Industrial Engineering Journal

ISSN: 0970-2555

Volume : 54, Issue 5, No.2, May : 2025

A COMPREHENSIVE REVIEW OF CURRENT RESEARCH IN VULNERABILITY MANAGEMENT, CVE SEVERITY AND EXPLOIT PREDICTION, CYBER-THREAT ATTRIBUTION

Prof. Rohit Sharma, Department Of Mechanical Engineering, JD College Of Engineering And Management, Nagpur, Maharashtra, India

Piyush Sharma, **Prajakta Zode, Parth Dhok, Harshal Nakade,** Student, Department Of Information Technology, JD College Of Engineering And Management, Nagpur, Maharashtra, India

Abstract

Despite increasing cybersecurity threats and the growing volume of software vulnerabilities, effec tive vulnerability management remains a critical challenge. This review of the literature synthesizes recent research in key domains, analyzing methodologies and findings in vulnerability severity pre diction, web application vulnerability detection (WAVD), exploit likelihood prediction, cyber threat attribution, and the use of vulnerability databases (VDBs) and expert systems. The analysis highlights the increasing prominence of Artificial Intelligence (AI), particularly Ma chine Learning (ML) and Natural Language Processing (NLP) techniques, including Transformers (like BERT and GPT-2), LSTMs, CNNs, and graph neural networks, applied to tasks ranging from predicting CVSS scores based on textual descriptions to identifying vulnerabilities in code and at tributing attacks using unstructured cyber-threat intelligence (CTI). Key findings reveal significant advances in automated prediction and detection accuracy, yet underscore persistent challenges. These include the crucial distinction and often weak correlation between theoretical vulnerability severity (CVSS) and actual exploitability in the wild (addressed by systems such as EPSS and exploit prediction models, the impact of data quality issues and incon sistencies within VDBs (like NVD's CVE/CPE mapping) on tool effectiveness, and the difficulties in reliable threat attribution stemming from data scarcity, imbalance, and lack of standardized CTI reporting. Future research must focus on improving data quality and consistency, improving context aware ness and generalizability of AI models, and developing integrated approaches that combine severity assessment with dynamic exploit prediction to enable more effective risk-based vulnerability man agement and strengthen cyber resilience.

Keywords: Vulnerability Management, Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), National Vulnerability Database (NVD), Common Platform Enu meration (CPE), Vulnerability Detection, Severity Prediction, Exploit Prediction, Exploit Prediction Scoring System (EPSS), Web Application Security, Cyber Threat Intelligence (CTI), Threat Attribution, Machine Learning (ML), Deep Learning (DL), Natural Language Processing (NLP), MITRE ATT&CK, Expert Systems.

I.Introduction

The management of cybersecurity vulnerabilities is an increasingly critical challenge, evidenced by the continuous rise in newly discovered vulnerabilities each year [2]. Organizations face the significant task of identifying, assessing, and prioritizing these vulnerabilities to safeguard their systems and data from potential exploitation [3]. This necessitates efficient and effective methods for both determining the severity of vulnerabilities and predicting the likelihood of their exploitation in the wild [4]. This review of the literature aims to explore the current landscape of research on CVE severity assessment, exploit prediction, and the broader field of vulnerability detection methodologies, drawing on a range of recent studies and specifications [5]. The Common Vulnerabilities and Exposures (CVE) system serves as a fundamental standard for tracking known vulnerabilities [6]. Assigning a severity level to these CVEs is crucial for prioritizing mitigation efforts, but the sheer volume of vulnerabilities makes manual assessment a challenging and 1 time-

