Virtual Election Booth

CS6362 - Computer Security & Privacy

Collins O. Oyedemi

Reem A. Alhathal

Paxton L. Walker

Abstract

The electronic voting system provides various advantages for voting and saves significant resources in the process of voting, collecting and counting of ballots. This implementation will provide a secure way for people to vote online, which also eliminates the hassle of physically being present at designated election locations. However, for all the above savings electronic voting systems must provide security in each stage of the process to avoid any compromise of the authenticity of the results. This project aims to provide one such secure framework by implementing a secure online election voting protocol which has the ability to maintain privacy, also a goal was to use this platform for finding the statistics of who voted and who did not vote.

In short, this is a secure, cost saving and easy to use one step online voting system. The project aims to improve features of the current voting system which are currently lacking. The phone or a personal workstation is a better and more convenient option for a user to vote with. Ways to improve the voting system interface should, therefore, be designed and developed in order to make voting more convenient in a secured way

**Table of Content**

**Chapter 1  
Introduction**

**Nature and Significance of the Problem**

every legal citizen of a democratic country like the United State is entitled to casting a vote and the statistics shows that about 50% of the population still cast their vote on a ballot paper and some has to be physically present on the voting center which may cause apathy for some voters and unless people choose the right candidate policies cannot be turned into reality making it imperative that all eligible voter find a convenient approach to casting their vote.

By taking advantage of the latest advancements in information technology, cryptography and the world wide web, the voting process can be made virtual while at the electorates convenience which plays a major role in eliminating the hitches in the current voting system which include longer voting time and counting of ballots.

**Objective of the Study**

The aim of this project is to implement an effective and secure virtual voting system.

Electronic voting (e-voting) will go a long way to solve the challenges attributed to traditional paper-based voting and lower the costs of voting. Several security requirements should be met, such as verifiability, recall, identifiability, vote uniqueness, tally correctness, unique identification for every voter.

We will cover and answer the following area in the project implementation:

· What are the entities in the virtual election system?

· securing the voting system?

· Technologies used to develop the secured virtual election booth?

**Definition of Terms**

In the attempt by the Virtual Election booth to implement secured authorization and authentication mechanisms to in casting a vote, legitimate users would be authorized through a secured process which include the CLA, CTF, and Voter verification.

Below are the tasks that each entity is capable of or authorized to perform:

***CLA (Central Legitimization Agency).*** The task of the CLA is to certify the voters. The CLA assigns validation numbers to the voters and maintains a list of validation numbers and voters to avoid any voter from voting twice.

***CTF (Central Tabulating Agency).*** The task of the CTF is to count the votes. CTF receives the votes and the validation number from voters and records the vote for a particular election candidate and updates the validation number as "voted" to prevent the same voter from voting twice.

***Voter validation.*** The person who will be using the electronic voting system to cast his vote after being assigned a validation number which is randomly generated by the system.

**Summary**

The virtual voting system provides various advantages for voting and saves significant resources in the process of voting, collecting and counting of ballots. The system not only eliminates the hassles of physically presenting oneself to vote on a ballot, it provides a secure system that eliminates doubt in the computed result.

This project aims to improve features of the current voting system by providing a secure framework by implementing a secure online election voting protocol which can maintain privacy. This voting system can itemize the voting statistics on a spot by identifying the numbers of those who assessed the system to cast a vote or not. Assessing the voting system can be achieved via the use of a smartphone or a personal computer which is a better and more convenient option for a user to vote.

In the following chapters, we will be examining the voting system interface design in detail and develop it to achieve a more efficient and secure voting system.

**Chapter 2**  
**Literature Review on Virtual Election Booth**

In this chapter, the background related to the problem of voting systems is described in depth and the literature that supports and encourages the building of a virtual election booth is discussed.

As the world watched the electoral drama unfold in the US 2020 election, people started wondering, “Wouldn’t all our problems be solved if they just used Internet Voting?”. People all over the world soon started taking a hard look at their voting equipment and procedures and trying to figure out how to improve them. There is a strong inclination towards moving to Electronic Internet Voting – at least, in order to enhance voter convenience, increase voter confidence and voter turnout.

