IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 2, Ser. 3 (Mar. – Apr. 2024), PP 11-16
www.iosrjournals.org

The Effect Of Data Information Security In Digital Voting And Electoral Processes

Tunbosun Oyewale Oladoyinbo
University Of Maryland Global Campus, 3501 University Blvd E Adelphi, Md20783

Abstract
Technology integration has called for increased debates regarding data information security, especially around digital voting and the overall electronic electoral process. Most voters are concerned about election security attributed to reports about possible voting results interference by foreign powers, increased unauthorized voting, and voter disenfranchisement. This article examines the effect of data information security in digital voting and electoral processes. The paper aims to explore the main information security problems associated with electronic voting systems. The paper will explore integrating digital technology into the electoral process, elections security requirements, security threats to the DRE voting systems, and the security threats associated with internet voting systems. The paper will employ a qualitative research design for data collection and analysis. An extensive literature review showcases the current discussion regarding information security and its impact on the digital voting process.

Keywords: *Data information security, Digital voting, Electoral process, Election security Security threats, Digital technology integration*

Date Of Submission: 01-04-2024 Date Of Acceptance: 10-04-2024

I. Introduction

Although not new, the increased adoption and utilization of computers and other digital devices in voting has raised discussions regarding data security during the electoral voting process. Using computers and associated technology has played a vital role in transforming the voting processes. Computers provide decisive roles in democratic organizations and help individuals cast ballots through computerized systems (Alvi et al., 2020). Several forms of elections exist, including the punched cards introduced in the 1980s and using perforated paper to store digital information. The punched card system was gradually overtaken by the optical scan system, which used optical scanners to read and tally marked votes on paper. Newer digital and internet-based voting systems have emerged, transforming the electoral and voting system across the globe. One of the newer voting systems is the direct-recording electronic voting machine (DRE), introduced in the past decade. DRE became the first computerized system to enable voters to vote through touch-screen digital devices (Park et al., 2022). The Internet voting system is the newest system that has received increased adoption by numerous nations across the globe. Internet voting systems are considered more effective, reliable, and user-friendly, especially because they allow voters to vote at the convenience of their location, provided they have access to the Internet through a computer system. Rapid technological innovations have made using computers in voting more convenient by allowing numerous options for voters to cast their votes. Computers have enabled the Internet, telephone, and voting through private computer systems.

These computerized voting approaches are associated with several benefits, such as increased precision in the overall voting process. Other key benefits associated with computerized and Internet voting include rapid implementation of the internet voting systems and increased accessibility for voting, especially to voters with disabilities (Jafar et al., 2021). Despite these advantages, internet voting is associated with increased data information security concerns. The concept has created numerous controversies in the voting realm, especially across democratic organizations and societies. This is attributed to the numerous cybersecurity challenges associated with digital technology and the use of the Internet in transferring and sharing information. For instance, internet voting has been associated with cases of electoral fraud and compromised voting processes, especially through the influence of foreign governments (Yang et al., 2020). The new ontological existence of the digital realm and new approaches to data flows and communication characterize the emergence of cyber voting. The development of the digital realm has caused increased transformation, including enhancing rapid and more paced communications across the globe and the commodification of voting and electoral information. These factors have also increased the number of actors participating in electoral processes and elections. Different states and nations have adopted technological innovations in electoral and election processes to enhance democratic goals (Park et

al., 2022). For instance, through technological innovations, such as digital space and computers, governments have improved their nation's democratic ideals, such as increasing political equality and enhancing the concept of popular control of government.

The main goal of the Internet and electronic voting should be to provide increased reliability and accuracy in recording and counting. Computerized and Internet voting processes aim to improve fairness and transparency in the electoral process (Jafar et al., 2021). Such systems should incorporate specific security requirements to ensure the integrity of elections and the electoral processes. For instance, the systems should have mechanisms to ensure voters can only vote once in each election exercise. The electronic or Internet voting systems should support audit logs for voter records, allowing the detection of errors and effective modifications (Yang et al., 2020). Election results should be effectively recorded and presented with increased precision at all times, including protection from voting fraud and possible data exchange.

II. Literature Review

Introduction

This literature review section will explore current literature regarding data information security and its influence on digital voting practices and the overall electoral processes. The review of literature takes a thematic approach, and the main themes explored include the integration of technology in electoral processes, the changing patterns in voting attributed to the emergence of the cyber voting era, election security requirements, security threats associated with the DRE voting systems, and the security threats associated with internet voting systems.

