European Journal of Electrical Engineering and Computer Science
Vol 9 | Issue 2 | March 2025
ISSN 2736-5751

RESEARCH ARTICLE

Enhancing Vulnerability Assessments for Electronic Voting Systems through an Augmented CVSS 3.1 Model

Demetrice Rogers and Yanzhen Qu*

ABSTRACT

This paper explores the application of the Common Vulnerability Scoring System (CVSS) to electronic voting systems, highlighting how unique considerations in these environments can be more accurately captured with an enhanced model. By incorporating criteria from the Voluntary Voting System Guidelines (VVSG), this research addresses the limitations of traditional IT-based evaluations in assessing vulnerabilities within electronic voting systems. The enhanced model was validated using a dataset of real-world vulnerabilities, showing significant improvements in accuracy and prioritization through statistical analyses. The findings offer a repeatable and extensible method for cybersecurity practitioners and election officials to assess operational risks and implement mitigation strategies to protect electrical integrity.

Keywords: Common Vulnerability Scoring System (CVSS), election integrity, Electronic voting, vulnerability assessment.

Submitted: December 25, 2024

Published: March 19, 2025

10.24018/ejece.2025.9.2.683

Colorado Technical University, USA.

*Corresponding Author:
e-mail: yqu@coloradotech.edu

1. Introduction

Switching to electronic voting systems aims to make elections more efficient and accessible, but it also brings up serious concerns about security and reliability [1]. These systems operate in environments where public trust, voter anonymity, and election integrity are crucial, requiring a specialized approach to vulnerability assessment. While tools like the Common Vulnerability Scoring System (CVSS) v3.1 are widely used to evaluate cybersecurity risks, they fall short when it comes to the unique challenges of electronic voting.

Critics of CVSS v3.1 point out its limitations, especially its inability to adapt to specialized contexts like operational technology and voting systems [2]. This is a significant issue for electronic voting, where vulnerabilities can undermine not just the system's functionality but also public trust in the democratic process. Traditional CVSS metrics don't account for the regulatory and operational nuances introduced by frameworks like the Voluntary Voting System Guidelines (VVSG) [2].

This study aims to bridge these gaps by proposing an enhanced CVSS v3.1 model specifically designed for electronic voting systems. By incorporating criteria from the VVSG, the model seeks to improve the accuracy of vulnerability assessments, offering a more reliable basis for resource allocation and risk mitigation. This work adds to the growing body of research advocating for domain-specific adaptations of cybersecurity tools, with potential applications beyond elections to other critical infrastructure sectors.

2. Related Works

2.1. Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) has been a cornerstone for assessing and quantifying risk since it was introduced in 2005 [3]. Over the years, CVSS has evolved through several iterations, incorporating feedback from both industry and the public to refine its metrics and adapt to the ever-changing landscape of cybersecurity. These updates have included adjustments to better address specific risks, more precise scoring mechanisms, and even adaptations tailored to particular industries. CVSS's scoring methodology has been widely adopted as a global standard for assessing and prioritizing vulnerabilities, forming the basis for frameworks such as the National Institute of Standards and Technology's (NIST) Risk Management Framework and its integration into vulnerability assessment tools like Tenable and Qualys [4]

CVSS's flexibility extends to non-traditional domains like operational technology (OT). In the Industrial Internet of Things (IIoT), CVSS metrics effectively quantify unique risks introduced by alternative communication protocols and specialized software. Research from the Software Engineering Institute at Carnegie Mellon University explores the use of CVSS in IoT environments, highlighting the challenges and considerations in assessing vulnerabilities within these systems [5]. Additionally, CVSS variables have been adapted to assess risks in critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) has implemented the Stakeholder-Specific Vulnerability Categorization (SSVC), which uses CVSS metrics to prioritize vulnerabilities based on stakeholder perspectives [6]. This approach enhances the protection of critical infrastructure sectors, similar to this research on electronic voting systems.