Many from sundry quarters have suggested that electronic voting, where the voter can securely vote from a remote location, seems to be the best step forward as it provides better voter convenience, and at the same time, does not compromise security.  
Electronic voting refers to the use of computers or computerized voting equipment to cast ballots in an election. Sometimes, this term is used more specifically to refer to voting that takes place over the Internet. Electronic systems can be used to register voters, tally ballots, and record votes.

In a report assessing the magnitude of the voting problems and issues including voting procedures, voting equipment, voter registration, polling places, absentee and early voting, ballot security, cost and public finance of elections, etc. their root causes and how technology can reduce them, A framework is agreed upon in which is a Modular Voting Architecture (MVA) in which vote generation is performed separately from vote casting, and the MVA forms a permanent audit trail, the importance of which cannot be overstressed. Here, the vote generation machine can be proprietary whereas the vote casting machine must be open-source and thoroughly verified and certified for correctness and security.

Electronic Voting according to Rivest addresses issues like the secure platform problem and the (im)possibility of giving a receipt to the voter. Therefore, the use of e-voting systems has the capability to reduce or even remove unwanted errors that might be caused by humans, and also e-voting is more reliable and can also handle multiple modalities which help physically handicapped (such as voice assistance) to vote and increase scalability for huge elections. With physical voting machines, it is not always possible for people like soldiers or immigrants to vote. If a potential voter does not live in the respective geographic proximity to the physical voting machines, the use of e-voting is also an excellent mechanism that doesn't require geographical proximity of the voters.

Ensuring that voting systems are secured and avoiding potential rigging is a complex task for the respective election departments or government agencies if the process is not e-voting.

The virtual election booth system can provide assurance of securing sensitive information of the voters, make every voter sure that their vote has been taken into consideration, that no duplicate votes are recorded to ensure no rigging of votes has occurred, and implement optional modules which help in various ways like generating data to determine who voted and who did not.

Also, current advancement in AI and data analysis can be implored to our advantage by retrieving data from the modular systems while analyzing it to develop voting strategies and to increase the voter’s empathy in the future.

**2.1 Background Theory**

Virtual Election Booth is a scheme that primarily facilitates the capturing, recording processing, and delivery of votes in a digital format.

It is a known fact that the electioneering process, which involves the registration of voters, collecting election votes, and counting of ballots, is an enormous task subject to flaws. The implementation of an Online Virtual Election Booth will offer an approach to voting that is more reliable than pressing a thumb on paper. Since the implementation of a voting system is multifaceted and requires a concerted approach, such an implementation must be accurate.   
Improving voting systems requires an interdisciplinary, collaborative approach. The systems must be accurate, consistent, cost-effective, secure, and usable. At the same time, it must be available and accessible at the right time for voters to cast their ballots, without compromising their confidentiality and the authenticity of the results.

Traditional elections have some important features, which the electronic voting, to be usable, should have also. We briefly sketch the most important ones of them:

**Voting committee**: takes care of voters, allowing only eligible voters to vote and ensuring that every voter votes at most once. After the elections, the voting committee counts the votes and publishes the result. Also, there is an implicit trust to believe that the voting committee is honest, and it would not disrupt the elections.

**Authorities**: Authorities manage the elections and oversee the voting committee. They have large computing power, and they can store large amounts of data in secret. Authorities can also act as voters.

**Voters**: In general, voters are not willing to bother with complicated and time-consuming voting processes. Therefore, voter’s actions and computations during the electronic voting should be kept at minimum, realizing the vote-and-go concept. Voter can abstain from voting if he wishes to – he need not participate in the voting, or he can stop his voting any time before it is finished resulting in his vote not counted.

**Votes**: The structure of votes depends on the type of elections. More precisely, it depends on the question that is put forward to voters in the election and possible answers.