consuming endeavor [3]. Consequently, significant research has been dedicated to automating the prediction of CVE severity [1, 7], with a notable focus on leveraging machine learning (ML) and natural language processing (NLP) techniques to analyze CVE descriptions [8]. For example, one study proposes a novel approach using the GPT-2 large language model to predict vulnerability severity based on CVE descriptions, achieving high accuracy [9]. This research also addresses the issue of imbalanced severity data through oversampling and contextual data augmentation. Beyond severity, understanding the likelihood of a vulnerability being exploited is paramount for effective risk management. Although the Common Vulnerability Scoring System (CVSS) [10] provides a standardized measure of the inherent severity of a vulnerability, it does not always correlate with the actual risk of exploitation [11]. Exploit prediction aims to predict which vulnerabilities are most likely to be leveraged by attackers, with "exploits in the wild" being a key outcome to predict [12]. Machine learning models, often incorporating features from CVE data, Common Platform Enumeration (CPE) information, and the presence of published exploits, are central to this area of research [8]. FastEmbed, an ensemble machine learning algorithm, is one such example that utilizes neural embeddings of vulnerability text combined with other features to predict exploitability [13]. The Exploit Prediction Scoring System (EPSS) [14] represents another significant effort to provide data-driven probabilities of vulnerability exploitation [12]. The broader domain of vulnerability detection methodologies encompasses a wide array of approaches beyond severity prediction and exploiting. These methods are crucial for identifying potential weaknesses in software systems and networks [2]. Research in this area, as highlighted in one review [5], can be classified into approaches such as matching-based methods, which utilize algorithms to compare system data with vulnerability databases. Other categories include methods based on static program analysis, analytic graphs, and feature modeling to represent and analyze vulnerabilities. Notably, AI based approaches, leveraging various machine learning and deep learning techniques, are also increasingly prevalent in vulnerability detection and cyber risk prediction [15, 16, 17]. Furthermore, cyber threat intelligence analysis (CTI) plays a vital role in understanding the context of vulnerabilities and potential attacks [18]. Extracting meaningful information from unstructured CTI reports using natural language processing (NLP) techniques is a key area of research, aiming to attribute cyber threat actors and predict future attacks [19]. Frameworks like MITRE ATT&CK serve as important benchmarks for understanding attacker tactics and techniques. This review of the literature will dive into these key areas, examining the methodologies, findings and limitations of various approaches to the prediction of CVE severity, the prediction of exploits and vulnerability detection. By synthesizing the information from these diverse studies, this review aims to provide a comprehensive understanding of the current state of research and highlight potential directions for future work in this critical field of cybersecurity.

II.Literature Review

This literature review delves into the multifaceted landscape of cybersecurity research, synthesizing recent advancements and persistent challenges across several interconnected domains critical for managing cyber risk: vulnerability severity prediction, exploit prediction, vulnerability detection methodologies, and cyber-threat attribution.

2.1 Vulnerability Severity Prediction

Accurately assessing the severity of vulnerabilities, typically using the Common Vulnerability Scoring System (CVSS) [10], is fundamental for prioritization, yet manual assessment struggles to scale with the volume of disclosures from sources like the National Vulnerability Database (NVD) [6]. Consequently, automating severity prediction has become an important research priority, using machine learning (ML) and natural language processing (NLP) applied to the rich textual information within CVE descriptions [1, 7]. A significant trend involves applying advanced deep learning models to extract semantic meaning from these descriptions. Studies demonstrate the

potential of Transformer architectures, such as BERT, for predicting individual CVSS base metrics by analyzing vulnerability text [20].Others explore the ca pabilities of large language models like GPT-2 for end-to-end severity level classification (e.g., Critical, High, Medium, Low), often achieving high reported accuracy (e.g., 84.2% accuracy with an F1 score of 0.82 reported in one study using contextual data augmentation) [9]. Such approaches frequently require sophisticated text preprocessing and techniques like oversampling or data augmentation to address the inherent class imbalance often found in VDB severity distributions [9]. Beyond Transformers, research 2 also highlights the utility of word embeddings combined with models such as convolutional neural net works (CNNs) and long-short-term memory networks (LSTMs) [9]. While these automated approaches show promise for efficiency, their accuracy can be sensitive to the correct classification of underlying CVSS metrics [11], and ensuring the generalizability of models trained on specific datasets remains an ongoing area of investigation [1, 7].

2.2 Exploit Prediction

Recognizing that CVSS severity alone is an imperfect proxy of real world risk [11], a distinct line of research focuses on exploit prediction, forecasting the likelihood that attackers will actively exploit a vulnerability. This moves beyond theoretical impact (CVSS) to practical threat assessment. A key distinction in recent work is the focus on predicting "exploits in the wild" (actual exploitation observed on networks) rather than just the availability of public "published exploits" (e.g., in Exploit DB or Metasploit) [12]. Studies like [12] utilize large-scale, real-world network monitoring data as ground truth and employ ML models trained on diverse feature sets, including vulnerability characteristics, vendor information, prevalence in scans, and tags extracted via text mining from CVE descriptions. Their findings indicate that while published exploits are an important feature, models incorporating broader data can more effectively identify the roughly 5-6% of vulnerabilities that see active exploitation, significantly outperforming simpler heuristics. Other research confirms the predictive power of features derived from vulnerability descriptions, vendor data, and external references [13], while also noting the critical impact of dataset quality on model performance. Furthermore, some researchers have explored novel data sources, demonstrating the potential of analyzing discussions on social media (e.g., Twitter) or extracting intelligence from dark/deep web forums using neural networks and embeddings to predict exploit threats, sometimes achieving F1-scores around 0.74 when combined with CVSS data [10]. The Exploit Prediction Scoring System (EPSS) [14] represents a standardized effort in this space, aiming to provide data-driven exploitation probabilities to complement CVSS [12]. Challenges in this area include the relative rarity of exploitation events, the need for comprehensive and reliable ground truth data, and the limitations associated with data sources focused on specific vendors or lacking real network traffic context.