Despite its success in various specialized domains, there is a noticeable gap in applying CVSS specifically to electronic voting systems. These systems present distinct challenges, such as threats to voter anonymity, the need to comply with election-specific guidelines like the VVSG, and the critical importance of maintaining public trust [7]. To address this gap, CVSS must be adapted to account for these unique factors, ensuring that vulnerabilities in electronic voting systems are accurately assessed and prioritized for mitigation.

2.2. *Factor Analysis of Information Risk (FAIR)*

An alternative to CVSS is the Factor Analysis of Information Risk (FAIR) framework. Where CVSS scores risk using technical parameters, FAIR's generative model takes a risk-focused approach that quantifies it in financial terms. It allows businesses to calculate the effects and probability associated with vulnerabilities, making informed decisions regarding the expenditure of resources [8]. CVSS assigns fixed values to variables, but FAIR considers context, for example, business goals, asset importance, threat environments, which make it easily applicable to various industries such as finance, healthcare, critical infrastructure, etc [9]. FAIR would necessitate detailed data contributions and expertise that might be resource-hungry. However, its use for electronic voting platforms may support CVSS by filling holes in strategic risk analysis, particularly for public trust and election integrity vulnerabilities.

3. Problem Statement, Hypothesis Statements, And Research Questions

3.1. *Problem Statement*

The issue this study addresses is that the Common Vulnerability Scoring System v3.1 does not effectively capture the critical impacts of vulnerabilities in electronic voting systems. This is due to its lack of specific considerations for the unique characteristics and operational environments of these systems. While the general CVSSv3.1 framework is widely used across various IT domains, it falls short when applied to electronic voting systems, which have distinct vulnerabilities and requirements. This gap poses a significant risk, as these systems are essential for national elections and must operate with the highest levels of security and integrity.

For instance, in 2022, a county commission in New Mexico refused to certify primary election results due to concerns over the reliability of voting machines [10]. This incident underscores the urgent need for a more tailored vulnerability assessment. Research indicates that a major concern among voters is the integrity and tamper-resistance of electronic voting systems [11]. Additionally, surveys show that about 80% of Americans are worried about the potential vulnerability of the nation's voting systems to cyber-attacks [12] highlighting a deep public distrust in these technologies.

3.2. *Hypothesis Statement*

- H_0: The integration of VVSG-specific criteria into the CVSSv3.1 model does not improve the accuracy of vulnerability assessments for electronic voting systems compared to the standard CVSSv3.1 model.
- H_1: The integration of VVSG-specific criteria into the CVSSv3.1 model improves the accuracy of vulnerability assessments for electronic voting systems compared to the standard CVSSv3.1 model.

3.3. *Research Question*

How does the integration of VVSG-specific criteria into the CVSSv3.1 model improve the accuracy of vulnerability assessments for electronic voting systems compared to the standard CVSSv3.1 model?

4. Methodology

4.1. *Method*

Design science research (DSR) is a fitting approach for this study because it focuses on creating and evaluating solutions to specific problems [13]. DSR is practical and results-oriented, which aligns well with the goal of developing an improved CVSSv3.1 model tailored to the unique needs of electronic voting systems. This approach addresses real-world security concerns that have significant implications.

The quantitative aspect of DSR allows for systematic testing and validation of the new model, ensuring it is both reliable and effective. Using quantitative methods provides the rigor needed to evaluate the model's performance through statistical analysis, supporting the objective of creating a robust security assessment tool.

The choice of quantitative design science research is well-supported by existing literature in information systems and cybersecurity. The design science approach is known for its ability to solve complex problems through innovative solutions [14]. This study's aim to create and validate an augmented CVSSv3.1 model fits within this tradition, enhancing the existing framework by incorporating specific criteria from the VVSG. Additionally, the quantitative approach ensures that the research is rigorous and grounded in empirical evidence, which enhances its credibility and relevance.

