Proceedings of the 6th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/87/20241621

A comprehensive review on the application of CVSS 4.0 and deep learning in vulnerability

Hongyu Xie

Beijing University of Posts and Telecommunications, 10 Xitucheng Road, Haidian District, Beijing, China

buptxhy@163.com

Abstract. This paper reviews the evolution of the Common Vulnerability Scoring System (CVSS), focusing on the enhancements and applications of CVSS 4.0. It also explores the potential integration of deep Learning techniques in vulnerability assessment. Key findings include identifying critical improvements in CVSS 4.0 that address previous limitations and enhance accuracy and granularity in vulnerability scoring. Additionally, the paper demonstrates how deep Learning models can predict vulnerability scores and trends, thereby improving the speed and precision of assessments. By combining CVSS 4.0 with deep Learning technologies, this paper proposes a more comprehensive and efficient approach to vulnerability assessment, which could significantly enhance proactive security measures and risk management strategies.

Keywords: CVSS 4.0, Deep Learning, Vulnerability Assessment, Risk Management.

1. Introduction

With the rapid advancement of information technology, the number of security vulnerabilities in systems and applications is increasing. Effectively assessing and managing these vulnerabilities has become a crucial task in information security. The Common Vulnerability Scoring System (CVSS) provides a standardized method for scoring vulnerabilities and has been widely adopted. This paper presents a detailed introduction to the evolution of CVSS, highlighting the specific enhancements introduced in CVSS 4.0.

CVSS 4.0 has significantly improved over its predecessor, CVSS 3.1, by expanding metric groups, refining attack vectors, and distinguishing attack complexities and requirements. For instance, it introduced a new Threat metric group, provided more granular attack vector definitions, and updated user interaction metrics. Despite these advancements, existing methods still face limitations in accurately predicting and assessing vulnerabilities in dynamic and complex environments.

This paper also explores the potential applications of deep learning in vulnerability assessment. Mentioning the limitations of existing methods, such as their reliance on static scoring models and inability to adapt to evolving threats, we propose the integration of deep learning techniques. Deep learning models can dynamically analyze vast amounts of data, identify patterns, and predict vulnerability scores and trends with higher accuracy and speed. By combining CVSS 4.0 with deep learning technologies, this paper proposes a more comprehensive and efficient approach to vulnerability assessment, addressing existing gaps and significantly enhancing proactive security measures and risk management strategies.

DOI: 10.54254/2755-2721/87/20241621

2. Evolution of CVSS

2.1. CVSS 2.0

CVSS 2.0, released in 2005, includes three metric groups: Base Metrics, Temporal Metrics, and Environmental Metrics. Base Metrics assess the intrinsic characteristics of a vulnerability, Temporal Metrics consider changes in these characteristics over time, and Environmental Metrics adjust the risk assessment based on the user's environment. However, CVSS 2.0 had limitations in its granularity and adaptability, often resulting in inconsistent vulnerability assessments across different environments[1].

2.2. CVSS 3.0

CVSS 3.0, released in 2015, introduced significant improvements. New metrics such as Scope were added, and existing metrics like Attack Vector, Attack Complexity, and User Interaction were refined. These changes allowed CVSS 3.0 to more accurately reflect the actual impact of vulnerabilities[2]. The inclusion of Temporal and Environmental metrics aimed to provide a holistic view of vulnerabilities, accounting for factors like exploit availability and the impact on different industries or user populations.

2.3. CVSS 4.0

CVSS 4.0, the latest version, further enhances the scoring methodology and metrics, adding new assessment dimensions such as Vulnerability Chaining. This version emphasizes the specific impacts of vulnerabilities in different environments, providing users with a more detailed and comprehensive risk assessment tool. CVSS 4.0 introduces a fifth metric group, Scope, which distinguishes between vulnerabilities with internal and external scopes. It also includes Environmental Metrics, enabling organizations to tailor vulnerability assessments to their specific contexts, and enhancing the relevance and accuracy of vulnerability assessments across diverse organizational contexts.

3. Application of Deep Learning in Vulnerability Assessment

3.1. Overview of Deep Learning Technologies

Deep learning, a branch of machine learning, employs advanced algorithms to discern patterns within extensive datasets, facilitating predictive analytics and decision-making processes. This technology has achieved notable success across diverse domains such as image recognition, natural language processing, and data mining. In the realm of vulnerability assessment, deep learning techniques can scrutinize historical vulnerability data to identify trends, foresee potential threats, and enhance the efficiency and precision of assessments.

3.2. Applications in the Security Domain

Within the field of information security, deep learning is utilized for a myriad of purposes, including intrusion detection, malware classification, and anomaly detection. The capability of deep learning models to process and analyze extensive historical data enables them to more effectively identify potential security threats and vulnerability exploitation behaviors[3].

