A. Lopez, “Many Electronic Voting Machines Are Not Secure. One County Is Trying To Fix That,” *NPR*, 13-May-2018. [Online]. Available: https://www.npr.org/2018/05/13/609443797/many-electronic-voting-machines-are-insecure-one-county-is-trying-to-fix-that. [Accessed: 25-Aug-2018].

* The electronic voting machines in Texas are old, and the state is looking to replace them due to design flaws and the hacking risks that come with old equipment. Many say that the electronic voting machines are easier to use, more convenient, and more accessible. However, many voters also want a machine that will produce a paper trail, to have physical confirmation that their vote has been counted correctly. The main goal of the program written as a result was to be efficiently audible. Though the code has been written, the problem now proves to be finding a company that produces open source machines, a feature that would make the machines cheaper for the counties.

“Benefits of electronic voting,” *Smartmatic*. [Online]. Available: http://www.smartmatic.com/voting/electronic-voting/. [Accessed: 25-Aug-2018].

* Paper-based systems have an advantage in having physical representations of a person’s vote, a reassurance of sorts. However, this does not mean that the vote will be correctly counted. Issues such as a “hanging chad” can cause a miscount, printers can run out of toner, a voter could mark for two or more candidates for one position, or a ballot could be lost or destroyed. A DRE system stores votes in memory and counts them electronically. Many, however, have no paper trail. Assuming it is secure, fast, and reliable, a DRE system can be much better than a paper-based system. Ballots can be in any language, print can be enlarged, or audio can be incorporated for blind voters. Because it is electronic, there is no running out of ballots and counting takes less time with less risk of mechanical error. Human error, however, is still a factor along with security risks and bugs. In the best possible DRE, counting is instant, and recounts are not needed.

“How E-voting Works,” *HowStuffWorks*, 12-Mar-2007. [Online]. Available: https://people.howstuffworks.com/e-voting1.htm. [Accessed: 25-Aug-2018].

* Electronic voting means to vote via an electronic system that also counts the votes. It is seen in forward-thinking countries to help improve elections. For some people, the automated elections are more trusted because it is auditable and secure, reducing human error. For other people, the faster results helps to build trust. In some countries, the technology used in the voting process has actually improved voter education, registration, and turnout. Electronic systems allow for better accessibility. Auditability is a key component of this company’s electronic voting systems, including a paper receipt for each voter. This makes recounts and audits easier and has, in fact, become a new standard in electronic voting. This also makes it easier to detect any hacking attempts as the electronic vote count would be different from the paper vote count, it the system was hacked into at all. Security is a high priority. One such security measure is redundancy, storing the data in many different locations that can be checked against each other. The features of this company are fast and accurate registration, faster voter authentication, preserving voter secrecy, and making every step secure. The company also advertises the ability to adapt the voting machines to each country’s requirements and laws.

“Electronic voting systems: Requirements, design, and implementation,” *Egyptian Journal of Medical Human Genetics*, 24-Jul-2006. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0920548906000754. [Accessed: 25-Aug-2018].

* Manual voting can have errors such as miscounting and delays, voting electronically can nullify or reduce some of these errors as well as increasing voter engagement and allowing votes to be counted from multiple different platforms and devices at any time.There are multiple types of electronic voting machines, such as those that scan the paper ballots, those that count the votes directly, those that must be run at registered areas and kiosks, and those that can be used from home. The e-voting system requirements listed by this paper are that all voters are registered and eligible, once someone casts a vote they cannot cast another, all valid votes will be counted, all invalid votes will be discarded, and a vote cannot be tampered with or viewed by anyone during the voting process. Voting systems that connect via the internet must allow multiple people to vote at one time, multiple elections to be run at one time, multiple access platforms at any time, and have high availability. Another feature mentioned by the paper is the ability to have election specific requirements. The paper discusses multiple types of platforms that may need to host or access such a system such as cell-phones, personal computers, and SMS servers. A system fulfilling these requirements was implemented using a server to host a modem database management system (DBMS) along with a number of software tools.

“E-Voting Systems for the IACR,” *International Association for Cryptologic Research*. [Online]. Available: https://www.iacr.org/elections/eVoting/requirements.html. [Accessed: 25-Aug-2018].

