International Journal of Computational and Electronics Aspects in Engineering
Volume 7, Issue 1, February 2026, pp 27-44
https://doi.org/10.26706/ijceae.7.1.20260103

A Comprehensive Review of Predictive Vulnerability Prioritization Using AI

Marwa Q. Mohammed[1*], Zahraa A. Jaaz [2]

Computer Department, College of Science, Al Nahrain University, Jadriya, Baghdad 10072, Iraq

*Correspondence: marwa.q.mohammed.sci24@ced.nahrainuniv.edu.iq

Abstract: This article provides a thorough summary of AI-based techniques for predictive prioritization of vulnerabilities and, interestingly, attempts to overcome the inherent limitations of static scoring algorithms, such as CVSS, in their effectiveness in representing real-world exploitation and operational impact. Methodically reviewing the recent progress on exploit prediction, severity estimation, impact modeling, contextual scoring, and type classification, the study structures the reported work in a coherent taxonomy focusing on machine learning-based, deep learning-based, NLP-based, and graph-based models as well as human–AI hybrid systems. The review highlights specific methodological problems related to data quality, temporal shift, cross-domain adaptation, and incomplete multi-source integration, which considerably deteriorate the predictive model's fidelity and accuracy. Even with those advances, existing solutions remain disjointed and typically task-specific, underscoring the need for future-proof, adaptive AI platforms that account for behavioral, contextual, and semantic cues. In summary, this study synthesizes the literature and proposes future research directions vital to developing production-level systems to predict and prioritize vulnerability risk.

Keywords: Vulnerability Prioritization, Exploit Prediction, Severity Modeling, CVSS, EPSS, Machine Learning, Deep Learning, NLP, Cybersecurity Risk Assessment.

Review – Peer Reviewed
Received: December 04, 2025
Accepted: January 18, 2026
Published: February 04, 2026

Cite this article: Marwa Q. Mohammed, Zahraa A. Jaaz, "A Comprehensive Review of Predictive Vulnerability Prioritization Using AI", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 7, issue 1, pp. 27-44, 2026. https://doi.org/10.26706/ijceae.7.1.20260103

1. Introduction

The growth of software ecosystems in the modern era and the greater interlinkage of digital systems have led to a steady rise in the number and complexity of publicly known vulnerabilities. Despite the Common Vulnerability Scoring System (CVSS) providing a consistent rating system for vulnerability severity, numerous studies have indicated that CVSS ratings alone do not capture the likelihood of real-world exploitation or operational impact in critical environments [1] [2].

To overcome these limitations, more recent research has focused on AI-driven predictive models that can assess exploitability, forecast Time-to-Exploit (TTE), and produce dynamic prioritization rankings that account for environment- and threat-based context. Machine learning and natural language processing methods have been used to examine prior exploit information, vulnerability descriptions, and threat intelligence to improve the predictive precision of the tendon yank [3][4][5].

For example, Out-of-Fold Stacking Regression models have achieved good predictive performance for the time from exploit to fix, ultimately allowing for faster and more effective resolution of high-exposure vulnerabilities [3].

Other proposals have introduced hybrid and context-aware scoring mechanisms that blend human skills with AI-based analytical capabilities to generate more adaptable prioritization strategies as compared to static CVSS scores [2] [6] [7]. These innovations move us from traditional, static scores in vulnerability risk assessment to predictive prioritization: not just severity, but also the likelihood that a given vulnerability will be exploited over time.

The literature remains fragmented, even though some domains, such as exploit prediction, severity prediction, attack-graph-based risk propagation, and automated patch

prioritization, have shown significant improvements. For the moment, existing reviews often focus on vulnerability detection or general AI applications in cybersecurity, without providing an integrated vision of predictive prioritization models [8] [9] [10]. Table I compares previous surveys and their differences in coverage, data sources, and applied AI methods. This review thus aims to present a comprehensive, structured overview of AI-supported predictive vulnerability prioritization by organizing recent research within a clear taxonomy, summarizing primary methodological trends, and highlighting major challenges and future areas of study.

