Securing Democratic Elections to Protect E-Voting System via Cryptography in the United States

Ekrem Ersen Emeksiz
Graduate Assistant, Cyber Forensics MS Program, University of Baltimore,
Baltimore, Maryland

Email:ekrem.emeksiz@ubalt.edu (E.E.E.)
Manuscript received May 8, 2024; revised June 7, 2024; accepted July 18, 2024
DOI: 10.18178/IJBTA.2024.2.2.70–77

Abstract: Electronic voting was proposed as an alternative and more reliable solution to the traditional voting system in the United States. Early efforts to integrate the old system into the new voting system consisted of various challenges. For instance, attackers, manipulators, or other criminal groups can collaborate with corrupt politicians and election officers who have falsified scores. Therefore, researches of various scholars were examined towards designing a highly secured e-voting system that would prevent hackers, corrupt politicians, and election officers from leveraging any form of fraudulent activities. The world cannot be a credible place without trustful elections to do anything. The purpose of this paper is to review the literature from different scholars and identify shortcomings in designing highly secured cryptographic methods to focus on current practices and future considerations of the United States`s e-voting system.

Keywords: E-voting system, Help America Vote Act (HAVA), Direct Recording Electronic (DRE) E-voting machines, E-voting frauds and cryptography, blockchain-based E-voting

1. Introduction

Elections are a prominent part of a democracy as well as a practice of basic human rights that are clearly emphasized in Article 21 of the Universal Declaration of Human Rights. Elections must be conducted fairly and periodically by the legitimate structure of a government and every eligible citizen has the right to vote to be elected or to choose their representatives in governments. The Constitution of the United States emphasizes the right to vote in three different Amendments (15, 19, and 26) to ratify fair elections. Dependable voting procedures are an indispensable way to secure fair elections in strong democracies [1]. Therefore, an electronic voting (E-voting) system is ideally designed for this purpose. E-voting replaced the traditional in-person-ballot system with digital installment with a secure voting machine in 2002 right after the US electoral fiasco of Florida State during the US Presidential Election in 2000 [2]. In parallel with policymakers, various scholars were examined towards designing a highly secured e-voting system that would prevent fraudulent activities to hinder corruption for the sake of maintaining a trustful democratic election. Furthermore, there is a growing cybersecurity concern over hacking into the e-voting system, especially after the 2016 election with the Russian government's involvement via social media campaigns as well as John Podesta`s e-mail compromised who was chairman of the Clinton election campaign [3]. Today one of the biggest security concerns of the e-voting system can be identified as maintaining voter`s privacy. Secrecy is the major component of the fair election process therefore protection of voter`s privacy must never be sacrificed. In addition to that fairness, receipt-freeness, coercion-resistance, individual verifiability,

universal verifiability, robustness, and double-voting prevention can be considered for holding country- wide secure e-voting implementation [4].

To maintain confidentiality, integrity, and availability on e-voting machines cryptographic solutions must be considered and already implemented in many states under the new regulatory and advisory process. Consequently, there are various types of cryptographic e-voting schemes stated by the authorities. Some of them are, mix-net-based e-voting, homomorphic e-voting, blind signature-based e-voting, blockchain-based e-voting, post-quantum e-voting, and hybrid e- voting. These are the proposed methods in the literature for better security and practical implementation. The E-voting system is highly controversial due to its security concerns. The main purpose of e-voting is to provide more accurate and faster election results, minimize human errors, more easiness for physically disadvantageous people.

This study will focus on the e-voting systems in the United States. It analyzes the current practices, the existence of state or federal level oversight mechanisms, private sector initiatives on e-voting fraud allegations, pitfalls of the current e-voting system, and finally it analyzes to design a robust technical structure for the e-voting system based on the most secure cryptographic method to protect voters' privacy as well as to preserve reliable election results.