The Integration of Technology in Electoral Processes

Technology has been integrated in numerous and diverse ways in the electoral processes for decades. Traditionally, radios and television sets were utilized to promote campaigns and disseminate election advertisements (Alvi et al., 2020). Technology has faced constant and rapid advancement over time. Newer and more innovative technological approaches have emerged, transforming how elections are conducted worldwide. For instance, most nations have incorporated digital devices and computerized systems, ensuring election offices have computer-based technologies. Increased revolution in technology has caused an increased adoption and integration of technology, especially in the effective management of electoral processes (Park et al., 2022). The modern days have showcased an explosion in technology integration, especially by introducing electronic and Internet voting approaches. Almost all nations have incorporated technological innovations in electoral and election processes.

The election process is a comprehensive aspect that involves extensive preparations, creation, and implementation of electoral laws and regulations, voter registration and verification, and selecting or appointing an electoral body to take responsibility for the electoral processes. All these aspects and facets in the election process integrate technology, from simple computerized databases to organizing a single polling station to complex and more comprehensive systems, such as voter registration (Jafar et al., 2021). Technological advancement has shown increased improvements in electoral activities, especially in voter registration and election management organizations. For instance, recent technological innovations such as biometrics have been integrated into the electoral processes, in which biometric data of voters is collected during voter registration and can be used for important processes like voter identification and verification (Shankar et al., 2021). Additionally, most governments have adopted and implemented online voter registration systems, allowing qualified voters to participate in the registration process remotely and at the convenience of their locations. Complex technological and computerized systems allow the automated addition of names to electoral databases from integrated government data sources, such as social security and insurance.

The campaigns have also illustrated a constant adoption of technological advancement, especially with the advent of social media and the Internet. The Internet and social media have transformed how election candidates perform campaign advertisements and promotions. These aspects have created numerous benefits and challenges in the overall electoral activities. For instance, voter's online activities and preferences can be monitored and captured to develop tailored and direct targeting by political parties, election candidates, and potential interest groups. Taş and Tanrıöver (2020) explain that many political organizations utilize social media data through hiring firms to structure targeted advertisements for their political journeys. Some of these practices are unethical, especially those that utilize voters' social media data or information from other sources for campaign purposes. It is, therefore, essential for election management organizations, the judicial branch, and electoral policymakers to develop effective frameworks to guide the appropriate use of such data (Yang et al., 2020). This includes the potential privacy issues associated with collecting and utilizing such data. The election day activities and the aftermath of the election results complete the election cycle. Technology is utilized in the actual voting process, including the casting of votes by the voters. For instance, electronic voting and internet voting systems are common and popular technological aspects integrated to aid in casting ballots on election day. The most popular Internet or electronic technology used for casting votes is the DRE, a computerized approach that helps

to cast and count votes (Khan et al., 2020). Other methods include optical scanning and online voting. The increased adoption and utilization of technology in electoral activities has created opportunities and several information security challenges in the election realm.

Election Data Information Security Requirement

Most nations, like the United States, utilize the evidence-based election approach in all their electoral processes. The principle of evidence-based elections emphasizes the importance of the election management bodies determining an election's true winners and providing convincing evidence to show that the winners won. Based on this requirement, the election system utilized to conduct the elections must be auditable, and the election conducted using the system must also be audited (Rathee et al., 2021). Secure elections must meet minimal security requirements, especially for nations that utilize the evidence-based election principle. One of the key security requirements for secure elections is enhancing ballot secrecy. Ballot secrecy is essential in maintaining and mitigating voter protection against possible corruption and coercion. The US Supreme Court clarifies that ballot secrecy prevents voter intimidation and election fraud (Yang et al., 2020). With effective ballot secrecy, the election managing body can foster robust security against voter selling practices by ensuring the voters cannot be paid or threatened to pressure them into voting the way a particular candidate, political party, or third-party interest group desires. Before the introduction of secret ballots, voter bribery and corruption were the key factors hindering election integrity in most nations, including the United States.