The secured online voting protocol should be capable of providing a secured voting process and prevent cheating. Therefore, the requirements to achieve aforementioned requirements for it to be usable in practice, are as follows:

**Eligibility**: Only eligible voters can cast the votes. Every voter can cast only one vote.

**Privacy**: No coalition of participants (of reasonable composition) not containing the voter himself can gain any information about the voter’s vote. By reasonable composition we mean coalition of at most t authorities and any number of voters. We say that information-theoretic privacy is achieved when the ballots of the voters are indistinguishable independent of any cryptographic assumption; otherwise, we say that computational privacy is achieved.

**Individual verifiability**: Each eligible voter can verify that his vote was really counted.

**Universal verifiability**: Any participant or passive observer can check that the election is fair: the published final tally is really the sum of the votes.

**Robustness**. Faulty behavior of any reasonably sized coalition of participants can be tolerated. No coalition of voters can disrupt the election and any cheating voter will be detected.

**Fairness**: NO vote can be duplicated and a counted vote cannot be changed.

**2.2 Development, Software and Frameworks**

The programming language implored in this project is the python programming language, using the MVC architecture, where we create the model, view and map the template to the URL where it is processed and served to the user. The MVC architecture encourages flexibility while building this project and helps to leverage control over the software, and to add in relevant third-party libraries when they’re completely necessary.

Python, which is an interpreted, object-oriented, high-level programming language with dynamic semantics is chosen because of it’s security feature to prevent basic exploitation of the software and because of the object oriented nature of python, its data in the form of fields, attributes, properties and code in the form of procedures or methods make development easier to develop, reuse and maintain.

**2.3 Summary**

The basic model and drawbacks of the traditional voting systems are discussed, and how the problems can be solved by implementing a virtual election booth.

The approach was further taken to implementing an MVC model with Python. The cryptographic techniques, authorization, and authentication techniques to overcome the drawbacks of the existing systems will then be implemented.

**Chapter 3**

**Methodology**

**3.1 Project Framework**The framework of this project is a secure election protocol that entails voting with two central facilities: a Central Tabulating Facility (CTF) and a Central Legitimization Agency (CLA). CLA's main function is to certify the voters, while CTF's main function is to count votes. These procedures outline an auditable approach that can be appraised to meet the baseline.

The protocol that this project will implement must satisfy the following requirements:

• Only authorized voters can vote.

• No one can vote more than once.

• No one can determine for whom anyone else voted.

• No one can duplicate anyone else's votes.

• Every voter can make sure that his vote has been considered in the final tabulation.

• Everyone knows who voted and who didn't.

3.2 **Project Specification**

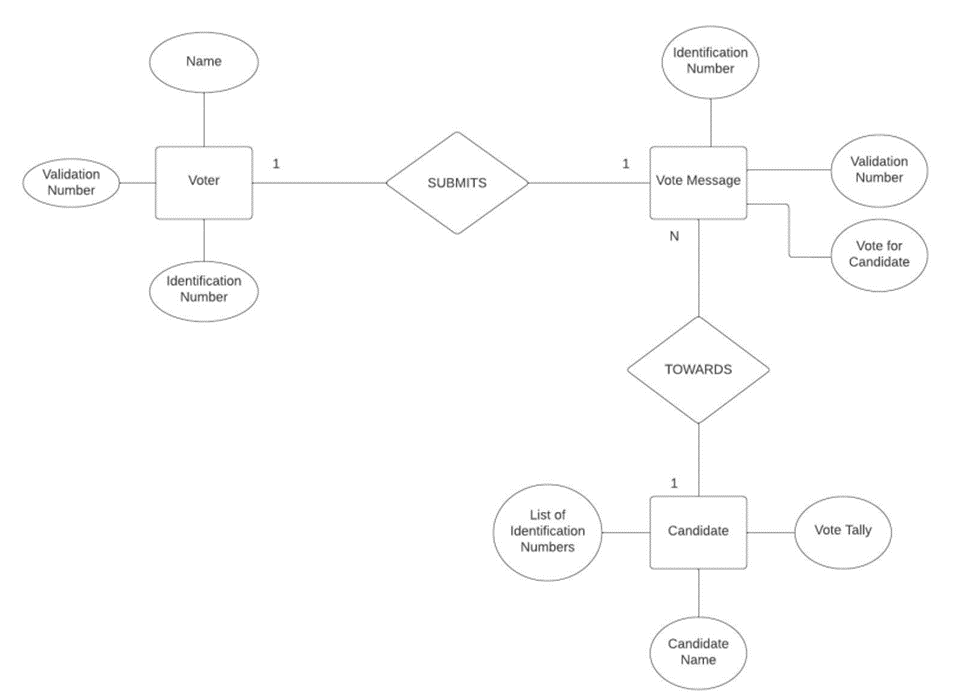
This project will simulate an election booth that will use a secure election protocol described in Applied Cryptography by Schneier to validate votes and ensure that no individual votes more than once. This protocol splits the responsibility of verifying the voters and their votes among two separate facilities: the Central Tabulating Facility (CTF) and the Central Legitimization Agency (CLA).