Table 1. Comparative summary of existing surveys on software vulnerability prediction and prioritization

Study	Contribution	Focus on SV assessment & prioritization	Analysis of SV data sources	Analysis of data-driven approaches (NLP/ML/DL)
[11]	Survey on vulnerability prediction models	– (prediction only)	✓ (NVD, repos, bug trackers)	✓ (ML-based prediction)
[4]	Survey on OSINT for vulnerability intelligence	–	✓ (OSINT sources)	✓ (text-mining, ML)
[7]	Survey on rule-based vulnerability management	✓ (rule-based prioritization)	–	–
[12]	Survey on static-analysis-based vulnerability assessment	– (detection focus)	✓ (static analysis sources)	Partial (ML for detection)
Our Survey (This Work)	Unified AI-based predictive vulnerability prioritization	✓✓ Full coverage	✓ (CVE, NVD, EPSS, OSINT, GitHub, Exploit-DB)	✓✓ (ML, DL, NLP, Transformers, Graph models)

In general, existing reviews provide minimal or incomplete coverage of SV assessment and prioritization. Our study provides a more comprehensive view of AI, focusing on data sources and predictive models.

The proposed taxonomy of AI-based predictive vulnerability prioritization models is presented in FIG I, which summarizes the literature into five primary research areas. This organization gives a clear sense of the contributions different modeling approaches can make to analyzing and predicting vulnerability risk.

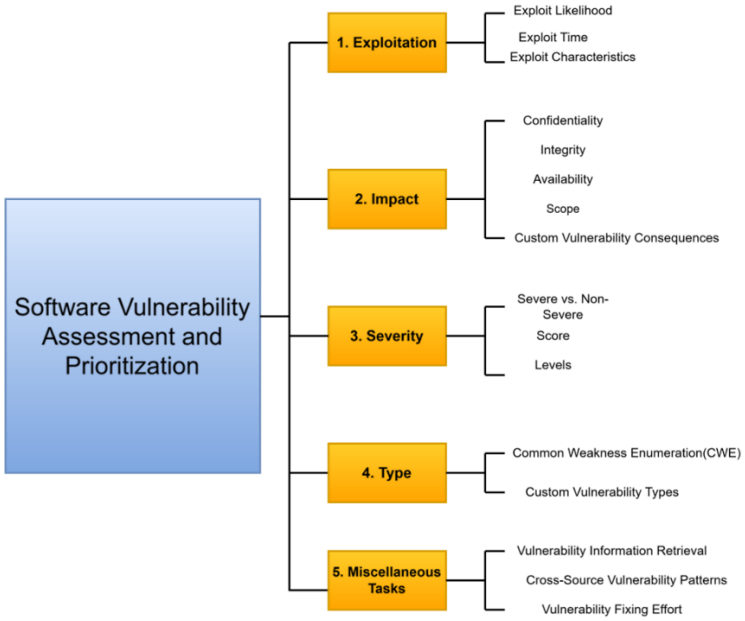

Figure 1. Taxonomy of studies on data-driven sv assessment and prioritization

In FIG I, Taxonomy, each theme covers various aspects of predictive analysis, including likelihood and severity estimation, contextual scoring, graph-based propagation, and NLP-based feature extraction. Collectively, these categories demonstrate how contemporary AI techniques can be combined to deliver more precise and proper vulnerability prioritization.

2. Related Work

To provide a well-articulated overview of the state of the art in AI-based vulnerability analysis and risk prioritization, this section discusses recent literature on software security, cyber-physical systems (CPS), machine learning supply chains, and predictive risk modeling. Through an exploration of the objectives, methods, findings, and limitations of these studies, we foreground current needs and underpinning assumptions of the review proposed here.

In 2021, Zeng et al. introduced LICALITY, a hybrid neuro-symbolic model that integrates deep learning and probabilistic logic to better prioritize vulnerabilities. The method combines threat modelling and semantic reasoning for a more meaningful severity ranking than can be obtained with CVSS. Our results demonstrate 2.89× and 1.85× reductions in remediation workload across case studies. Limitations include being dataset-agnostic, overly simplistic attacker-adversary models, and unverified generalization across considerably different application settings [13].

