**Secure Electronic Voting**

**By: Robert Irwin and Pete Mollica**

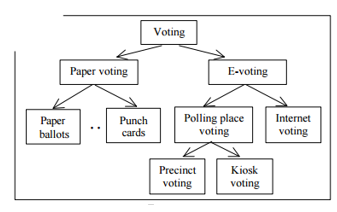
**Introduction:**

Voting is one, if not the most, important practices a citizen can exercise in a democratic society. However, we find that every election there is a large number of eligible voters who do not vote. For example, in the 2016 presidential election 95,899,111(41.4%) of the eligible United States population did not vote. There can be many reasons that contribute to this, including that some voters may not be able to get to the polls. We also hear about questions of fraud, illegal voting, inaccuracies in the voting tally, and the long amount of time it takes to tally all of the votes. However secure electronic voting or secure internet voting can help address a lot of these issues.

This project aims to address some of these issues through a secure electronic voting system using Internet Protocol (IP). Our proposed system uses symmetric encryption for voter verification and vote casting. These are kept as two different parts of the system to ensure that a vote cannot be attributed to a specified voter. In the following sections we will discuss some of the background and system requirements of secure electronic / Internet voting. We will also discuss our proposed implementation in more detail.

**Background:**

According to Wikipedia, electronic voting “is voting using electronic means to either aid or take care of the chores of casting and counting votes”. This can cover a range of different implementations from basic data transmission to fully-functional online voting. We can visualize the voting process in figure 1, below.



**Figure 1: Types of Voting**

If we look specifically at the E-voting part of figure 1(right) we can see that electronic voting can be broken up into two main sections, polling place voting and Internet voting. Polling place voting would be very similar to a typical vote polling place, where your registration is checked and vote in paper ballot voting machine. However, the difference would be that instead of voting on a paper ballot machine you would vote on an electronic machine, such as a kiosk. The other main type of electronic voting is full Internet voting, where an eligible voter would be able to vote from the comfort of their home. As one can imagine a full secure internet voting system is much more complicated than say a kiosk voting system. For this project we are simulating a kiosk type implementation.

Both types of electronic voting implementations have a basic set of requirements. A secure electronic voting system would need to meet the following general voting principles:

* Only eligible voters can vote
* Each eligible voter only get one vote
* The vote is secret
* Each vote gets counted
* The voters trust that their vote is counted

More specific system design requirements, according to the *Internet Policy Institute*, are the following:

* *Authentication*: Only eligible voters should be able to vote.
* *Uniqueness*: No voter should be able to vote more than once.
* *Accuracy*: The system should record the votes correctly.
* *Integrity*: Votes cannot be changed without detection.
* *Auditability*: There should be a reliable and demonstrably records
* *Reliability*: Systems must work robustly, even when faces with numerous failures.
* *Secrecy*: Each vote cannot be connected to a specific voter.
* *Non-coercibility*: Voters cannot prove that they have voted.
* *Flexibility*: The voting equipment should allow for a variety of questions and formats.
* *Convenience*: Each voter should be able to cast their vote with minimal skills.
* *Certifiability*: Systems should be testable against different and specific criteria.
* *Transparency*: The whole process should be easy to understand.
* *Cost-effective*: Should be efficient and affordable