* This page is the requirements and evaluation criteria page the International Association for Cryptologic Research (IACR) was using while debating replacing the current mail-based voting system. The system must be usable (they use the word “exist”), be user-friendly, and be easy to use. Voters must be able to vote exactly once, must be verified as eligible, individual votes must remain secret, the system must be auditable, and everyone must be able to verify that only valid votes were counted, the tally was accurate, and each voter can see that their vote was counted. The system must also be accessible, available, and reliable. Additional, non-required, features include having quick-fix options for outages, offering resistance to viruses and malware, minimalizing the trust needed to operate the system, allow voters to cast “fake votes” to be discarded during counting in the event that they are being coerced, defending against attacks based on vote correlation. Specified non-requirements of this system are complete resistance to coercion and vote-selling, a paper trail, and allowing for the extension of voting deadlines and such adjustments.

“South Carolina Voter Registration Information,” *Voter History Statistics for Recent SC Elections*. [Online]. Available: https://www.scvotes.org/south-carolina-voter-registration-information. [Accessed: 27-Aug-2018].

* In order to register to vote in the state of South Carolina one must possess proof of US citizenship, proof of South Carolina Residency, one must be at least 18 years of age, one must not be in a public prison resulting in the conviction of a crime, one must be mentally competent and have not be convicted of a felony. If one is convicted of a felony, the sentence must be served in its entirety including probation or parole or have received a pardon for the conviction. Students may register to vote while attending college within a South Carolina institution, however the student must register with the physical address of their dormitory. South Carolina provides multiple methods for voter registration, the first is an online resource, the second is by mail/fax/email with a completed voter registration form or one may register to vote in person at a local county board of voter registration.

R. Haenni, R. E. Koenig, and Wikström Douglas, *E-Voting and Identity 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4, 2015, Proceedings*. Cham: Springer International Publishing, 2015.

* In 2015, Switzerland proposed adopting a “Cast-as-intended veri’’cation” e-voting system. This system attempts to prove to the voter that their vote reflects what they indicated on the ballot. This system was created with the fear that malware may change the voter’s selection, thus this “verification” based e-voting system was adopted. The voter can check if their voting choices were received correctly by the voting servers via return codes. If the voter gets a code back that doesn't match their private return code, they can discard the vote with the suspicion that malware has intercepted their vote. However, some bugs were encountered when voters discarded their votes. Some voters were unable to cast a new vote, because the system thought the voter was attempting to vote twice.

Quora, “How Blockchain Will Make Electronic Voting More Secure,” *Hacker Noon*, 25-May-2018. [Online]. Available: https://hackernoon.com/how-blockchain-will-make-electronic-voting-more-secure-fba15d752bee. [Accessed: 27-Aug-2018].

* Recently, blockchain based e-voting has been brought up more frequently because of blockchain’s immutable and verifiable nature. Blockchain would make sure only one vote could be cast per voter, no votes could be deleted, and those in charge of counting votes would have a final and absolute record of every vote casted at any time. In addition, blockchain would provide a encrypted results to protect voter privacy. Due to voter results being immutable and immediately available it is proposed that utilizing blockchain in e-voting is highly more efficient than the status-quo.

“i-Voting,” *e-governance*. [Online]. Available: https://e-estonia.com/solutions/e-governance/i-voting/. [Accessed: 27-Aug-2018].

* In 2005 Estonia became the first nation in the world to participate in electronic voting, called “i-Voting”. Voters can cast their vote from anywhere in the world with internet connection. The voter logs onto the system using an ID-Card or Mobile-ID and casts their ballot. The privacy of the voter is protected because before the ballot reaches the National Electoral Commission the identity of the voter is removed. Voters can vote multiple times, however each time they vote their previous ballot is deleted ensuring that voters can cast a ballot that truly reflects their view. It is reported that this electronic voting system has saved estonians 11,000 working days.

K. Gjøsteen, “The Norwegian Internet Voting Protocol,” *Lecture Notes in Computer Science E-Voting and Identity*, pp. 1–18, 2012.

* In 2011 Norway ran a trial of internet voting during local government elections. In order to avoid the danger of coercion voters were allowed to vote more than once, unless the voter submitted a paper ballot. In which case, the voter would only be able to submit the single paper ballot cancelling the electronic ballot if one had been submitted previous to the submission of the paper ballot. Ballots were encrypted using a homomorphic cryptosystem. The ballots were then sent to a mix net, the mix net is supposed to ensure that that the output (the ballot) cannot be associated with the input (voter identification).
  + Homomorphic cryptosystem: a form of encryption that allows computation on ciphertexts. ( I had to look this up, because I had never heard of it before).