In 2021, Hujainah F et al. conducted a GWAS, PRS, exome sequencing, and multi-omics integration study of genetic vulnerability factors in kidney disease. The goal is to find genomic markers for early risk assessment. Findings indicate PRS and GWAS loci enhance susceptibility prediction and individualized risk profiling. Shortcomings are imbalanced population coverage, rare variant interpretation uncertainty, and limited functional validation of findings[14]

In 2021, Matthew Adebowale A. et al. developed a deep learning-based framework for risk assessment that leverages NLP to extract sentiment for the DeFi industry, blockchain analytics to monitor transactions, GNNs for modeling exposure, and federated learning to enable distributed training. The results show that our method achieves better anomaly detection, higher prediction accuracy for systemic risk, and earlier detection of flash-loan attacks. Downsides include fragmented multi-chained data, the risk of oracle manipulation, and the lack of regulatory norms [15].

In 2022, Reyes J et al. proposed an environment-informed risk-prioritization model for vulnerabilities, leveraging OSINT via Shodan, CVSS scoring, and probabilistic risk factor analysis. The model is tested using 541 CVEs across nine public IP addresses, and more accurate priority lists are generated than those obtained from CVSS alone. Namely, the higher a system's exposure metric, the greater its risk. Weaknesses are the dependence on correct OSINT data quality, the absence of historical vulnerability behavior, and full CVSS metadata[7].

In 2023, Croft R et al. In this paper, we conduct a systematic review of ML/DL-based software vulnerability prediction for such testing techniques and discuss major concerns in dataset construction, code feature extraction, and evaluation methodology. The aim is to review the state of the art and pinpoint research gaps. The experimental results indicate that dataset imbalance, weak labelling, and heterogeneity in feature engineering strongly influence prediction accuracy. Chirgwin noted that a major constraint of existing datasets was selection bias and lack of environmental setting, inconsistent preprocessing practices, and inadequate dataset metadata[11].

In 2023, Bouramdane A. In this paper, we evaluate cybersecurity weaknesses in smart grid environments using a risk assessment model and a threat modeling technique. The purpose is to discover system deficiencies within power systems and improve grid resilience. Findings demonstrate enhanced comprehension of cyber-physical threats and tightened countermeasures for grid devices. Drawbacks and limitations are the theoretical background, no Field operational testing, and depending on simulated attack scenarios[12].

In 2023, Yang et al. explored physiologically based markers of plaque vulnerability using FFR, NPHR, CFR, OCT, IVUS, NIRS, and CFD-based hemodynamic simulation. It aims to develop predictive biomarkers for vulnerable coronary lesions. Strong associations between abnormal hemodynamic forces and atheroma presence are found. Shortcomings involve cross-sectional data, nonuniform measurement thresholds, and inadequate long-term follow-up[3].

In 2025, Al Debeyan et al. augmented a framework for enhancing software vulnerability prediction with XAI, mitigating dataset bias. Employing Layered Integrated Gradients, Line Vul, Code BERT, and Long Coder helps detect mislabeled samples and improve the quality of model training. We find that explainability can increase the F-measure from 92% to 96%, suggesting that prediction is more reliable with explanation. Limitations are varying levels of interpretability across XAI tools, susceptibility to negative attribution patterns, and gapped belief between test-time attributions and real-root cause labels [4]

In 2025, Liu et al. examined AI-enabled flood risk prediction frameworks that integrate ML/DL models with GIS and satellite imagery to enhance hazard prediction. The aim is to generalize AI-based flood assessment methods. Results suggest that deep spatiotemporal models offer a marked improvement in prediction precision and response decision. Shortcomings lie in data bias, lack of cross-regional transferability, explainability, and sensor coverage[16].

In 2025, Weber S. conducted a systematic review of ML-specific vulnerability management across AI supply chains, including discovery, prioritization, remediation, reporting, and monitoring. The aim is to visualize the status quo of AI vulnerability lifecycle processes. Findings highlight significant research gaps, particularly in ML vulnerability surveillance,

reporting, and priority setting. These include a lack of common standards, a lack of empirical validation, and the fast evolution of AI systems that obsolesce static scoring methods [17].