2. Literature Review

Current e-voting policy varies from state to state, there are many experimental new e- voting methods taking place to implement in practice. E-voting policy is basically in how the U.S. Constitution describes authority on election processes. States are given the power to regulate election proceedings. This includes several responsibilities including registration, absentee voting, polling locations, counting votes, as well as costs for the election process. These responsibilities can be differentiated even at the local level as well. Controversy on e-voting system has been managed with a few fundamental laws. These laws are the Help America Vote Act (HAVA), Digital Millennium Copyright Act (DMCA), Uniform Computer Information Transactions Act (UCITA), and Voter Confidence and Increased Accessibility Act of 2003. The HAVA binds that there must be at least one Direct Recording Electronic (DRE) machine per county. The law, however, lets the states decide how they will implement the specific terms of the HAVA. The act does not establish what types of technologies to use, nor how many there should be per precinct. Overall, this law has not provided any national standards for electronic voting by the federal government.

Besides the main legislative bodies, the e-voting system has also been under the oversight of some independent commissions, and public and private institutions. The Election Assistance Commission (EAC) oversees assisting state and local governments with more e-voting devices under HAVA. The commission, supported by the National Institute of Standards and Technology (NIST), includes the Technical Guidelines Development Committee (TGDC), which guides the EAC on voluntary standards and procedures related to voting machines. Another example is the National Academies of Sciences, Engineering, and Medicine released a technical report regarding cybersecurity concerns about e-voting in 2018. According to the report, cybersecurity is a dynamic and constant challenge due to malicious threat actors' constant efforts to execute new attack methods to exploit vulnerabilities and cripple the system. Moreover, e-voting system uses the internet which is the most vulnerable to attack during data transmission. It is stated that e-voting mechanisms either remote e-voting or E-voting at polling stations are highly vulnerable to Denial of Service (DoS) attacks, malware attacks, and voter credentials thefts. Furthermore, the 2020 elections triggered mistrust in the electronic voting system. Many states converted their method back to paper ballots due to rigged voting machines and voter fraud cases [5]. It is stated that 93% of the nationwide votes had a paper record in the 2020 election. On the other hand, if a new system wants to be adapted, it must be trustworthy as the paper ballot. With Direct Recording, Electronic (DRE) voting machines must rely on electronic records

to be the true records of the ballots. DRE systems have their pros and cons. The advantage of a direct recording electronic system includes the fact that it can accommodate persons with various disabilities and provide features that protect against known voter errors.

Most of the state governments have adopted paperless Direct Recording Voting Systems (DRE) without carefully screening the security vulnerabilities of vendors' products. Up until recently, such vendors` systems have been "certified" for use without any public release of the analyses behind these certifications. the US Election Assistance Commission has a testing and certification program for vendors by the Voluntary Voting System Guidelines (VVSG) which are the set of specifications and requirements to control systems security and functionality [6].

After the Russian interference in the 2016 election, especially three major e-voting vendors were put under the spotlight by politicians and the press. One of the correspondences conducted legal investigations revealed that except ES&S, both dominion voting systems and Hart intercivic shared detailed information about their ownership, shareholders, and technical parts of voting machines which come from China [7]. Company representatives naively stated that these foreign-origin parts are the nature of the global supply chain. Therefore ES&S claims that they carefully inspected the components of the e-voting machines then the company asked voluntarily to Idaho National Labs for penetration testing and they did not share the results unless it was stated that their e-voting system is not vulnerable to remote cyber-attack over the internet but could be "inoperative and unusable". ES&S company hasn`t shared the full report with the public but some of the congress members specifically dig into this issue for more clarification, especially after the FBI counterintelligence director Frank Figliuzzi's notice quoted "Chinese manufactured products the concern of machines shipped with undetected vulnerabilities or backdoors that could allow tampering." The ES&S on the other hand defend themselves for saying that all overseas manufacturing products successfully audited by the Election Assistance Commission (EAC) to ensure that components are trusted, tested and free of malware. After a while, The Senate generated $425 million in federal support to the States for enhancing the security of voting machines to safeguard democratic elections as well as eliminating cybersecurity risks and vulnerabilities.