The Central Legitimization Agency certifies the voters. The CLA will give each voter a validation number upon request and then keep track of which validation numbers belong to which voters. This record is then given to the Central Tabulating Facility.

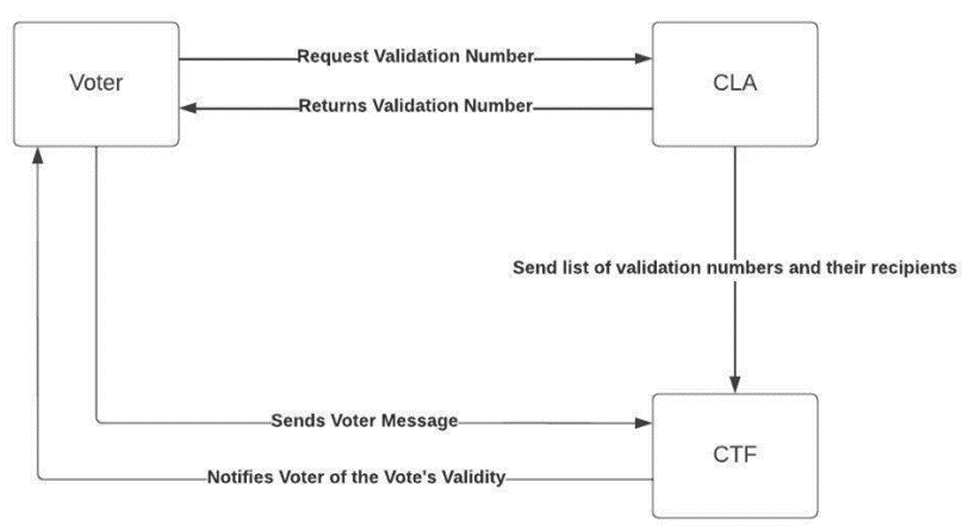
The Central Tabulating Facility certifies and counts the votes. Using the record of validation numbers, the CTF will verify if a voter is cleared to vote. The identification number, a value randomly chosen by the voter, will represent the voter in the CT F 's vote tally. The CTF will then print the results of the vote, including the total number of votes and the amount of votes each candidate received.

3.3 **Design**

This section is an overview of the design of the Virtual Election Group project. For this project, we developed an entity-relationship diagram, or ERD, and a block diagram that describes the actions and data flow between the voter and the two facilities: CLA and CTF.

**Entity-Relationship Diagram**

Above is an entity-relationship diagram of the Virtual Election Booth. The main entities of this system are the voter, the vote message, and the candidate. The voter is identified by a unique identification number, which will correspond to the voter's name. The voter will have a validation number that will help the election booth keep track of who already voted and if a vote message is valid. The vote message will include the identification number of the voter, the vote for the candidate, and the validation number used to gauge the legitimacy of the vote. Each candidate in the election will be identified by their name and will have a tally of votes towards them as well as a list of identification numbers that correspond to the people who voted for them.