Another key election security requirement is ensuring software independence. Software independence is critical for ensuring that election systems' casting, collecting, and tallying components can be audited. Additionally, software independence lessens the possibility of widespread mistakes or assaults and ensures that any mistakes are apparent (Rathee et al., 2021). System failure due to scalability is more common in software-based systems than in non-software-based ones. In contrast to physically accessing and managing each paper ballot individually, a remote programmer may modify numerous electronic ballots quickly by simply modifying a single line of code. For a system to be considered software-independent, all software-based components must be able to have their work verified using methods that do not rely on software (Yang et al., 2020). For every particular execution, a system that records votes cast, collected, and tallied must generate an evidence trail with a corresponding verification mechanism to ensure that the system recorded votes correctly, collected them as intended, and tallied them as gathered. If there is no software independence, an unconfirmable mistake in the election results could be caused by an undetected bug in some code. Secure elections must enhance voter-verifiable ballots. Voters need to be able to check their ballots to make sure they reflect their selections before casting a ballot. Paper ballots are advantageous over electronic voting systems because they can be verified and recorded correctly (Alvi et al., 2020). Voters can be reasonably assured that the human-readable mark on a hand-marked paper ballot is for the candidate genuinely meant by the voter, and the marks on the ballot inevitably reflect what the voter did. By reviewing their paper ballot, voters can easily verify that their choices have been marked and identify any mistakes they may have made.

Another unanswered topic remains whether software is considered independent on its own. Since anybody may do the verification technique, the second question becomes irrelevant because some mistakes may be easily detectable by the public. Some verification techniques, however, may not be publicly available. For instance, an individual voter may be the only one capable of seeing certain mistakes in their vote (Rathee et al., 2021). Whenever a mistake is found, a voting method that can be challenged offers publicly verifiable proof that the election result cannot be trusted. Elections should be auditable and auditable only. Regarding systems for tallying votes, audits ensure the data is reliable and matches the declared results. Elections based on evidence require both auditability and auditing. Among the audits that should be conducted are those that aim to limit risks and ensure compliance (Yang et al., 2020). Software error detection must not be flawless; it must occur with a high enough probability. The public has a right to know about any problems with the election process, so the system must be built to prevent errors and detect them quickly when they happen (Alvi et al., 2020). These requirements interact in a very complicated way; designing systems that meet even the most basic requirements simultaneously is incredibly difficult, and no technology, including blockchain, is even close to making it possible for Internet or mobile voting systems to meet all these requirements simultaneously.

Security Threats Associated with the DRE Voting Systems

Diebold Corporation of the USA is the manufacturer of the DRE system. Using DRE technologies is not without its security drawbacks. One of its most significant flaws is the lack of transparency around the Diebold software's source code, a collection of instructions written in computer programming languages. The Diebold software is protected by copyright and cannot be modified or examined by anyone other than the owner. This makes it closed-source software. Consequently, a major issue with the Diebold software leads to elections (Rathee et al., 2021). The program's makers can make various alterations to the software, which could impact the voting process. This raises worries about the reliability of the voting results. Owners of DRE systems are opposed to

making their source code publicly available for error detection or vote tallying purposes due to their desire to maintain copyright (Yang et al., 2020). Diebold machine owners may claim their software is safe and dependable, but many still worry that the company's coders might favor one candidate over another by adding extra votes to the tally. Beyond what was already mentioned, we also saw that the smartcards did not do any cryptographic operations when we looked at the Diebold code. Just this fact alone should raise red flags. The capacity of smartcards to execute cryptographic operations internally with physically secured keys is one of the main benefits over traditional magnetic-stripe cards. Due to the absence of cryptography, there is no foolproof method of authenticating the smartcard to the voting terminal (Alvi et al., 2020). A real possibility is that an attacker could use a homemade smartcard in a voting machine. The ease with which an attacker may create such a homebrew smartcard is a reasonable concern. Furthermore, a malicious actor aware of the protocol used by voting terminals and official smartcards might create a homebrew card that communicates similarly.

Diebold DRE devices are equipped with software called a Global Election Management System. The GEMS program employs Microsoft Access, a database management system, to keep track of the votes. The GEMS Access database is vulnerable to hacking due to its inadequate security measures (Yang et al., 2020). Therefore, a big issue with using the Diebold DRE machines is the lack of security in the GEMS database. Instead of using the GEMS program, regular or expert users can access the database and manipulate the vote results through Microsoft Access. Mystery Case Using the Microsoft Access database to keep track of the votes cast by the electro-voters would compromise the GEMS program's security and make the voting process less fair (Alvi et al., 2020). The GEMS program's database appears to have a security flaw, leaving it open to several attacks. Voters in conventional elections can rest assured that their ballots were counted and that the results are secure because they use paper ballots. One important step in ensuring that the voting results are accurate and unaltered is the implementation of Voter-Verified Audit Trails. First-Phase Taping This is not possible with electronic voting devices. Since it is hard to establish that votes have been counted without verification, this is a big flaw in DRE systems. The credibility of the voting process could take a hit if this situation were to cause a security breach.