To test the augmented CVSSv3.1 model, we will apply it to a selected sample of documented vulnerabilities. Each vulnerability will be scored using both the standard CVSSv3.1 model and the augmented model. By comparing the results, we can evaluate how well the augmented model provides a more comprehensive assessment of vulnerabilities in electronic voting systems.

4.2. Population and Sample

The study focuses on 15 documented vulnerabilities in electronic voting systems, along with the existing CVSSv3.1 models and relevant security guidelines like the VVSG. These vulnerabilities are sourced from academic journals, industry reports, and databases such as the National Vulnerability Database (NVD). As of June 26, 2024, the NVD contains over 255,241 vulnerabilities, though not all are specific to electronic voting systems. By selecting 15 relevant vulnerabilities, the study strikes a balance between relevance and manageability, concentrating on those directly related to the operational and security needs of electronic voting systems. This approach follows established methodologies in vulnerability assessment studies, which often prioritize context-specific sampling to test the applicability of new frameworks [15].

The sample includes a representative set of vulnerabilities from various electronic voting systems, both current and historical. For instance, as of June 6, 2024, there are nine vulnerabilities associated with Dominion Voting Systems. These vulnerabilities are chosen based on their relevance and frequency in real-world scenarios. Additionally, the sample incorporates the current CVSSv3.1 metrics and scoring used to evaluate these vulnerabilities. Selecting 15 vulnerabilities provides enough data points for paired t-tests and descriptive statistical analysis, as these methods are robust even with small sample sizes when the data is representative and specific [16]. This targeted approach aligns with the pragmatic nature of design science research, balancing theoretical progress with actionable insights for real-world applications [14].

4.3. Definitions and Formula

- *Augmented CVSS Base Score:* The calculated score that incorporates traditional CVSS metrics alongside augmented metrics tailored for electronic voting systems, such as VVSG compliance, tamper resistance, data integrity, and system reliability.
- *VVSG Compliance (VC):* A measure reflecting the system's adherence to Voluntary Voting Systems Guidelines. Scores can be Non-Compliant (0.0), Partially Compliant (0.5) or Fully Compliant (1.0).
- *Tamper Resistance (TR):* An indicator of a system's ability to withstand unauthorized physical or digital tampering, with higher values denoting stronger resistance. Scores can be Low (0.3), Medium (0.6), or High (1).
- *Data Integrity (DI):* A metric assessing the impact of vulnerabilities on the integrity of stored and transmitted voting data. Scores can be Low (0.3), Medium (0.6), or High (1).
- *System Reliability (SR):* Evaluates the likelihood of a system-wide failure resulting from a vulnerability, with higher values indicating better reliability. Scores can be Low (0.3), Medium (0.6), or High (1).
- *Augmented CVSS 3.1 Formula:* This formula ensures that vulnerabilities with higher criticality, as determined by the VVSG-related metrics, are appropriately prioritized. By modifying the scoring weights and introducing election-specific metrics, the augmented model prioritizes vulnerabilities that directly impact critical voting system functions, such as vote recording, tallying, and data security. This adjustment ensures that vulnerabilities with significant implications for election integrity are highlighted for mitigation. A fully compliant system reduces risk, while non-compliance adds penalties to the augmented score.

$$\text{Augmented Score} = \min(\text{Traditional CVSS } 3.1 \text{ Score} + (1 - VC) + \left(\frac{TR + DI + SR}{3}\right) \times 1.5, 10).$$

5. Experiment And Results

5.1. Results

The augmented CVSSv3.1 model significantly improved the accuracy and prioritization of vulnerabilities in electronic voting systems. Statistical analysis, including paired t-tests, showed that the augmented model provided a more precise evaluation of risks compared to the standard CVSSv3.1 model:

1. *Statistical Validation:* The paired t-test revealed a statistically significant difference between the traditional CVSSv3.1 scores (mean: 6.55, SD: 2.03) and the augmented scores (mean: 7.91, SD: 1.68), with a p-value of less than 0.001. This indicates that the augmented model is better at identifying critical vulnerabilities.
2. *Correlation Analysis:* A correlation coefficient of 0.69 suggests a strong positive relationship between the traditional and augmented scores, validating the model's consistency while enhancing its sensitivity to election-specific risks.