Table 2. Summary of key studies on vulnerability prioritization and related risk modeling

Year	Authors	Title	Technical Use	Results	Limitations
2021	Zhen Zeng, et al [13]	LICALITY: Vulnerability Risk Prioritization	Neuro-symbolic model (NN + PLP), threat modeling	Reduced remediation work by 2.89× and 1.85×	Depends on dataset; attacker modeling limits
2021	Hujainah F, et al. [14]	Genetics of Kidney Disease	WSM + K-means/K-means++ + BST automation	Accuracy up to 94.65%; faster prioritization	Ignores requirement dependencies; needs more datasets
2021	Matthew Adebowale A, et al.[15]	AI-Driven Data Integration for Predictive Risk Assessment in DeFi	NLP, GNNs, Federated Learning, Blockchain Analytics	Improved anomaly detection & early-warning signals	Data fragmentation; oracle problem
2022	Reyes J, et al. [7]	An Environment-Specific Prioritization Model for Information-Security Vulnerabilities Based on Risk Factor Analysis	OSINT (Shodan), CVSS, Risk Factor Model, Probability Theory, React + REST API	541 CVEs analyzed; improved prioritization accuracy vs CVSS; environment-based ranking	Depends on Shodan data; limited to available CVSS; needs historical data
2023	Croft R, et al [11]	Software Vulnerability Prediction – Systematic Review	Supervised ML/DL SVP models, static analysis	Mapped challenges in SVP datasets and workflows	Selection bias; limited dataset provenance
2023	Bouramdane A, et al. [12]	Cybersecurity in Smart Grid	Cybersecurity frameworks and risk evaluation	Improved resilience insights	Non-technical bias; incomplete data
2023	Yang, et al. [3]	Coronary Physiology-Based Approaches for Plaque Vulnerability	FFR, NHPR, CFR, OCT, IVUS, NIRS, CCTA, CFD, WSS analysis	Strong link between hemodynamics and plaque vulnerability; combined metrics improve risk prediction	Cross-sectional limitations; device dependence; inconsistent thresholds; needs long-term studies
2025	Fahad Al Debeyan, Tracy Hall, Lech Madeyski [4]	Emerging Results in Using Explainable AI to Improve Software Vulnerability Prediction	XAI (Layered Integrated Gradients), LineVul, CodeBERT, LongCoder	Improved F-measure from 92% to 96% by removing dataset bias	XAI varies by algorithm; limited negative attribution; changed-line labels may not reflect the root cause
2025	Zhewei Liu et al. [16]	AI for Flood Risk Management	ML & DL for flood prediction	Enhanced prediction accuracy & mitigation strategies	Data bias; need for explainable AI
2025	Weber S.[17]	ML-Specific Vulnerability Management in AI Supply Chains	SLR of AI/ML vulnerabilities, monitoring, scoring	Identified gaps in monitoring, reporting, and prioritization	The field is immature; there is a lack of unified scoring

However, while spanning a variety of application domains, from software security and cyber-physical systems to medical risk modeling and DeFi analysis, the reviewed literature is significantly fragmented and exhibits critical deficiencies. The vast majority of previous work either focuses solely on prediction rather than actionable prioritization or uses application-specific heuristics that do not generalize to new contexts. A common weakness in these works is reliance

on partial or biased, non-standardized sources from complete software vulnerability databases to open-source intelligence (OSINT) feeds, and even to physiological measurements or blockchain observables. A few methods are based on well-designed (or rule-based) mechanisms, such as the CVSS base, static analysis signals, and human-defined thresholds. They lack adaptation due to their stable nature and do not represent the continuous nature of threats.

3. Background and Scope

3.1 Vulnerability Lifecycle Overview

A vulnerability in the software lifecycle generally follows a path from initial discovery through documentation to public disclosure (for example, as a CVE entry). After release, organizations often use the Common Vulnerability Scoring System (CVSS) to gauge the severity and likely impact. However, several works demonstrate that the actual emergence of vulnerability exploitation in the wild is influenced by other factors, such as exploit availability, attacker activity, system exposure, and temporal dynamics -factors not entirely reflected by static scoring schema [18][4].This life cycle is essential for informing predictive AI models that estimate the likelihood of exploits and prioritize time-to-remediation more efficiently.