Regarding the security of the Internet voting system, two major concerns exist. Denial of Service attacks can lead to electoral fraud in democratic societies and malware, which is harmful code. Most dangerous codes are spread through Trojan horses, viruses, and worms; malware is software designed to destroy computer systems (Rathee et al., 2021). Certain PCs out there do not have enough protection against viruses. Internet voting systems are vulnerable to two types of malicious programming. First, developers working on the system might compromise it by inserting malicious software into the election web server to erase the vote data. The second concern is malicious software being distributed to voters' computers and then impacting the electoral process. Malicious software like this could influence the voting process covertly since it is hard to detect (Yang et al., 2020). To achieve this, it either modifies the electors' inputs, removes their votes from the tally, or prevents them from casting a ballot altogether. Concerns regarding the integrity of the vote when using the Internet arise from the lack of adequate security measures in the election web server and the computers of electors involved in the process. Internet voting systems also risk Man-in-the-Middle attacks when an attacker tries to block the client and server from communicating. Spoofing attacks are one way an adversary might become a Man-in-the-Middle; these attacks trick voters into thinking they are interacting with the election web server when, in fact, they are not (Alvi et al., 2020). An attacker could, for example, trick voters into visiting a phony election website when they try to access the real one. This attack aims to manipulate electors' votes in favor of a certain party by tricking them into thinking they are on a legitimate voting website. In addition to tampering with voting records, a seven spoofing assault may compromise individuals' privacy by stealing sensitive information such as their names, dates of birth, and signatures.

Research Questions

i. How does the public's perception of data security in digital voting systems affect voter turnout and participation in elections?
ii. What factors influence the electorate's confidence in the security of digital voting systems, and how can these factors be improved?
iii. How do demographic variables such as age, education level, and technological proficiency affect digital voting attitudes and concerns about data security?

III. Methodology

To address the research questions, a survey was crafted to gauge the willingness of participants to vote, scaled from 0 to 10 (not willing to completely willing to vote). The SurveyMonkey platform was used to deploy the questionnaire for the study.

IV. Results

The level of digital security of the voting system barely accounts for 1.7% of the variance in the inclination to vote, as indicated by the R-squared value of 0.0171. As a result, we can infer that the correlation between the two is quite weak and that digital security levels do not account for a significant portion of the variation in voting intentions. When the model fails to enhance the fit relative to a model without predictors, a somewhat negative Adjusted R-squared value of -0.0146 might be seen. The F-statistic provides additional evidence that the model does not hold statistical significance, which stands at 0.5398, along with a high p-value of 0.4680. Therefore, it is likely that any link between digital security and voting intentions is just coincidental rather than indicative of a real relationship. A statistically significant intercept of 4.3237 was found when we examined the coefficients (p-value = 0.0001). Based on this model, the average readiness to vote would be 4.3237 units when digital security is zero. There is no statistical significance ($p > 0.05$) for the voting system's digital security level coefficient, 0.2442, with a p-value of 0.4680. Further evidence that digital security levels do not significantly affect willingness to vote is provided by confidence intervals for this coefficient, which range from -0.4337 to 0.9222, including zero.

SUMMARY OUTPUT

Regression Statistics		
Multiple R	0.1308	
R Square	0.0171	Only 1.7% of variation in willingness to vote is explained by variation in level of digital security of the voting system
Adjusted R Square	-0.0146	
Standard Error	3.2323	
Observations	33	

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	5.6395	5.6395	0.5398	0.4680
Residual	31	323.8756	10.4476		
Total	32	329.5152			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	4.3237	0.9420	4.5899	0.0001	2.4025	6.2450	2.4025	6.2450
Security of Digital voting syste	0.2442	0.3324	0.7347	0.4680	-0.4337	0.9222	-0.4337	0.9222

V. Discussion

The statistical evidence from this investigation indicates that the correlation between data security and voter confidence is not as substantial as one might assume despite the intuitive link. The current state of data security only partially explains the variation in voters' propensity to cast ballots electronically, according to an R-squared value of 0.0171. It appears that voters' political consciousness, faith in government, and the perceived simplicity and accessibility of voting online are other, perhaps more important, elements that impact their propensity to participate in digital electoral processes. The lack of a statistically significant relationship between digital information security and voter participation is supported by the non-significance of the model, as shown by the F-statistic ($p = 0.4680$). This finding goes against the grain of the current conversation, which frequently highlights security concerns as the main reason voters are wary of using digital voting. Among the many possible explanations for this disparity is a misalignment between the study's quantitative measures of information security and the way voters feel about the topic. More studies are needed to tease out the intricacies of this association since the outcome might have been influenced by the individuals' demographics or the sociopolitical climate when the data was collected. For politicians and technologists attempting to establish electronic voting systems, it is critical to consider the larger ramifications of these results. While data security might not be the main issue impacting voter willingness, it is still essential to ensuring elections are honest and trustworthy. It is possible to close the knowledge gap and change public opinion by informing voters about the security precautions and being open and honest about the technologies employed. In addition, the study may lead to a rethinking of how we measure voters' faith in electronic voting systems, which could lead to more holistic and multi-faceted methods that better account for the nuances of voter behavior. For this reason, researchers should incorporate a broader range of variables into their future assessments of digital security perception to fully grasp the complex nature of online voting.