Hale and Brown [8] clarify the state response to federal certification of electronic voting systems as the interface between the normative vision of a federal system and the realities of participation in a democratic society. Elections must depend upon public trust and confidence. Particularly e-voting must reflect accuracy, security, and consistent operation in the context of inclusive democracy. However, it is indicated that the operation of elections remains largely a state matter. They compare their research results with the other studies and what stands out is federal law binds state governments to prepare an election plan and this regulation is scrutinized under the election administration reform post-HAVA for requirements for paper audit tracks of E-voting machine transactions. These binding rules also apply to the private third parties who provide technological solutions for the electoral process. The US federal government allocated $3.9 billion to upgrade older election equipment with the Help America Vote Act and used nearly 75 percent of that grant for new voting systems to replace lever machines and punch card equipment during the election in 2002. These renewed systems were later identified as problematic in terms of cybersecurity.

3. Research

From registration to result, a safe and securely held electoral process is a major concern for every American citizen. Many organizations significantly care about this concern to safeguard democratic and fair elections. For example, The Heritage Foundation's election fraud database provides recent samples of election fraud cases from across the United States. The Heritage Foundation also presents an Election Integrity Scorecard to observe transparently various fraud cases in each state and the level of preparedness

of each government to protect voters and the election process. However, this mechanism does not reflect sufficient information about e-voting security or vulnerabilities of the e-voting machines in the specific state.

When it comes to e-voting fraud among many allegations, some of them take serious public attention and are investigated in detail by the Congress and judicial authorities in the United States. For example, Dominion Voting Machines' hacking allegation was significantly considered and assessed by the Cybersecurity and Infrastructure Security Agency (CISA) in 2021 right after the controversial 2020 election. According to the CISA advisory report, some versions of the Dominion Voting Systems Democracy Suite ImageCast X which is an in-person voting system have known vulnerabilities. Exploitation of these vulnerabilities can cause unauthorized access to individual ImageCast X devices and access to the Election Management System (EMS) and as a result, malicious actors might have the ability to modify files or infiltrate data from the ImageCast X devices. The CISA recommended risk mitigation strategies in ICSA-22-154A including technical, physical, and operational controls that prevent unauthorized access or hacking. Besides it is added in the CISA report there is no evidence to reflect that these vulnerabilities have been exploited in the Dominion voting system in any election [9].

Another fraud case was discovered on Diebolt e-Voting Systems. It was almost the same period on both started to use the Diebold election system and its fraud allegation. Many organizations from both public, private, and academic sides put the spotlight on discovering security flaws and the legitimacy of the Diebold system to uphold the power of democracy against any intentional or accidental attempt to manipulate election results. After the 2000 controversial elections in Florida. Diebolt was one of the e-voting machines that started to be utilized in many States in all over the United States. After the company`s proprietary information such as software and election files, hardware, and software specification, voting program patches were released in Wired magazine in 2003. Later this scandal incident, firstly in 2004 Information Security Institute at Johns Hopkins University revealed significant security flaws that might jeopardize the accuracy and legitimacy of the election results. Johns Hopkins University forensic investigation analysis led by Prof. Avi Rubin and it is resulted to say that *"this voting system is far below even the most minimal security standards applicable in other context*" [10]. This striking outcome inspired other initiatives for chasing the truth about Diebold's e-voting systems. According to the Johns Hopkins University report, "the technological controls in the Diebold software do not provide sufficient security to guarantee a trustworthy election. The software contains serious design flaws that have led directly to specific vulnerabilities that attackers could exploit to affect election outcomes. These vulnerabilities include vulnerability to malicious software, susceptibility to viruses, failure to protect ballot secrecy, and vulnerability to malicious insiders [11].

It presents many weaknesses of Ohio Ohio-based Diebold e-voting system by a group of researchers from the University of California (2007). According to their analysis, Diebold software does not have adequate security to safeguard a trustworthy election. Moreover, the study reveals that the software of the Diebold system has serious security architecture and cryptographic problems that could trigger the attacker's exploit to manipulate election results. Most of the Diebold system vulnerabilities were found and disclosed. For instance, one of the biggest flaws was the lack of cryptography in Diebold's smartcards, which is the main advantage of smartcards over magnetic cards. Due to the lack of cryptographic implementation, an attacker who knows the protocol spoken between voting terminals and legitimate smartcards could easily imitate one that aligns with the same protocol.