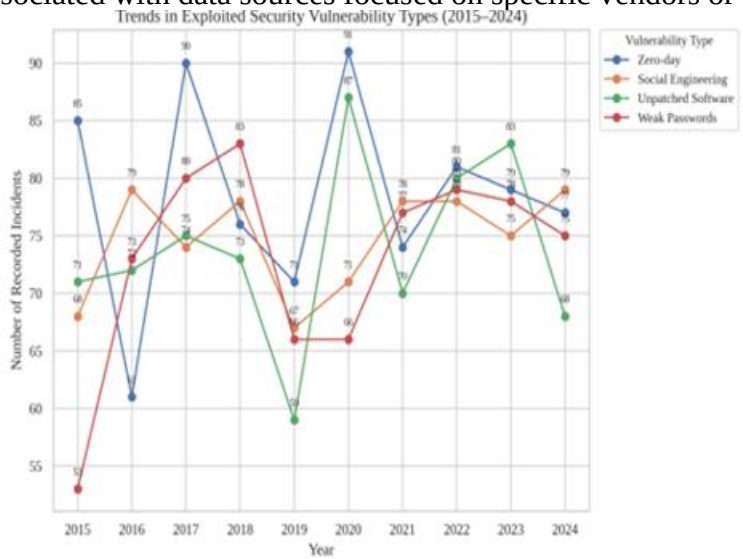

Figure 1: Trends in Exploited Security Vulnerability Types (2015–2024).

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 5, No.2, May : 2025

2.3 Vulnerability Detection Methodologies

Identifying vulnerabilities within systems and applications requires robust detection methodologies, and research continues to refine existing techniques and explore new paradigms, often categorized into several distinct approaches as highlighted by comprehensive reviews [5, 2].

2.3.1 Matching-Based Approaches

Matching-Based Approaches Remain fundamental, particularly for Vulnerability Management Systems (VMS) mapping system assets to known vulnerabilities in VDBs like NVD [6]. Techniques range from using regular expressions for Passive Vulnerability Detection (PVD) by parsing logs [5] to employing string similarity algorithms like Levenshtein distance or Jaro-Winkler to match potentially inconsistent software names from system inventories or advisories against the Common Platform Enumeration (CPE) dictionary [5]. Some methods focus specifically on automating the generation of correct CPE identifiers by combining structural analysis (CPE tree) with keyword analysis from banner text. While these methods are essential, their accuracy (reported around 79-83% in some studies) is fundamentally limited by inconsistencies within and across VDBs, such as missing CPE entries for CVEs and non-standardized software naming conventions [5]. Recent explorations using LLMs (GPT-3/4, ChatGPT) to answer VMS queries suggest they currently lack the completeness and accuracy of structured VDB data for complex tasks [5].

2.3.2 Graph-Based Approaches

Offer a powerful alternative by modeling systems and vulnerability relationships as graphs. Techniques utilize structures like Abstract Syntax Trees (ASTs), Program Dependency Graphs (PDGs), and Con trol/Code Property Graphs (CPGs) often analyzed using Graph Neural Networks (GNNs). Approaches like VulSPG [5] combine static analysis with property graphs, while others like GRACE [5] integrate graph structures with LLMs to leverage semantic, lexical, and syntactic information for enhanced detec tion. These methods excel at mapping complex dependencies but can be computationally intensive

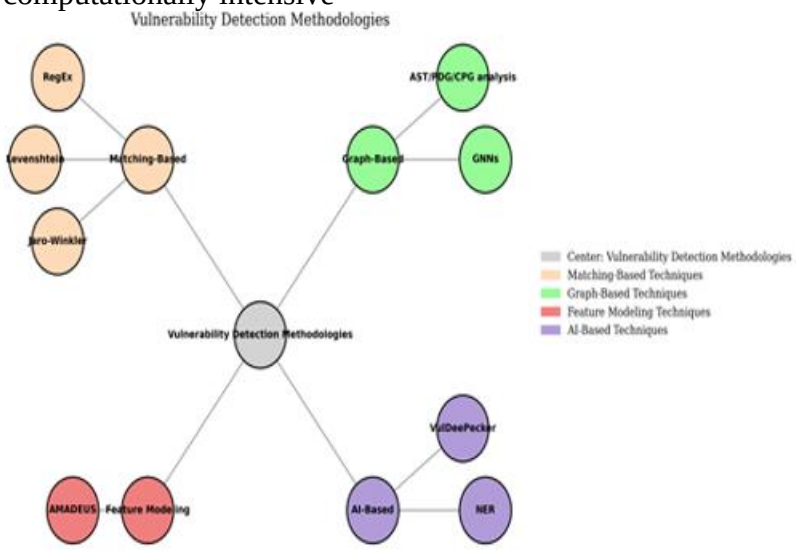

Figure 2: Vulnerability Detection Methodologies.