Block diagram  
 

Above is a block diagram that represents the flow of information between the voter and the two major facilities of the system, namely the Central Legitimization Agency (CLA) and the Central Tabulation Facility (CTF). The voter will request a validation number from the CLA. In response, the CLA will return a validation number. As the CLA serves voters, it will keep a tab on all of the validation numbers and their recipients. It will then send this list for the CTF to use.

When the voter constructs and sends a vote message to the CTF, the CTF will use the list it received to check the validity of the vote and will notify the user accordingly.

**3.4 Algorithm**

Step 1 — Communication between Voter and CLA

Voter to CLA

Each voter sends a message to the CLA asking for a validation number. The voter securely sends a random identification number to the CLA and requests for a validation number.

CLA to Voter

The CLA generates a validation number and sends it to the voter. The CLA also keeps a list of the validation numbers' recipients, In case someone tries to vote twice.

Step 2 — Communication between CLA and CTF

CLA sends the list of validation numbers to CTF.

Step 3 — Communication between Voter and CTF

Voter to CTF

Each voter creates a message and sends it to the CTF with the validation number, the random identification number and the vote.

CTF to Voter

CTF receives the message; it would cross reference the validation number with the list it received from the CLA and update the list for all voters who have voted. If the validation number is there, the CTF crosses it off (to prevent someone from voting twice).

Step 4 — Election Results

Once all the votes have been received, the CTF publishes the results. The result also includes a list of random identification numbers of voters who cast their vote to a particular candidate.

**Chapter 4  
Design Implementation and Codes**

**4.1 Security Support**

Security in virtual election systems is implemented by hashing sensitive data like social security numbers using secure hash algorithms. By hashing the SSN at the stage of registration no authority will be able to know the private details of voters which are used for the authentication process such as SSN. This message digest class provides applications with the functionality of a message digest algorithm, message digest object then starts out initialized.

Message digests are secure one-way hash functions that take an arbitrary-sized amount of data and provide an output of a fixed-length hash value. The hash is calculated using the message digest algorithm i.e., SHA-1 in this case. The SHA-1 algorithm used in the virtual election system and was developed by the National Institute of Standards and Technology (NIST) and National Security Agency (NSA), implemented by creating a message digest object. SHA-1 produces a 160-bit (20 bytes) message digest used for creating unforgeable digital signatures. This is slower than the Message Digest 5(MD5) algorithm but is more resistant to brute force than the MD5 hashing algorithm and thus is more secure.SHA-1 is a one-way hashing function. It is easy to compute the SHA-1 message digest of a document; however, it cannot go backwards and compose a document based on a given message digest and it is not an encryption method. To ensure the security, privacy and the integrity of the voting system a hashed validation number is generated during the time of registration and saves the hash of the validation number instead of the validation number itself.

Therefore, in case of an attack on the database, the sensitive details will not get compromised and the data won’t be misused by hackers. If any unauthorized users or hackers get a hold of the sensitive data like SSN or validation numbers, they could spoof or fabricate it by appearing to be authorized users by knowing details such as SSN and validation number which are enough to vote which appears to be a complete failure of the Virtual voting system. To avoid this, the hash value of the sensitive information is generated and saved in the database rather than storing the plaintext equivalent of it.

Transparency in the voting process is ensured by making the Central Legitimizing Agency (CLA) unaware of which voter had exercised their vote until the Central Tabulating Facility(CTF) sends the voting status of the voter, and towards which candidate the vote had been exercised, is only with the CTF to CLA. This technique is implemented in the virtual election system by creating two different tables for CLA and CTF while designing the database, so that the above-explained criteria can be successfully implemented. The results will be only released by the CTF. To take care that a voter has voted only once there must be proper communication between CLA and CTF. This process is implemented in a proper flow i.e. at the time of registration the CLA sends the hash of validation to CTF and the CTF gets a record of it.