The problem of data information security about digital voting and electoral processes is becoming more important as technology is becoming an integral part of democratic activities. If digital voting methods are to remain reliable, data information security must be a top priority. Voters' trust in modern voting systems depends on safe and accurate voting tallying guarantees in the digital era. Mistrust in the electoral process might result from data breaches or worries about the security of voting technologies, which can affect both the digital and voting processes. The public's faith in democratic institutions and their willingness to cast ballots are both impacted by this. Protecting the confidentiality of voters' data and ensuring the voting process resists manipulation requires strong encryption methods and security measures. The public's faith in free and fair elections could be

eroded, and the democratic process could be undermined if there is no guarantee of rigorous security standards for digital voting equipment. Apathy or mistrust towards technological advancements in voting can develop due to the psychological effects of feeling unsafe. Therefore, implementing safe digital voting is crucial, as is the electorate's impression of security. In addition, issues of digital literacy, accessibility, and equality collide with data information security in the context of digital voting. We will need all-encompassing measures to resolve these interconnected issues if we want everyone to have faith in and access to digital voting. We must balance the benefits of technology, such as efficiency and ease, and the necessity to reach out to and educate a diverse audience as voting becomes more digitalized. The link between data security and digital voting is fundamental to the ongoing evolution of democratic processes in the 21st century, and the interplay of both elements dictates it. It demands that engineers, lawmakers, and the general public maintain an open line of communication in order to create creative and inclusive voting methods.

References

[1] Alvi, S. T., Uddin, M. N., & Islam, L. (2020, August). Digital Voting: A Blockchain-Based E-Voting System Using Biohash And Smart Contract. In 2020 Third International Conference On Smart Systems And Inventive Technology (Icssit) (Pp. 228-233). Ieee. Https://Ieeexplore.Ieee.Org/Abstract/Document/9214250/

[2] Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain For Electronic Voting System—Review And Open Research Challenges. Sensors, 21(17), 5874. Https://Www.Mdpi.Com/1424-8220/21/17/5874

[3] Khan, K. M., Arshad, J., & Khan, M. M. (2020). Investigating Performance Constraints For Blockchain Based Secure E-Voting System. Future Generation Computer Systems, 105, 13-26. Https://Www.Sciencedirect.Com/Science/Article/Pii/S0167739x19310805

[4] Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going From Bad To Worse: From Internet Voting To Blockchain Voting. Journal Of Cybersecurity, 7(1), Tyaa025. Https://Academic.Oup.Com/Cybersecurity/Article-Pdf/Doi/10.1093/Cybsec/Tyaa025/42533672/Tyaa025.Pdf

[5] Rathee, G., Iqbal, R., Waqar, O., & Bashir, A. K. (2021). On The Design And Implementation Of A Blockchain Enabled E-Voting Application Within Iot-Oriented Smart Cities. Ieee Access, 9, 34165-34176. Https://Ieeexplore.Ieee.Org/Abstract/Document/9360732/

[6] Shankar, A., Pandiaraja, P., Sumathi, K., Stephan, T., & Sharma, P. (2021). Privacy Preserving E-Voting Cloud System Based On Id Based Encryption. Peer-To-Peer Networking And Applications, 14, 2399-2409. Https://Link.Springer.Com/Article/10.1007/S12083-020-00977-4

[7] Taş, R., & Tanrıöver, Ö. Ö. (2020). A Systematic Review Of Challenges And Opportunities Of Blockchain For E-Voting. Symmetry, 12(8), 1328. Https://Www.Mdpi.Com/2073-8994/12/8/1328

[8] Yang, X., Yi, X., Nepal, S., Kelarev, A., & Han, F. (2020). Blockchain Voting: Publicly Verifiable Online Voting Protocol Without Trusted Tallying Authorities. Future Generation Computer Systems, 112, 859-874. Https://Www.Sciencedirect.Com/Science/Article/Pii/S0167739x17327656