2.3.3 Feature Model (FM)-Based Approaches

Drawing from software product line engineering, represent system configurations and variability using feature models. This allows for analyzing vulnerabilities in the context of specific feature combinations. Tools like AMADEUS and AMADEUS-Exploit exemplify this by querying VDBs (like NVD [6]) and incorporating exploit information to build feature models representing potential attack scenarios based on system assets.

2.3.4 AI-Based Approaches

Represent a rapidly evolving category. Beyond the NLP/ML techniques used in severity/exploit pre diction, AI is applied broadly in detection [15, 16, 17]. Examples include deep learning models like Bidirectional LSTMs (e.g., VulDeePecker) analyzing code "gadgets", Named Entity Recognition (NER) techniques automating CPE extraction [5], NLP-driven recommender systems narrowing down vulnera bility searches, and ML classifiers identifying database inconsistencies (e.g., VERNIER). While promising 4 for accuracy and speed, these methods often require significant labeled data and face generalizability chal lenges [21]. Across all detection methodologies, persistent challenges include managing high rates of false positives/negatives, addressing the inherent inconsistencies and gaps in VDB data [5], and the effort required for accurate asset inventory, particularly for FM-based approaches [5].

2.4 Cyber-Threat Attribution

Identifying the actors behind cyberattacks (attribution) remains one of the most challenging aspects of cybersecurity due to sophisticated obfuscation and deception tactics. A primary focus of research is developing automated methods to extract actionable intelligence from the vast amounts of unstructured Cyber Threat Intelligence (CTI) reports published by security vendors, researchers, and news outlets. The core challenge lies in processing this unstructured text (often in PDF or plain text) lacking a standard format. NLP techniques are central to extracting key features indicative of specific actors, including their Tactics, Techniques, and Procedures (TTPs)– often mapped to frameworks like MITRE ATT&CK or CAPEC– as well as tools, malware families, targeted sectors/organizations/countries, and specific Indicators of Compromise (IoCs) [19]. Research highlights the importance of domain-specific word embeddings, with models like "Attack2vec" demonstrating superior performance (e.g., 96 percent accuracy reported) compared to general embeddings (like Word2vec) when trained on cybersecurity corpora [19]. Including a richer feature set beyond just TTPs, such as target demographics, has also been shown to improve attribution accuracy [19]. Once features are extracted, various ML classifiers (e.g., SVM, Random Forest, Decision Trees) are typically employed for the final attribution step [19]. Tools like STIXGEN aim to convert extracted information into standardized formats like STIX for better sharing and analysis [19], while frameworks like IL-CyTIS focus on improving threat action extraction [19]. Despite these advancements, significant limitations persist, including the scarcity of large, labeled attribution datasets, the inherent imbalance in available data, and the difficulty in comparing results across studies due to varying methodologies and datasets [19].

III. Advantages of Discovered Approaches

One significant advancement is the introduction of deep learning models for automated vulnerability analysis. The approach proposed by [9] leverages the large-scale language modeling capabilities of GPT 2 to predict CVE severity based on vulnerability descriptions, thereby automating a challenging task that typically requires manual effort. This automation leads to a reduction in manual workload and enables quicker identification of high-severity vulnerabilities, facilitating more efficient mitigation efforts. Furthermore, this method addresses the imbalance in CVSS severity values distribution through over sampling and contextual data augmentation, contributing to its high accuracy (84.2%) and F1 score (0.82) on a substantial dataset of CVEs. Comparative analysis demonstrates the superior performance of this approach against state-of-the-art methods, particularly in terms of precision and F1 scores across all severity classes, and recall for critical, high, and medium severity vulnerabilities.

Another promising area is the application of natural language processing for predicting vulnerability exploitation. [13] introduce fastEmbed, an exploit prediction model combining fastText and Light GBM, which offers the advantage of effectively capturing the semantics and morphology of words in vulnerability-related text. This allows the model to perform well on unbalanced datasets

and outper form baseline models in predicting both proof-of-concept (PoC) exploits and exploits found in the wild. Notably, fastEmbed demonstrates an average overall improvement of 6.283% in predicting PoC exploits and 33.577% in predicting exploits in the wild, with the ability to predict PoC release a median of one day ahead and more effectively detect exploited vulnerabilities in security blogs. The model's focus on the vulnerability summary as a crucial predictive feature highlights the importance of textual information in assessing exploitation likelihood.