In the low-risk use case, CVE-2022-48506 saw its score increase from 2.4 to 5.1, highlighting concerns about ballot secrecy. For the medium-risk use case, CVE-2022-1741's score rose from 6.8 to 8.4, emphasizing operational disruptions. In the high-risk use case, CVE-2023-7129's score escalated from 8.8 to 10, showcasing severe implications for vote tampering.

Fig. 1 shows the traditional vs augmented scores for each CVE tested. As shown, the augmented scores are consistently higher for most CVEs because the model incorporates additional dimensions such as tamper resistance, data integrity, and system reliability. These adjustments allow the model to better capture operational risks and compliance issues that traditional scores often

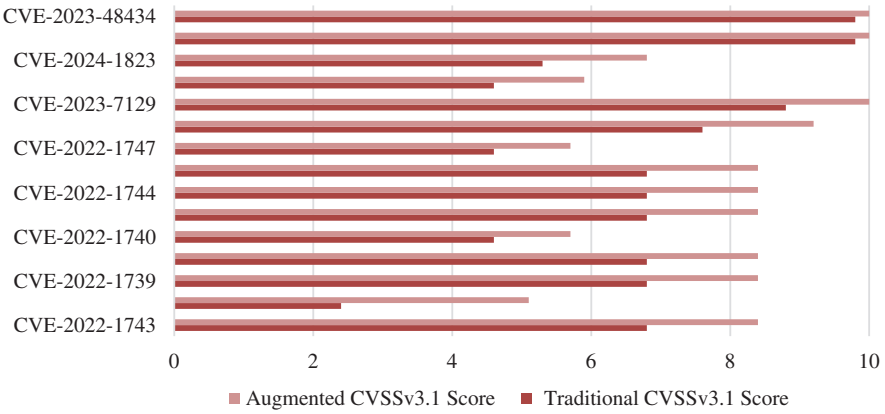

Fig 1. Traditional vs Augmented Scores

overlook. For example, CVE-2022-1741 shows a significant increase in its score under the augmented model, reflecting its operational risks and partial compliance. By accounting for these additional factors, the augmented model improves the prioritization of vulnerabilities, particularly in critical systems like electronic voting, where reliability and security are essential.

5.2. *Summary*

This study showed how effective an augmented CVSSv3.1 model can be when tailored for electronic voting systems. By incorporating election-specific metrics like VVSG compliance, tamper resistance, data integrity, and system reliability, the model provided a more accurate assessment of vulnerabilities. The findings confirmed that the model is capable of prioritizing vulnerabilities that could significantly impact election integrity.

The enhanced model gives stakeholders a practical tool for identifying critical risks, allowing for better resource allocation and more effective mitigation strategies. These results highlight the importance of customizing general vulnerability assessment frameworks to meet the specific needs of different domains.

6. Conclusion

This research successfully developed and validated an augmented CVSSv3.1 model tailored to the unique security challenges of electronic voting systems. By incorporating VVSG-specific criteria, the model showed statistically significant improvements in assessing vulnerabilities. It prioritizes vulnerabilities that directly impact election integrity, making it a valuable resource for election officials and cybersecurity practitioners.

Future research should look into applying this model to other critical infrastructure domains, such as healthcare and energy systems, to see if it can be broadly applicable. Additionally, automating the integration of these augmented metrics into vulnerability management tools could further enhance its usability and effectiveness. This study advances election security by providing a robust framework for protecting the integrity of democratic processes.

References

[1] Wolff J. How Secure Are U.S. Electronic Voting Systems? | Econofact. *econofact.org*. 2022 Nov 01. Available from: https://econofact.org/how-secure-are-u-s-electronic-voting-systems.