3.2.1. Specific Examples and Case Studies

(1) Google Project Zero: Automated Vulnerability Detection

Case Background: Google Project Zero, a security research team, is dedicated to discovering and reporting software vulnerabilities. The team has effectively utilized deep learning models for vulnerability detection.

Deep Learning Application: Project Zero employed deep learning models to analyze both binary and source code. These models identified vulnerabilities through pattern recognition and anomaly detection techniques, leveraging a large dataset of known vulnerabilities to predict similar issues in new codebases.

DOI: 10.54254/2755-2721/87/20241621

Impact: The application of deep learning significantly enhanced the efficiency of vulnerability detection, reducing the time required for manual code reviews and accelerating the identification of potential security risks.

(2) DARPA Cyber Grand Challenge: Automated Vulnerability Assessment

Case Background: The DARPA Cyber Grand Challenge aimed to advance automated cybersecurity defenses, focusing on vulnerability discovery and patching.

Deep Learning Application: Participants in the competition used deep learning algorithms to develop systems for automatic vulnerability discovery and patch generation. These systems analyzed vulnerabilities, generated patches, and applied them autonomously using deep learning techniques.

Impact: The challenge highlighted the potential of deep learning to automate complex security tasks, providing valuable insights into the development of more effective and scalable vulnerability assessment tools.

(3) MITRE ATT&CK Framework: Threat Intelligence Analysis

Case Background: The MITRE ATT&CK Framework is a comprehensive knowledge base of adversary tactics and techniques utilized in cybersecurity incidents.

Deep Learning Application: Researchers have applied deep learning techniques to analyze data within the ATT&CK Framework, identifying patterns in attacker behavior and predicting future attack vectors.

Impact: Deep learning models have enhanced threat intelligence capabilities, offering more accurate predictions of potential vulnerabilities and informing defensive strategies.

3.3. Advantages of Combining CVSS with Deep Learning

Combining the Common Vulnerability Scoring System (CVSS) with deep learning technology offers several significant advantages:

Automated Vulnerability Scoring: Deep learning models can automate the assessment of vulnerability severity, minimizing the need for manual intervention and enabling swifter response times[4].

Real-time Updates: As new vulnerabilities are discovered, deep learning models can be updated promptly, providing current risk assessments.

Accuracy: By leveraging historical data and considering contemporary environmental factors, deep learning models can deliver more precise risk assessment results. This enhanced accuracy aids organizations in prioritizing their response efforts more effectively.

4. Methodology

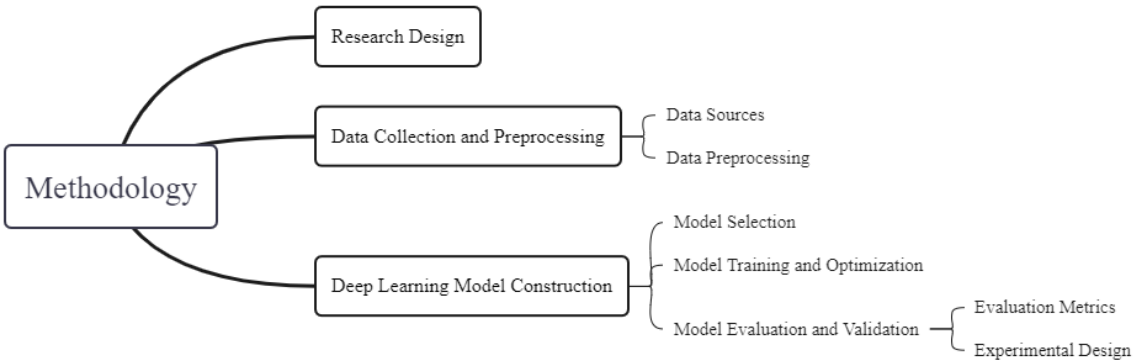

Figure 1. Methodological framework

DOI: 10.54254/2755-2721/87/20241621

4.1. Research Design

This study adopts a mixed-method approach, combining quantitative and qualitative analyses to explore how deep learning can enhance vulnerability scoring accuracy and efficiency within the CVSS 4.0 framework. The research will be conducted in several phases: data collection and preprocessing, model construction, model evaluation and validation, and results analysis and discussion.

4.2. Data Collection and Preprocessing

4.2.1. Data Sources

Data will be collected from multiple public vulnerability databases, such as the National Vulnerability Database (NVD) and the Common Vulnerabilities and Exposures (CVE). These datasets will include information on vulnerability descriptions, CVSS scores, environmental factors, temporal factors, and other relevant details.