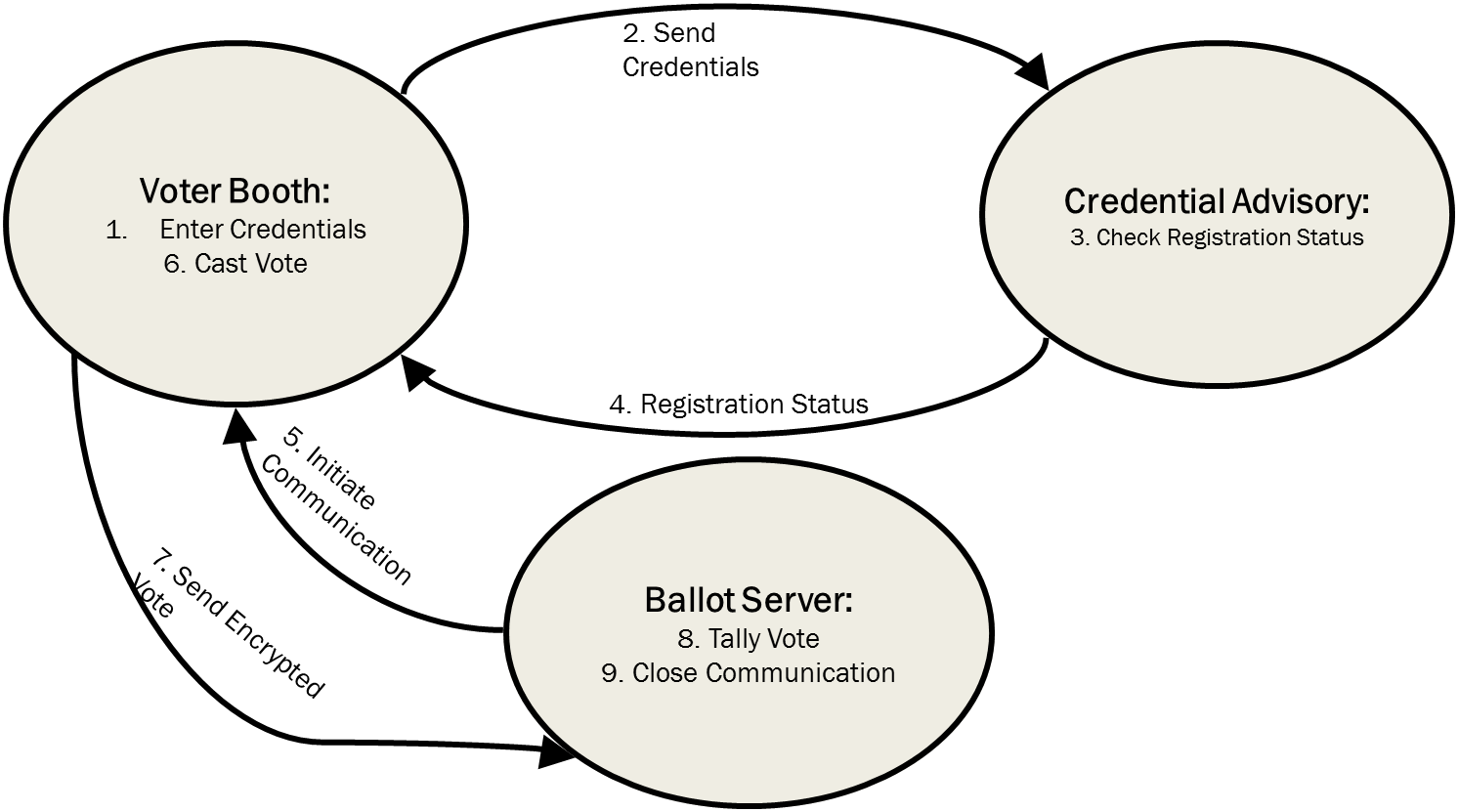
It is important to discuss how the secure electronic voting problem is typically approached. There are generally 4 stages or phases, which are:

1. *Registration Phase* – Prior to Election Day an eligible voter will need to register as a valid voter. This process would not change from the current voter registration process.
2. *Validation Phase* – On Election Day before an eligible voter will be able to cast his/her vote they will need to be verified. For example this could be done by providing a login and password along with other personal information to be compared against a national database.
3. *Vote Casting* – The process by which the eligible voter’s vote is sent to a tallying station. This is at the heart of the problem and is the most important aspect of secure electronic voting.
4. *Tallying Phase* – All encrypted votes are decrypted and counted for each candidate efficiently and accurately.

Our proposed system attempts to address all of these requirements and the specific implementations will be discussed in more detail in the following section.

**Proposed Methods:**

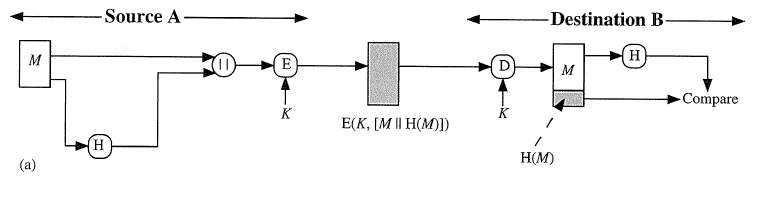
A general overview of our system can be visualized below in figure 2:



**Figure 2: Overview of Proposed System**

In our proposed method we have 3 main entities which are the Voter Booth, the Credential Advisory, and the Ballot/Tallying Server. The voting booth is the main entity, which will talk to both the Credential Advisory and Ballot/Tallying Server. The Credential Advisory stores all of the credentials of registered voters and keeps track of whether or not that eligible voter has voted or not. The Credential Advisory maintains this record as a blockchain, which is a decentralized database. The Ballot/Tally server takes the result of the ballot from the Voter Booth and stores the candidates and the counts for each candidate. It is important to note that the Credential Advisory and Ballot/Tally server are two separate entities that do not talk to one another. This is to help ensure that no vote can be associated to a voter.

Secure communication between the booth and the other two entities is done across TCP/IP using symmetric encryption. Specifically, we use AES-256 with Cipher Block Chaining (CBC) to do encryption and decryption. We also include sha-256 hash, which insures authentication and data integrity. We can visualize the structure of the system below in figure 3.



**Figure 3: Authentication and Confidentiality Structure**

**Conclusion:**

The proposed method addresses some of the issues of electronic voting such as:

* Data Integrity- through sha-256 as well as TCP
* Voter Verification-through the blockchain
* Anonymous Voting-through the blockchain
* Vote Authentication-through AES CBC

With this method of cryptographically secure e-voting, some issues are not addressed, and vulnerabilities still exist. The current system is susceptible to replay attacks, in which the attacker keeps casting the same vote. This problem can be solved with a key distribution center that gives each user and the ballot server their own symmetric key. In the current state of the design, there is no mechanism in place that handles the scenario in which the symmetric key is compromised. This leaves the system vulnerable to man in the middle attacks if the key is compromised.