When the voter tries to exercise their vote by entering his validation number and SSN it gets authenticated and is redirected to the CTF. Where the voter votes for a candidate, this information is stored at the CTF and the voting status of the voter is changed at the CTF side and this status is communicated even to the CLA. CLA updates the voting status against that particular validation number and voter status is changed to “VOTED”. If the same user tries to vote again, the CLA will not oblige the request and displays a warning message. The database is designed in a way that there are no redundancies in the data which could lead to issues. The database design properties for an efficient database are commonly described as atomicity, consistency, isolation and durability (ACID), have been implemented which results in a safer and more efficient system.

Session timeouts have also been implemented. It represents the event occurring when a voter does not perform any action on a website during an interval of some specified time period in the virtual election system, in this case a session timeout duration of 60 seconds. The event, on the server side, changes the status of the user session to “invalid” (i.e. "not used anymore") and instructs the web server to delete all data contained in that session. This helps in maintaining the authenticity of the session and unauthorized use is prevented.

**4.2 CIA Implementation**

Confidentiality, Integrity and Availability are three main security goals of the virtual election booth which addresses the following three goals:

* Protect the confidentiality of the voters
* Preserve the integrity of the voters and the casted vote details
* Promote the availability of the virtual election system to vote from a remote location

***Confidentiality***: To protect the confidentiality of the voters is one of the three security goals of the virtual election system. Various techniques have been implemented to provide confidentiality to the voters.

In the first step, when the voter enters the details in the registration page and clicks on submit, the virtual election system validates the information entered by the voter and generates an alphanumeric validation number which is unique for each voter. This validation number is used by the voters to login into the system. The generated validation number and all the sensitive information of the voter are hashed using the MD5 hash algorithm. Therefore, the data cannot be compromised from the database as the sensitive information is hashed.

Even the CTF and CLA cannot know the details of the voter, CLA can just know if the voter has voted but cannot know who the specific voter has voted for.

***Integrity:*** All the necessary precautions have been taken to protect the integrity of the data.

The virtual election system takes care to protect the integrity of the data, at every point of time the voter tries to vote; the data is saved either after the voter has cast his vote completely or the system will remain the same before the vote has been cast.

***Availability:*** The CTF is authorized to start the elections, stop the elections, show the results or lock the results. Once the CTF has authorized to start the elections the virtual election system is available to the voters until the CTF again stops the election process.

**4.3 Tools**

The following tools are deployed in the implementation of the project:

Front-end

• HTML, for building the webpage.

• CSS, for controlling the style of HTML.

• JavaScript, to allow frontend computing.

Back-end

• The back-end of our project will be programmed using Python which is a high-level programming language.

Database

• Our database will be stored and managed using Microsoft SQL Server.

**4.4 Screen-Shot**s

4.3 Codes

**Chapter 5**

**Summary**

Electronic Voting has been attracting considerable attention during the last years. This fact is based upon interest and attention devoted to making democracy and governance open which is founded in problems with domestic election systems, e.g., lacking flexibility with respect to timeframes and physical accessibility of polling stations, which progressively prevent citizens to cast their vote at these places.

Interest in e-voting has taken root in various quarters: government, parliaments, electorate, academia, and other industry - with each having sometimes conflicting interests. They can differ with respect, e.g., to speed, individual leadership, safety, user friendliness, etc

Several countries, worldwide, have started or considered starting thinking and experimenting as well as implementing e-voting. In Europe, a variety of e-voting schemes is developed, tested, and piloted across the continent. In the USA, electronic voting at polling stations is widely practiced - progressively followed by Mexico and Brazil and considered by other Central and Latin American countries.

In addition to e-voting activities by countries, a remarkable development on e-voting by international organizations is the standard-setting exercise within the framework of the Council of Europe (CoE).

However, considering the introduction of e-voting, legal, and political challenges must be defeated, and this step, once achieved, subsequently gaining the interest of the public, meaningful advances on the way to e-voting can be achieved.

**Future Improvement**

Future Improvement to this project may include the inclusion of haptic feedback and ability to verify a voters ballot using audible or voice recognition pattern. This may be an advantage to enabling physically disabled persons to cast their ballot.