Another vulnerability that could be exploited by the attackers is an outsider would ability to create an administrator card. If this card was produced with a lack of cryptography, administrative functionalities could easily be apprehended by the hackers and the consequences would be so devastating such as terminating the elections. According to the research, there is no cryptographic techniques have been used to protect the ballot

definition file, an attacker can add, remove, and change information on the ballots. These attacks can also be executed physically by an insider. They also offered remediation for most of the Diabold vulnerabilities, first and foremost to eliminate the chain of custody and as cryptographers have suggested a protocol known as end-to-end cryptographic voting. It is mentioned that the end-to-end concept is to provide voters with confidence in the integrity of election results, regardless of the software used, and without the need to blindly trust election officials. And finally quoted "*All that must be accomplished without enabling the voters to prove to others how they voted. Generally, end-to-end systems provide the voter with some kind of assurance that his vote was recorded as intended (ballot casting assurance) in the form of encrypted proof.*"

4. Key Findings

According to the various reports from election officials from the national, state, and local levels, e-voting machines in use today are becoming rapidly out of date. They also warn that the current system would not be feasible to update hardware and software very shortly. Moreover, expensive, and ineffective federal certification process that promotes voluntary de facto standards for voting equipment manufacturers in the private sector initiatives. Therefore federal certification process must address current confidentiality, integrity, and fraud threats on e-voting machines otherwise states or private vendors cannot seem to fill the absence of effective government oversight. After the HAVA legislative efforts, States considered standards and testing and the use of Direct Read Electronic (DRE) voting systems (DRE also known as touchscreen machines). A new adaptation by the state led to national controversy about integrity, confidentiality, and results of touchscreen electronic voting machines, as well as overarching disputes about the reliability of computers generally and the susceptibility of electronic equipment to hacking and fraud. One of the recent examples is the Idaho National Laboratory penetration test for ES&S e-voting machine vendor. it was a legitimate and necessary attempt to show the company`s transparency and reliability but at the of the test, they refused to share the results with the public. At this point, there is no legal obligation to force private vendors to publicize the results which is the center of the trust problem.

According to the National Election Defense Coalition, there are 35 voting systems exist and certified by the US Election Assistance Commission. However, there are three largest voting machine manufacturing companies. These are dominating the vast majority of the US electoral process and the names of the companies are Election Systems& Software (ES&S), Dominion Voting Systems, and Hart InterCivic. Even though these voting machines have to follow certain standards and features, none of them have any responsibility to comply with cybersecurity requirements. According to the NIST cybersecurity framework, voting systems should not have wireless network connections. However, all voting machines have wireless modem connections and the systems conduct their operations online which might cause or result in data breach, infiltration, or denial of service attacks by hackers. But these are just suggestions for private companies, there are no binding rules or regulations to force them to comply with certain cybersecurity standards. Consequently, inadequate government inspection of those e-voting vendors causes suspicion and creates an untrustful election environment in public.

5. Recommendations

Many suggestions can be addressed to enhance the cybersecurity e-voting system. These suggestions should be categorized to align with different compartments of the electoral process. for example, some security measures that affect an adversary's ability to breach the system. If the system is designed, configured, and updated properly, in addition to that the system should be operated and managed accordingly. The risk of being compromised by e-voting machines would be reduced significantly. As mentioned in Kho et al article and many other studies urge that the internet is unsuitable for transmitting ballots, and currently, there is no

realistic mechanism to fully secure the casting of votes and tabulation of election results from cyberattacks. In addition, there are no technical mechanisms to guarantee that a computer system can generate accurate results, and each layer of the computer system is not modified. Furthermore, e-voting schemes that deploy emails are more vulnerable than other forms of e- voting. Moreover, not all vendors follow the best practices in developing, maintaining, and operating e-voting systems. However, it is possible to achieve strong defenses against cyber threats with the necessary to deploy state-of-the-art cryptographic technologies and practices to mitigate the risks as well as enhance the public trust in the e-voting system in the US. For example, one of the most critical parts of the e-voting system is the "Voters Registration Data Base" (VRDB). There are significant cyber-threats in this section if it is not protected properly that could lead to a major data breach and cripple the e-voting system. Incident response procedures should be implemented to prevent account compromise or third- party system compromise to maintain the security of the election [12].