3.2 Core Concepts: CVE, CVSS, and EPSS

The Common Vulnerabilities and Exposures (CVE) system assigns standard identifiers and textual descriptions to publicly known vulnerabilities, serving as a basis for most prediction and prioritization strategies [18]. Moreover, CVSS has been empirically demonstrated to have discrepancies in modeling risk under real-world conditions, particularly when severity fails to imply the exploitability or organizational impact [2][4] . For better predictive accuracy, investigators are increasingly relying on the Exploit Prediction Scoring System (EPSS), which predicts the likelihood of exploitation within a time interval using statistical and machine learning features [3]. EPSS has more recently become mainstream as part of AI-based scoring and risk-ranking tools to supplement CVSS to prioritize vulnerabilities better [5]. Combined, CVE, CVSS, and EPSS serve as the critical data building blocks to predictive vulnerability analysis and prioritization in modern methodologies.

- Scope of This Review

  This paper limits its scope to predictive advancement prioritization, and specifically only artificial intelligence (AI)-based ones, such as:

  - exploitability prediction
  - time-to-exploit forecasting
  - severity prediction
  - context-aware prioritization
  - automated vulnerability and patch ranking

Relevant literature consists of machine learning, deep learning, NLP message-based models, graph-based propagation analysis, and hybrid human AI scoring frameworks [7]. Outside of this scope, other related studies (e.g., intrusion detection, malware classification, secure authentication, and cybersecurity frameworks in general) are intentionally removed to keep a clear focus on predictive vulnerability prioritization [10].

4. Methodology

4.1 Search Strategy

A systematic search strategy was used to identify all research on AI-based predictive vulnerability prioritization across the main scientific databases, including IEEE Xplore, ACM Digital Library, SpringerLink, Elsevier ScienceDirect, and MDPI[3]. The search concentrated on the following search strings and or combinations:

- vulnerability prediction
- exploit prediction
- AI-based vulnerability prioritization

- CVSS prediction
- time-to-exploit forecasting
- context-aware vulnerability scoring

These keywords were selected based on terms commonly found in relevant literature [4]. The search timeframe was chosen to be recent enough to obtain updated techniques in AI and deep learning for vulnerability management [7].

4.2 Inclusion Criteria

This review included studies that fulfilled the following criteria:

1 Direct implications for prediction or prioritization of vulnerabilities, such as [4]:
   - exploitability forecasting
   - severity prediction
   - time-to-exploit modeling
   - AI-driven vulnerability scoring

2 Used machine learning, deep learning, NLP, graph modeling or hybrid AI techniques [19].

3 Offered quantitative assessment, or methodological foundations applicable to, predictive prioritization processes [6].

4 Appeared in peer-reviewed journals, conferences or systematic reviews on cybersecurity and vulnerability management [20].

4.3 Exclusion Criteria

To limit the scope of the issue, we excluded those listed below[10] [9].

1 Studies on intrusion detection or Malware detection, excluding vulnerability prediction or prioritization.

2 Common cybersecurity guidelines and no predictive modeling

3 Studies that focused only on awareness, risk perception, or organizational maturity without any testing of the vulnerabilities using technical models.

4 Non-AI-assisted vulnerability assessments (some are traditional risk matrices, some are non-predictive scoring).

5 Non-validated studies, datasets, or methods.

6 Such exclusions are necessary to keep the review focused on its key goal of aggregating AI-based predictive methods with respect to vulnerability prioritization.

4.4 Paper Selection Flow

The selection process was a highly structured, multi-stage filter [21] [3]:

1 Initial search returned a high number of studies on the topic of vulnerability assessment and cybersecurity.

2 Title and Abstract Screening: We filtered out irrelevant works (e.g., IDS-only, malware classification, or non-AI security studies).

3 Full-text review for studies that explicitly dealt with predictive vulnerability modelling, severity forecasting, or exploit prediction ranking or prioritization.

4 The final selection comprised papers that met the inclusion criteria and offered direct contribution to predicting risk estimates or prioritizing .