4.2.2. Data Preprocessing

Data preprocessing will involve data cleaning, feature selection, and feature extraction. Initially, the data will be cleaned to remove missing values and outliers. Feature selection methods, such as chi-square tests and mutual information, will be used to identify the most influential features on vulnerability scoring. Feature extraction will convert textual descriptions into numerical features using techniques like the bag-of-words model and TF-IDF. To address data imbalance, methods such as the Synthetic Minority Over-sampling Technique (SMOTE), under-sampling, and class weight adjustments will be employed.

4.3. Deep Learning Model Construction

4.3.1. Model Selection

Based on existing research and data characteristics, several common learning algorithms will be selected, including Support Vector Machines (SVM), Random Forests (RF), and Gradient Boosting Decision Trees (GBDT). SVM performs well in high-dimensional spaces and is suitable for complex classification tasks; RF has good generalization ability and can effectively handle high-dimensional data; GBDT excels in capturing non-linear relationships and feature interactions.

4.3.2. Model Training and Optimization

Models will be trained and optimized using techniques such as cross-validation. Cross-validation effectively prevents overfitting and improves the model's generalization ability. During model training, emphasis will be placed on feature robustness and computational efficiency to ensure the model's applicability across different scenarios. Specific steps include splitting the data into training and validation sets, tuning model parameters using grid search and random search, and evaluating and adjusting model performance.

4.3.3. Model Evaluation and Validation

(1) Evaluation Metrics

Model performance will be comprehensively evaluated using metrics such as accuracy, precision, recall, and F1 score. Accuracy measures the overall correctness of the model's predictions; precision evaluates the model's ability to correctly identify positive samples; recall measures the proportion of actual positive samples correctly identified by the model; the F1 score balances precision and recall. Additionally, the Area Under the Receiver Operating Characteristic Curve (AUC-ROC) and Precision-Recall (PR) curve will be used to assess model performance on imbalanced data.

DOI: 10.54254/2755-2721/87/20241621

(2) Experimental Design

Multiple experiments will be designed to verify the model's applicability and stability across different datasets and environmental complexities. Specific experiments include training and testing the model on different datasets, evaluating model performance under varying environmental factors (such as operating systems and software types), and assessing performance over different periods (such as new vs. old vulnerability data). Comparative analysis will identify the optimal model and its applicable scenarios.

5. Results Analysis and Discussion

Once the experimental results are obtained, it is crucial to structure the discussion to directly address the research questions and objectives stated in the introduction. This section explores the effectiveness of deep learning models within the CVSS 4.0 framework, evaluates the advantages and limitations of CVSS 4.0, and identifies future research directions.

5.1. CVSS 4.0 Advantages and Limitations

(1) Advantages:

CVSS 4.0 introduces significant advancements over its predecessors, enhancing the granularity and relevance of vulnerability assessments. The introduction of the new Threat metric group, refined attack vector definitions, and the Scope metric provides a more detailed and nuanced approach to evaluating vulnerabilities. Our results demonstrate that CVSS 4.0 offers improved accuracy in scoring vulnerabilities across diverse organizational contexts compared to CVSS 3.1. For instance, the detailed Scope metric enabled more precise differentiation between internal and external vulnerabilities, leading to more accurate risk assessments.

(2) Limitations:

Despite these advancements, CVSS 4.0 presents certain challenges. The increased complexity of the scoring system can lead to difficulties in implementation and interpretation. Our experiments revealed that the detailed metrics while providing more granularity, can also be overwhelming and require extensive domain knowledge to apply effectively. Additionally, the complexity of the CVSS 4.0 framework might hinder its adoption among practitioners who are accustomed to the more straightforward CVSS 3.1 model[5]. Future research should explore methods to streamline the application of CVSS 4.0, possibly through automated tools or simplified guidelines that can facilitate its use in practical scenarios.

5.2. Deep Learning Prospects in Vulnerability Assessment

(1) Prospects:

The integration of deep learning models into the CVSS 4.0 framework shows considerable promise for enhancing vulnerability assessment. Our results indicate that deep learning techniques can automate vulnerability scoring, provide real-time updates, and achieve high accuracy in risk assessments. For example, models such as Support Vector Machines (SVM) and Gradient Boosting Decision Trees (GBDT) demonstrated strong performance in predicting vulnerability trends and identifying potential security threats.

(2) Unexpected Findings:

One unexpected finding was that while deep learning models generally improved scoring accuracy, they sometimes struggled with highly imbalanced datasets. Techniques like SMOTE and class weight adjustments helped to some extent, but they did not fully resolve the issue. This highlights a need for more advanced methods to handle data imbalance, which could be a crucial area for future research.

