for some delicate people. (Make the system keeping user's health in mind).

5. Implementation

    5.1 Sublevel-1:

- Man-Man-approach : There are two ways:
  - One way is via distributing pamphlets using volunteers in public places on the new system keeping the educated in view.
  - Peer-to-peer spreading of information. People knowing about this should be able to spread it to their neighbours. This, just being a conservation would be useful independent of being educated or uneducated.

    5.2 Sublevel-2:

- Social-Media-approach :
  - Living in a digital world, people can get proper awareness via social media. Awareness could be provided via advertisements, radio, TV news channels headlines/scrollings or displaying them in news feed online. As most of the people are deeply immersed in social media, this would be a great idea to get the matter spread faster. Alternatively, radios help the uneducated to get awareness about the new system.
  - Most famous social network sites worldwide as of January 2018. Facebook(2167 Million users) , Youtube(1500 Million user),whatsapp(1300 million users).

6. Table of Challenges
- ○ **Challenges that still remain**
    - ● Those who can't afford to buy a mobile.
    - ● Unavailability of proper network in rural areas.
    - ● The public perception would need to be changed and use of mobile voting system should be encouraged.
    - ● Takes a lot of time for this system to get implemented.

Table representing challenges:

Challenges	Manageable / non manageable	Reason
Inability to buy a mobile	Non manageable	Extreme Poverty
Networking Issues	manageable	Increasing more ISP's

Time Constraint	Non manageable	Takes time to know the importance of the system
Public perception	manageable	Could be achieved by more campaigning

7. References

- ○ **http://www.socialfish.org/2012/08/online-voting-advantages-and-challenges-for-associations/**

- ○ **http://www.elections.in/political-corner/voters-awareness-and-its-importance/**

8. Use-Case Diagram