Beyond prediction, the automation of knowledge base creation for expert systems in information secu rity risk analysis presents a valuable advantage. The method proposed by [22] focuses on the automated conversion of CVE data from the National Vulnerability Database into an expert system's knowledge base, flagging CVE records with existing exploit tools and incorporating the CISA Known Exploited Vulnerabilities Catalog. This approach enhances the precision and efficiency of risk analysis, providing small- and medium-sized businesses with access to analyses of potential vulnerabilities based on the most up-to-date information. By proactively identifying and mitigating threats, this method contributes to safeguarding critical assets. Furthermore, research into cyber-threat attribution has yielded a novel approach for identifying at tackers based on cyber-threat intelligence (CTI) reports. The proposed framework utilizes a novel em bedding model, "Attack2vec," trained on domain-specific data, enabling more efficient and accurate attribution [19]. A key advantage of this approach is the inclusion of a detailed feature set– encom passing tactics, techniques, procedures, malware, tools, target country, target organization, and target 7 application– offering a more comprehensive attacker profile than previous methods that often focused on a limited set of technical features. The demonstrated high performance (96% accuracy, 96.4% precision, 95.58% recall, and 95.75% F1-measure) underscores the effectiveness of this detailed feature set and the domain-specific embedding model in achieving accurate cyber-threat attribution [19].

In summary, the discovered approaches reviewed in this paper showcase significant advancements in vulnerability management through automation, enhanced feature extraction, improved prediction accuracy, and more comprehensive analysis. These innovations promise to empower cybersecurity pro fessionals with more effective tools and strategies to proactively address vulnerabilities and attribute cyber threats.

IV. Challenges

Despite the advancements highlighted in this review, the automation of cybersecurity vulnerability man agement faces several significant challenges that impact the effectiveness and widespread adoption of these discovered approaches. One prominent area of concern revolves around the quality and consistency of vulnerability data. Several sources emphasize issues with the National Vulnerability Database (NVD) [6]. [5] point out challenges including lack of synchronization between the CPE dictionary and CVE feeds, CVE entries lacking CPE metadata, missing CPE identifiers for software products, and deprecation and typographical errors that lead to mismatches and inaccuracies. The inconsistency of program names across multiple VDBs is also noted. These inconsistencies directly affect the accuracy of matching-based approaches and can introduce errors in fully automated vulnerability analysis. Furthermore, the imbalance in CVSS severity value distributions [10] within vulnerability data poses a challenge for predictive models, although some approaches like the one by [9] attempt to address this through oversampling and data augmentation. Another significant challenge lies in the inherent complexities of vulnerability analysis and prediction. While deep learning models like GPT-2 show promise in automating severity prediction [9], the process of manually evaluating vulnerability severity is inherently challenging due to the need for careful analysis of characteristics and potential impact. Even with automated methods, ensuring high accuracy and minimizing both false positives and negatives remains a hurdle. For exploit prediction, as discussed by the fastEmbed model [13], the accuracy and quality of exploit labeling in databases and the identification of exploits in the wild still require improvement. Prior

research in exploit prediction has also been criticized for potential biases due to data balancing and temporal intermixing [e.g., 12]. Cyber-threat attribution, while benefiting from novel embedding models like Attack2vec [19], is a particularly challenging task due to attackers employing obfuscation and deception techniques to hide their identities. [19] highlight the limited availability of CTI reports due to privacy concerns, leading to imbalanced datasets. The lack of a standard format for these reports further complicates automated information extraction. Moreover, extracting truly meaningful information from the vast amount of unstructured data available in the cyber threat intelligence landscape remains a significant obstacle. The reliance on benchmark frameworks like MITRE ATT&CK for validation, while valuable, also highlights the need for unified benchmarks to enable more consistent and comparable research outcomes.[23] The practical implementation of automated vulnerability management systems also presents chal lenges. Fully automated CPE assignment, crucial for matching-based approaches, is prone to errors due to the aforementioned inconsistencies in VDBs and software naming difficulties [5]. Some methods still require human interaction, such as the CPE assignment step in the Levenshtein distance-based approach, which can be labor-intensive [5]. Furthermore, the diversity and complexity of modern IT environments, including legacy systems, IoT devices, and cloud environments, pose scalability and performance chal lenges for automated detection and response systems. The lack of standardization in CPE, vendor names, and protocols across these diverse environments further complicates automated vulnerability identifica tion [3]. Finally, the rapidly evolving nature of cyber threats presents a continuous challenge [2]. New tech nologies and increasingly sophisticated cyberattacks, including advanced persistent threats and zero-day exploits, can quickly render existing vulnerability detection and mitigation strategies outdated. Main taining up-to-date automated platforms that can continuously learn and adapt to the latest threats is therefore crucial but also a significant undertaking. In conclusion, while the discovered approaches offer promising advancements in vulnerability man agement automation, overcoming the challenges related to data quality, the inherent complexities of vulnerability analysis and threat attribution, practical implementation hurdles, and the ever-evolving threat landscape remains critical for realizing their full potential.