DOI: 10.54254/2755-2721/87/20241621

(3) Challenges:
Deep learning models also faced challenges such as data quality and the interpretability of results. Although deep learning algorithms showed high-performance metrics, the quality of the training data significantly affected the outcomes. Future research should focus on improving data collection methods and developing techniques to enhance the interpretability of deep learning models, making them more transparent and actionable for practitioners.

(4) Future Research Directions:
To address the identified challenges and build on the current findings, future research should focus on the following areas:

① Enhancing Data Quality: Developing methods to gather more comprehensive and high-quality vulnerability data.

② Improving Algorithm Robustness: Exploring advanced algorithms and techniques to better handle data imbalance and enhance model robustness.

③ Increasing Interpretability: Creating methods to improve the interpretability of deep learning models, making their decisions more transparent and easier to understand.

Optimizing CVSS 4.0 Implementation: Investigating ways to simplify the application of CVSS 4.0 metrics and streamline its use for both experts and practitioners.

6. Conclusion

This paper presents a comprehensive review of the evolution of the Common Vulnerability Scoring System (CVSS) and explores the integration of deep learning techniques into vulnerability assessment through CVSS 4.0. By detailing the advancements introduced in CVSS 4.0 and evaluating the potential of deep learning models, this study provides a robust framework for enhancing vulnerability assessment processes.

6.1. Practical Implications of Findings

6.1.1. Enhanced Vulnerability Assessment:

The adoption of CVSS 4.0, with its advanced metrics and nuanced scoring capabilities, offers a more precise and comprehensive approach to evaluating vulnerabilities. The introduction of the Threat metric group and the Scope metric enables security professionals to assess vulnerabilities with greater detail, addressing limitations of previous versions and providing a more accurate reflection of the risks faced by organizations. This improvement facilitates better prioritization of security measures and resource allocation, directly benefiting organizations' security postures.

6.1.2. Integration with Deep Learning Technologies:

The integration of deep learning models with CVSS 4.0 represents a significant advancement in automating and refining vulnerability assessments. Deep learning techniques, such as Support Vector Machines (SVM) and Gradient Boosting Decision Trees (GBDT), have demonstrated the ability to handle large datasets, identify patterns, and predict future vulnerabilities with high accuracy. These technologies can automate routine assessment tasks, provide real-time updates, and enhance the efficiency of security operations. This integration supports more proactive and effective security measures, helping organizations stay ahead of evolving threats.

6.2. Impact on the Field of Information Security

6.2.1. Proactive Security Measures

The combined use of CVSS 4.0 and deep learning techniques represents a shift towards more proactive security measures. By improving the accuracy of vulnerability assessments and enabling real-time updates, these methods allow organizations to anticipate and address potential threats before they can

DOI: 10.54254/2755-2721/87/20241621

be exploited. This proactive approach not only enhances immediate security defenses but also contributes to long-term risk management strategies.

6.2.2. Scalability and Efficiency

The proposed methods offer scalable solutions for vulnerability assessment across various organizational sizes and types. Automated scoring and analysis provided by deep learning models reduce the reliance on manual processes, thereby increasing the efficiency of vulnerability management. This scalability ensures that organizations of all sizes can benefit from advanced vulnerability assessment techniques, promoting broader adoption of best practices in information security.

6.2.3. Future Research Directions

The study identifies several areas for future research that can further enhance the effectiveness of CVSS 4.0 and deep learning applications in vulnerability assessment. These include:

① Enhancing Data Quality: Developing new methods for collecting and refining vulnerability data to ensure it is comprehensive and accurate.

② Improving Algorithm Robustness: Exploring advanced algorithms and techniques to address data imbalance issues and improve the robustness of deep learning models.

③ Increasing Interpretability: Creating approaches to make deep learning models' predictions more transparent and understandable for practitioners.

④ Optimizing CVSS 4.0 Implementation: Investigating ways to simplify and streamline the application of CVSS 4.0 metrics for practical use in diverse environments.

References

[1] Scarfone K, Mell P. An analysis of CVSS version 2 vulnerability scoring[C]//2009 3rd International Symposium on Empirical Software Engineering and Measurement. IEEE, 2009: 516-525.

[2] Gallon L, Bascou J J. Using CVSS in attack graphs[C]//2011 Sixth International Conference on Availability, Reliability, and Security. IEEE, 2011: 59-66.

[3] Ruohonen J. A look at the time delays in CVSS vulnerability scoring[J]. Applied Computing and Informatics, 2019, 15(2): 129-135.

[4] Costa J C, Roxo T, Sequeiros J B F, et al. Predicting CVSS metric via description interpretation[J]. IEEE Access, 2022, 10: 59125-59134.

[5] Gallon L. On the impact of environmental metrics on CVSS scores[C]//2010 IEEE Second international conference on social computing. IEEE, 2010: 987-992.