[2] Brash R. CVSS 3.1 is still missing the point for OT and critical infrastructure. Linkedin.com. 2019 Jul 16. Available from: https://www.linkedin.com/pulse/cvss-31-still-missing-point-ot-critical-ron-brash/. (accessed Dec. 13, 2024).

[3] Forum of Incident Response and Security Teams. Common vulnerability scoring system v3.1: specification document. *Forum of Incident Response and Security Teams*. Available from: https://www.first.org/cvss/v3.1/specification-document.

[4] National Institute of Standards and Technology. NIST releases NIST IR 8409: measuring the common vulnerability scoring system base score equation. *National Institute of Standards and Technology*. 2022 Nov 15. Available from: https://csrc.nist.gov/News/2022/nist-releases-nist-ir-8409-measuring-the-cvss-base.

[5] Klinedinst D. CVSS and the Internet of Things. *Carnegie Mellon University*. 2015 Sep 02. Available from: https://insights.sei.cmu.edu/blog/cvss-and-the-internet-of-things/.

[6] Householder A, Hatleback E, Sarvepalli V, Spring J, Tyzenhaus L, Yarbrough C. CISA adapts innovative SEI approach to transform vulnerability management landscape. *Carnegie Mellon University*, Feb. 12AD. Available from: https://www.sei.cmu.edu/publications/annual-reviews/2023-year-in-review/year_in_review_article.cfm?customel_datapageid_315013=496833.

[7] Chaeikar SS, Jolfaei A, Mohammad N, Ostovari P. Security principles and challenges in electronic voting. *2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW)*, pp. 38–45, Gold Coast, Australia, 2021.

[8] The Importance and Effectiveness of Cyber Risk Quantification. FAIR Institute. Available from: https://www.fairinstitute.org/what-is-fair. [Accessed: 15-Dec-2024].

[9] Ross T, Tran C. The FAIR model: an objective approach to risk measurement. *Logicgate*. 2023 Apr 05. Available from: https://www.logicgate.com/blog/the-fair-model-an-objective-approach-to-risk-measurement/. (accessed Dec. 22, 2024)

[10] Sanchez GR, Middlemass K. Misinformation is eroding the public's confidence in democracy. Brookings Institution. 2022. Available from: https://www.brookings.edu/articles/misinformation-is-eroding-the-publics-confidence-in-democracy/. [Accessed: Dec. 22, 2024].

[11] Kumar AV, Sarvani GV, Dama S. Blockchain based public cloud security for E-voting system on IoT Environment. *IOP Conf Ser: Mater Sci Eng*. 2020;981(4):042013. doi: 10.1088/1757-899X/981/4/042013. [Accessed: Dec. 22, 2024].

[12] Morgan B. New survey reveals concerns about the security of the nation's voting system ahead of the midterm elections. Harris School of Public Policy, University of Chicago. 2018. Available from: https://harris.uchicago.edu/news-events/news/new-survey-reveals-concerns-about-security-nations-voting-system-ahead-midterm. [Accessed: Dec. 22, 2024].

[13] Hevner AR, March ST, Park J, Ram S. Design science in information systems research. *MIS Q*. 2004;28(1):75–105. doi: 10.2307/25148625. [Accessed: Dec. 22, 2024].

[14] March S. Design and natural science research on information technology. *Decis Support Syst*. 1995;15(4):251–66. doi: 10.1016/0167-9236(94)00041-2. [Accessed: Dec. 22, 2024].

[15] Moret W. Vulnerability Assessment Methods. FHI360, 2014. Available from: https://www.fhi360.org/wp-content/uploads/dru

pal/documents/Vulnerability%20Assessment%20Methods.pdf. [Accessed: Dec. 22, 2024].

[16] Bartlett J. The t-test and robustness to non-normality. The Stats Geek. 2013. Available from: https://thestatsgeek.com/2013/09/28/the-t-test-and-robustness-to-non-normality. [Accessed: Dec. 22, 2024].