V.Future Directions and Research Gaps

Based on a thorough analysis of the provided sources, several research gaps and potential future directions can be identified:

5.1 Research Gaps:

• Limitations in Existing Vulnerability Severity Prediction: While significant work has been done using machine learning and NLP for CVE severity prediction [9, 20], the accuracy and reliabil ity of these predictions can still be improved. For instance, the study by Kühn et al., 2022 utilizes open-source intelligence, suggesting that relying solely on CVE descriptions might not capture all relevant factors influencing severity. The paper focusing on FastEmbed for exploit prediction also notes that it captures semantics and morphology of words in vulnerability-related text, highlighting the importance of text analysis [13]. However, a comprehensive understanding of which specific textual features or external factors most significantly impact severity prediction is still evolving.

• Challenges in "Exploits in the Wild" Prediction: Predicting real-world exploitation ("ex ploits in the wild") is more critical than predicting the existence of published exploits. [12] em phasize this distinction. While machine learning has been applied to this area, gaps remain in the availability of comprehensive datasets reflecting actual network traffic and exploit activity be yond published repositories. The paper on FastEmbed acknowledges a gap in the ground truth of exploits in the wild, indicating a need for better data collection and labeling methodologies [13]. Furthermore, understanding the temporal dynamics of exploit development and deployment (duration, density, fragmentation, time to first exploit, co-exploitation) needs further investigation.

• Issues with Vulnerability Databases (VDBs): Multiple sources highlight challenges related to the quality and consistency of data in VDBs like the NVD [5]. These issues include: Lack of synchronization between CPE dictionaries and CVE feeds; Missing CPE metadata in CVE entries; Absence of CPE identifiers for certain software products; Deprecation and typographical errors leading to mismatches; Inconsistent naming of software products across different VDBs; Incom pleteness of exploit data in databases like ExploitDB. These inconsistencies impact the effective 5 ness of matching-based vulnerability detection approaches and the overall accuracy of vulnerability management systems [5].

• Limitations of Automated Vulnerability Detection Methods: While various vulnerability detection methodologies exist (matching-based, graph-based, feature modeling-based, AI-based) [5, 2], each has limitations:– Matching-based approaches: Suffer from errors in string-matching algorithms and are heavily reliant on the accuracy and completeness of CPE data in VDBs [5]. They might not provide specific details on accuracy rates.– Graph-based approaches: Face challenges related to the need for unified ontologies, lack of comprehensive high-quality datasets for training and validation, explainability and complexity of results, and adaptation to new data processing paradigms.– Feature modeling-based approaches: Require high initial effort for asset cartography and secu rity control identification, depend on accurate models (errors can lead to incorrect diagnoses), and often need manual updates of feature models. They can also suffer from the quality of security event data in VDBs.– AI-based approaches [e.g., 8, 16, 17, 15]: Can be heavily dependent on the availability and quality of labeled datasets (which can be labor-intensive and time-consuming to create). They might also face challenges in applying to compiled programs if they rely on source code analysis and may be limited to specific vulnerability types. Ensuring the reliability of AI models and reducing hallucination issues requires further study and real-world evaluation.

• Cyber-Threat Attribution Challenges: Attributing cyber-attacks is a complex task with sev eral research gaps [19]. These include: Limited availability of labeled datasets for training attribu tion models; Lack of a standard format for CTI reports (unstructured nature) making automated information extraction difficult; Data imbalance in available datasets; Difficulty in comparing re sults across different studies due to the use of varying datasets and evaluation metrics; The need for more detailed feature sets beyond just TTPs and tools to improve attribution accuracy (including target organization, country, and application); Lack of fully automated, online tools for extracting meaningful information from raw text; Absence of a single benchmark framework for evaluating and comparing different attribution techniques; The challenge of incorporating behavioral features of cyber threat actors due to data availability and extraction difficulties.

5.2 Future Directions:

Based on the identified research gaps, future work could focus on:

• In-depth Analysis of Factors Influencing Vulnerability Severity and Exploitability: Delve deeper into identifying and analyzing the specific vulnerability characteristics (beyond high-level descrip tions) and external factors (e.g., vendor reputation, software popularity, threat landscape trends) that have the most significant impact on both predicted severity and the likelihood of real-world ex ploitation. This could involve a meta-analysis of existing studies to identify consistently important features.