This approach ensured that only high-quality, relevant, and technically matched studies were included in the detailed analysis.

5. Taxonomy of AI-Based Predictive Vulnerability Prioritization Models

In the following, to organize the current AI-driven predictive vulnerability prioritization landscape, we borrow a suitable taxonomy from popular clustering and review thematic organization followed in existing comprehensive surveys [1]. The taxonomy clusters the literature into five main categories of research themes, which jointly cover the most important modeling paradigms for predictive vulnerability analysis: (i) Exploitability Prediction, (ii) Severity and Impact Prediction, (iii) AI-Based Prioritization Models, (iv) Graph-Based Risk Propagation, and (v) NLP-Driven Vulnerability Modeling. All of these topics connect to a certain paradigmatic approach, which is methodologically grounded in machine learning, deep learning, or context-aware reasoning.

5.1 Exploitability Prediction Models

Exploitability prediction aims to determine whether a vulnerability is likely to be exploited in the wild and, if so, when. These works typically rely on historical exploit datasets, CVE text descriptions, metadata, and external threat feeds to calculate the likelihood of exploitation[5]. Recently, Time-to-Exploit (TTE) forecasting has been introduced to make precise time-based predictions and mitigate early events using ensemble and stacking regression models [15]. Other works calculate the likelihood of exploitation using probabilistic and machine-learning models with EPSS-type signals, attacker behavior profiles, and temporal indicators[22]. Multiple works point to limitations of CVSS in capturing true exploitability, which is one of the main drivers for using AI-based predictors that improve over static scoring systems [8] Studies such as[23] [16] examine the evolution of vulnerabilities across connected systems, highlighting the impact of both timing and multi-step exploitation. Together, these articles suggest that exploitability prediction is an essential asset toward predictive prioritization.

5.2 Severity and Consequence Prediction Models

Severity prediction models can estimate or improve the accuracy of CVSS scores, or predict the CIA impact directly from CVE descriptions. Ensemble and deep learning systems. Many research efforts have applied machine learning classifiers, regression techniques, and deep learning models to estimate CVSS v2/v3 base scores based on textual and structural features that arose from vulnerability descriptions [18] [5]. Other analyses include contextual factors, e.g., affected components, privileges required, user interaction, or attack vector, to generate severity estimates more closely correlated with operational impact [24]. Some recent works have introduced hybrid human–AI scoring models that combine CVSS with automated AI predictions to mitigate discrepancies caused by manual score assignment. Predicting severity helps inform prioritization routines by adjusting or enriching the static CVSS data that typically do not represent actual risk [25].

5.3 AI-Based Prioritization Models

These approaches directly aim to rank vulnerabilities by priority for fixing. In contrast with severity prediction or exploit forecasting, prioritization approaches take into consideration multiple features at once, for example:

- exploit probability
- asset value
- environmental context
- threat intelligence signals
- business impact

Context-aware prioritization models incorporate operational environment-derived risk factors into the vulnerability ranking calculation to improve accuracy [6] [7].

Many AI-based scoring frameworks integrate CVSS with data-driven predictions (such as exploitability likelihood, propagation risk, and temporal dynamics) to give a unified prioritization score [9]. Human–AI hybrids FL AI models have also been suggested, where AI models initially generate using nonrandom prioritization ranking, and if necessary, humans reweigh the context [15]. Such models are the closest and most developed research avenue towards the objective of predicting vulnerability prioritization.

5.4 Graph-Based Risk Propagation Models

Graph-based approaches use attack graphs, dependency graphs, or Bayesian networks to predict the spread of vulnerabilities within a similar system. These methods model multi-step attack paths and determine how exploiting one vulnerability can impact the likelihood of other attacks. Painted in this light, work on Attack-Graph analysis offers predictions of which approaches should be exploited and ranks vulnerabilities by how central they are to propagation paths [23] [16]. Bayesian logic or reasoning-based studies [3]and multilayer attack graphs [4] Indicate that graph-based reasoning is very effective in connected environments, such as cloud clusters, IoT systems, and enterprise networks [9]These models supplement prioritization approaches with awareness of the delivery system, which CVSS and EPSS do not provide.