Among other cryptographic methods, this study focuses on blockchain-based e-voting systems to suggest and give an example for facilitating strong defense against any type of cyber threat on e-voting systems.

Blockchain-based E-voting System and Practical Implementation

Despite the inadequate binding rules for implementing the most secure cryptographic methods on e-voting, there are still solid legal and advisory frameworks that acquire and deploy best practices to protect elections all across the United States. For instance, the National Election Defense Coalition, the HAVA, NIST, and CISA have security assessments and regulatory structures. However, there are still independent initiatives of each state to follow these structures to be on the secure or less secure side in terms of conducting a reliable e-voting process. Each state's practices would directly affect the election`s accountability as well as public trust in democracy, therefore it is indispensable to deploy the most relevant, transparent, and controllable cryptographic method to safeguard secure elections

Before proposing the blockchain-based crypto-voting method, it would be better to clarify what should be expected from secure e-voting as a person who wants to vote freely and fairly even though the existence of some physical or any type of negative circumstances such as different geographic location, election hygiene, disability or elderlies. First and foremost, the most convenient e-voting system should allow voters can vote from wherever there is an internet connection [13]. However, this connection must be adopted to the e-voting system securely with the convenient method by which blockchain technology can be utilized to overcome security problems with its decentralized nodes for e-voting. It also enables end-to-end verification and non-repudiation advantages for audit track to check integrity and reliability. It is used to hold both boardroom and public voting. A blockchain can be defined as a growing list chain of blocks that connect one another with cryptographic ties. Each block contains a hash, timestamp, and transaction data from the previous block. We all become familiar with blockchain technology with famous cryptocurrencies Bitcoin and Ethereum. Especially Bitcoin was the initial cryptocurrency solution that lays down a blockchain data structure. Today it is called blockchain technology which combines the blockchain data structure, distributed consensus algorithm, public key cryptography, and smart contracts. For e-voting, it is necessary to determine how it is possible to implement a crypto e-voting system using two linked blockchains [14]. The first links voters and voting procedures, and the second link counts votes and provides voting results.

The blockchain-based system emphasizes the importance of anonymization of the network consensus nodes. Smart contracts will be responsible for managing voting procedures and results" E-voting is a new phase of blockchain technology; in this field, many researchers come up with solutions to leverage benefits of this technology such as transparency, secrecy, and nonrepudiation that are essential for voting applications. Moreo John Podesta's e-mail compromised who was chairman of the Clinton election campaign John Podesta's e-mail compromised who was chairman of the Clinton election campaign over, the idea of using blockchain technology to create a tamper-resistant electronic/online voting network is gaining more privacy

and anonymity. The blockchain e-voting system is decentralized and completely open thereby ensuring that voters are protected which means anybody can count the vote by utilizing a blockchain-based system however nobody knows who voted to whom. Adapting blockchain-based e-voting methods may create users to unpredictable security risks and flaws. Blockchain technology requires a more sophisticated software architecture as well as managerial expertise. As indicated the major concerns should be addressed in more depth during actual voting procedures, based on experience.

In the final analysis, blockchain-based e-voting systems should be implemented in limited pilot areas before being expanded. Many security flaws still exist in the internet and various vendor-owned polling machines. Electronic voting over a secure and dependable internet will need comprehensive security improvements. Despite its appearance as an ideal solution, the blockchain system may not be able to address the whole e-voting system problems but it is obvious that blockchain is a revolutionary technology that reflects a complete shift towards a decentralized network, delivering accuracy and cybersecurity for e-voting, beyond that blockchain-based e-voting system would provide unavoidable benefits for gaining people`s trust and confidence on fair elections to uphold substantial values of democracy.