• Comprehensive Evaluation of Datasets for Exploit Prediction: Critically evaluate publicly available and proprietary datasets used for exploit prediction, focusing on their coverage of "exploits in the wild," temporal granularity, and reliability of labeling. Explore strategies for improving the collection and sharing of real-world exploit data while addressing privacy concerns.

• Systematic Assessment of Vulnerability Database Quality and Interoperability: Provide a compar ative analysis of major VDBs, quantifying the extent of data inconsistencies (e.g., missing CPEs, naming variations) and their impact on downstream security processes. Explore existing and po tential solutions for improving VDB data quality and synchronization.

• Comparative Study of Vulnerability Detection Methodologies: Offer a more structured comparison of the strengths and weaknesses of different vulnerability detection approaches (matching-based, graph-based, FM-based, AI-based) across various application domains and software types. In clude quantitative comparisons of performance metrics where available and qualitative analysis of practical applicability and limitations.
• Focus on Hybrid and Ensemble Approaches in Vulnerability Detection: Investigate the growing trend of combining different techniques (e.g., AI with graph-based methods or metaheuristic algo rithms) to enhance vulnerability detection accuracy and reduce false positives/negatives.
• Survey of Techniques and Challenges in Cyber-Threat Attribution: Provide a comprehensive survey of existing techniques for cyber-threat attribution, categorizing them based on features (technical, behavioral, contextual) and methodologies (rule-based, machine learning, knowledge graph-based). Critically analyze challenges like data scarcity, lack of standardization, and verification difficulty.
• Exploration of Benchmark Datasets and Evaluation Frameworks for Cyber-Threat Attribution: Highlight the current lack of standardized datasets and evaluation metrics and discuss potential directions for developing such resources to facilitate more rigorous and comparable research.
• Analysis of the Role of Threat Intelligence Sharing Platforms and Standards: Examine the role of standards like STIX and platforms like TAXII in facilitating CTI sharing and improving attribution efforts. Discuss challenges and opportunities of leveraging open-source intelligence (OSINT).
• Discussion of the Integration of Vulnerability Management and Threat Intelligence: Explore how advancements in vulnerability severity/exploit prediction, detection, and attribution can be in tegrated into a more holistic and proactive cybersecurity strategy. Discuss information flow and synergy opportunities. Addressing these research gaps and exploring future directions can provide a more comprehensive overview and pave the way for future advancements

VI. Conclusion

This review has examined recent advances in cybersecurity vulnerability management, highlighting novel techniques that significantly enhance automation and prediction accuracy through machine learning and natural language processing.

Key advancements include the use of large language models like GPT 2 for high-accuracy CVE severity prediction [9], the application of hybrid models such as FastEmbed to improve the prediction of both proof-of-concept and in-the-wild exploits based on textual analysis [13], the automated conversion of CVE data into structured knowledge bases to streamline risk analysis [22], and the development of domain-specific embeddings like Attack2vec for more effective cyber-threat attribution [19]. Despite these promising developments, the field faces persistent and significant hurdles. A primary concern is the quality and consistency of foundational vulnerability data, with well-documented issues in databases like the NVD, including synchronization problems and incomplete metadata, hindering the reliability of automated tools [5, 6].

Furthermore, the inherent complexity of accurately predicting vul nerability severity [11, 9] and forecasting real-world exploitation [12, 13] remains a fundamental challenge. Cyber-threat attribution efforts are hampered by sophisticated attacker obfuscation, data scarcity, and the lack of standardized CTI reporting and benchmark frameworks [19, 23]. Practical implementation is also complicated by the difficulties in automated asset identification (e.g., CPE assignment) and the need to scale solutions across diverse and complex IT infrastructures [3, 5]. Compounding these issues is the dynamic nature of the cyber threat landscape, which demands continuous adaptation of detection and mitigation strategies [2]. Addressing these challenges requires focused future research efforts.

Key directions include system atically improving the quality, consistency, and interoperability of vulnerability databases [5]. Further work is needed in developing and evaluating robust datasets specifically for predicting exploits "in the wild" [13]. Enhancing predictive models through hybrid

approaches and deeper analysis of contextual factors influencing severity and exploitability is crucial [9]. In threat attribution, research should focus on developing benchmark datasets, exploring behavioral feature extraction, and leveraging threat intel ligence sharing standards [19]. Moreover, developing scalable, adaptable, and integrated vulnerability management systems, potentially incorporating real-time data processing and new curated datasets [16], is essential for improving overall cyber resilience. Pursuing these future directions is vital for overcoming current limitations and advancing the effectiveness of cybersecurity vulnerability management

References

[1] A. Khazaei, M. Ghasemzadeh, and V. Derhami. An Automatic Method for CVSS Score Prediction using Vulnerabilities Description. Journal of Intelligent & Fuzzy Systems, 30(1):89–96, 2016.
[2] Ömer Aslan, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6):1333, 2023.
[3] Hugo Riggs, Shahid Tufail, Imtiaz Parvez, Mohd Tariq, Mohammed Aquib Khan, Asham Amir, Kedari Vineetha Vuda, and Arif I. Sarwat. Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. Sensors, 23(8):4060, 2023.
[4] Mary Jane C. Samonte, Andrea Camille Garcia, Jealine Eleanor E. Gorre, and Joshua Angelo Karl R. Perez. CrowdSurge: A crowd density monitoring solution using smart video surveillance with security vulnerability assessment. Journal of Advances in Information Technology (JAIT), 13(2):173–180, April 2022.
[5] Khalid Bennouk, Nawal Ait Aali, Younès El Bouzekri El Idrissi, Bechir Sebai, Abou Zakaria Faroukhi, and Dorra Mahouachi. A comprehensive review and assessment of cybersecurity vul nerability detection methodologies. Journal of Cybersecurity and Privacy, 4(4):853–908, 2024.
[6] National Institute of Standards and Technology. National vulnerability database (nvd). https: //nvd.nist.gov/. Accessed: 2025-04-27.
[7] C. Elbaz, L. Rilling, and C. Morin. Fighting N-day Vulnerabilities with Automated CVSS Vec tor Prediction at Disclosure. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES ’20), pages 1–10, 2020.
[8] R. Vinayakumar, Mamoun Alazab, K. P. Soman, Prabaharan Poornachandran, and Ameer Al Nemrat. Deep learning approach for intelligent intrusion detection system. IEEE Access, 7:39325 39350, 2019.
[9] A. Manjunatha, Kethan Kota, Anoop S. Babu, and Sree S. Vivek. CVE severity prediction from vulnerability description- A deep learning approach. Procedia Computer Science, 235:3105–3117, 2024.
[10] Common Vulnerability Scoring System. [Online], 2015. Accessed: 2023-03-16.
[11] P. Johnson, R. Lagerström, M. Ekstedt, and U. Franke. Can the Common Vulnerability Scoring System be Trusted? A Bayesian Analysis. IEEE Transactions on Dependable and Secure Computing, 15(6):1002–1015, 2016.
[12] Jay Jacobs, Sasha Romanosky, Idris Adjerid, and Wade Baker. Improving vulnerability remediation through better exploit prediction. Journal of Cybersecurity, 6(1):tyaa015, 2020.
[13] Yong Fang, Yongcheng Liu, Cheng Huang, and Liang Liu. Fastembed: Predicting vulnerability exploitation possibility based on ensemble machine learning algorithm. PLOS ONE, 15:e0228439, 02 2020.
[14] FIRST.org. Exploit prediction scoring system (epss). https://www.first.org/epss/. Accessed: 2025-04-27.

[15] Rakshit Sethi and N. Sivakumar. Utilizing artificial intelligence for automated vulnerability assess ment and patch management. International Journal of Research Publication and Reviews, 5(3):3053 3062, March 2024.
[16] Sravan Kumar Pala. Study to develop AI models for early detection of network vulnerabilities. International Journal of Enhanced Research in Science, Technology & Engineering (IJERSTE), 13(2):88–91, February 2024.
[17] Obaloluwa Ogundairo and Peter Broklyn. Automated vulnerability assessment using machine learn ing. Joural of Cyber Security, 08 2024.
[18] Friederikos Fotis. Economic impact of cyber attacks and effective cyber risk management strategies: A light literature review and case study analysis. EasyChair Preprint 15244, October 2024.
[19] Ehtsham Irshad and Abdul Basit Siddiqui. Cyber threat attribution using unstructured reports in cyber threat intelligence. Egyptian Informatics Journal, 44(3):349–363, 2023.
[20] M. R. Shahid and H. Debar. CVSS-BERT: Explainable Natural Language Processing to Determine the Severity of a Computer Security Vulnerability from its Description. In 20th IEEE International Conference on Machine Learning and Applications (ICMLA), pages 1600–1607, 2021.
[21] Aarthy A. Devi, A. K. Mohan, and M. Sethumadhavan. Wireless Security Auditing: Attack Vectors and Mitigation Strategies. Procedia Computer Science, 115:674–682, 2017.
[22] Dovydas Benetis, Donatas Vitkus, Justinas Janulevicius, Antanas Cenys, and Nikolaj Goranin. Automated conversion of cve records into an expert system, dedicated to information security risk analysis, knowledge-base rules. Electronics, 13:2642, 07 2024.
[23] Bader Al-Sada, Alireza Sadighian, and Gabriele Oligeri. Mitre att&ck: State of the art and way forward. arXiv preprint arXiv:2308.14016, 2023