6. Conclusion

This study initially used the literature review method to obtain a wide range of information about voting systems in general. Then it is focused on current and past implementations of e-voting systems in the United States. To understand overall concerns, legal background, flaws, fraud cases, security risks, and the current controversial environment regarding the e-voting system, it is applied to learn from peer-reviewed articles, government reports, and some national media investigation reports. Throughout this intense reading and learning process, some of the research results are noted and reorganized along with the purpose of this study. It is reflected in some statistical analysis and shared visual images to add interactivity to this study to enhance learning capacity.

To sum up; this study proposes that electronic voting is a benefit to society if it is utilized correctly and made so that it will not be misused or not being hacked. For this reason, Congress enacted the Help America Vote Act (HAVA) of 2002 which established the Election Assistance Commission (EAC) to support both state and federal administrative entities for elections. The HAVA also facilitated a program to provide funds to states to replace older punch cards and mechanical lever voting equipment. If this study and other research about the improvement of the e-voting system would be taken into consideration by the election authorities, that would provide a quite sufficient contribution to the field in terms of increasing the quality of democracy. As a result, it is necessary with advanced cryptographic methods such as blockchain-based systems to provide additional security and integrity for voters' privacy as well as reliable election results. Hence on the way to upcoming the Presidential Election, security measures for the e-voting system in the United States have been enhanced to ensure the confidentiality, integrity, and availability of the e-voting system in 2024 and afterward.

Conflict of Interest

Author declares that there are no conflicts of interest.

References

[1] S. Debnath, M. Kapoor, and S. Ravi, "The impact of electronic voting machines on electoral fraud, democracy, and development," *Democracy, and Development*, 2017.

[2] A. R. Jorba, J. A. O. Ruiz, and P. Brown, "Advanced security to enable trustworthy electronic voting," in *Proc. the 3rd European Conference on e-Government*, 2023, pp. 377–384.

[3] J. Schwartz and The NewYork Times. (July 2003). Computer voting is open to easy fraud. [Online]. Available: https://www.nytimes.com/2003/07/24/us/computer-voting-is-open-to-easy-fraud-

experts-say.html?smid=url-share
[4] Y. X. Kho, S. H. Heng, and J. J. Chin, "A review of cryptographic electronic voting," *Symmetry*, vol. 14, no. 5, 858, 2022.
[5] MIT Election Data Science Lab. (April 2023). Voting technology. [Online]. Available: https://electionlab.mit.edu/research/voting-technology
[6] The United States Election Assistance Commission. (January 2024). Certified voting systems. [Online]. Available: https://www.eac.gov/voting-equipment/certified-voting-systems
[7] B. Popken, C. Mc Fadden, and K. Monahan, (December 2019). Chinese parts, hidden ownership, growing scrutiny: Inside America's biggest maker of voting machines. [Online]. Available: https://www.nbcnews.com/news/all/chinese-parts-hidden-ownership-growing-scrutiny-inside-america-s-biggest-n1104516
[8] K. Hale and M. Brown, "Adopting, adapting, and opting out: State response to federal voting system guidelines," *Publius: The Journal of Federalism*, vol. 43, no. 3, pp. 428–451, 2013.
[9] Cybersecurity and Infrastructure Security Agency. (2022, March 6). Vulnerabilities affecting dominion voting systems ImageCast X. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-22-154-01
[10] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," *IEEE Symposium on Security and Privacy*, pp. 27–40, 2004.
[11] J. A. Calandrino, A. J. Feldman, J. A. Halderman, D. Wagner, H. Yu, and W. P. Zeller, *Source Code Review of the Diebold Voting System*, University of California, Berkeley under contract to the California Secretary of State, vol. 40, 2007.
[12] M. Berger, *The State and Local Election Cybersecurity Playbook*, Harvard Kennedy School, Belfer Center for Science and International Affairs, 2018.
[13] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," *Sensors*, vol. 21, no. 17, 5874, 2021.
[14] F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, "Crypto-voting, a blockchain-based e-voting system," *KMIS* pp. 221–225, 2018.