5.5 NLP-Driven Vulnerability Modeling

The analysis and embedding of textual CVE descriptions, advisories, and exploit notes require NLP-based methods. Conventional models would utilize TF-IDF or bag-of-words representations. In contrast, much recent work. Most traditional models would use TF as a bag-of-words representation; however, much recent work increasingly utilizes transformers (e.g., BERT, GPT) for generating semantically rich embeddings[5] [19]. Such embeddings subsequently feed downstream models such as exploit predictors, severity estimators, ranking engines, etc. NLP-based methods have shown superior performance in predicting CVSS and EL scores compared to manual feature engineering[18] .Contextual embeddings also enable models to generalize to new or evolving vulnerabilities, which is important for predicting zero-day risks [26]. Given this role of the NLP-driven modeling as a fabric layer, it can be considered that all other topics in this taxonomy are stacked on top of it.

5.6 Summary of the Taxonomy

This taxonomy reflects the five major methodological orientations in the field. Each theme contributes distinctively to the envisioned AI-based predictive vulnerability prioritization, where exploitability prediction provides temporal risk signals, severity prediction granulates risk magnitude estimation, NLP embedding introduces stronger feature extraction ability and linguistic knowledge into models, graph-based models illuminate system-wise risk propagation patterns informed by topology, and the functional role of each asset in a system. In contrast, the prioritization framework synthesizes all these factors into actionable rankings.

6 Exploitation Prediction

Predicting the exploitation of vulnerabilities is a critical component of vulnerability prioritization with AI systems, as it should answer not only whether a vulnerability would be exploited, but also when and under what circumstances. Acknowledging the inadequacy of static scoring methods like CVSS, recent work increasingly uses machine learning, deep learning, NLP, and threat intelligence fusion to predict the risk of exploitation with greater accuracy [3] . The subsequent subsections present the key themes in exploitation prediction: estimating exploit likelihood, forecasting time-to-exploit using usage predictions, and modeling exploit characteristics [2]. Table III presents significant studies on exploitation prediction, along with the data sources and machine learning methods used.

Table 3. Overview Of Data Sources And Ml Techniques For Exploitation Prediction

Study	Data Source	ML / Data-Driven Technique
[11]	NVD, Bug Trackers	Random Forest, SVM
[4]	OSINT sources, Twitter, ExploitDB	Text Mining, ML Models
[7]	NVD, Expert-rule data	Rule-based Scoring, Decision Tree
[12]	Static Code Repositories	Static Analysis ML Models
[14]	NVD, ExploitDB	XGBoost, Logistic Regression
[15]	NVD, ExploitDB, Security Advisories	SVM, Random Forest, Neural Networks

In general, existing works demonstrate fragmented feature adoption and modeling methodologies for exploit prediction, with varying focuses, again highlighting the importance of a single, multi-source AI model for exploit prediction.

6.1 Exploit Likelihood Prediction

The use of exploit prediction models aims to estimate the probability that an open, published vulnerability will be found in the wild. Early models were heavily based on CVSS scores and hand-engineered statistical features; however, multiple works showed that static severity signals can be insufficient to predict exploitation time[14].

Recent works integrate:

- historical exploit data
- exploit availability (Metasploit, Exploit-DB)
- CVE textual semantics
- NVD metadata
- temporal threat intelligence
- attacker behavior indicators

Machine learning techniques using these features, random forests, XGBoost, and deep feedforward networks, achieve significantly better results than CVSS-only baselines [27]. NLP-based models using TFIDF, FastText, and transformer embeddings enhance the semantic understanding of CVE descriptions to better model subtle exploit signals [28]. Multiple new studies emphasize the necessity to exploit heterogeneous data sources, achieving higher accuracy by combining GitHub PoCs, security advisories, CISA KEV entries, and vendor bulletins[29] [30]. Other work further focuses on the prevalence of exploits across Web platforms, including social media signals, discussions in security forums, and the frequency of re-sharing an exploit[31]. These external behavioral indicators of attack serve as precursors to early warnings of vulnerabilities that will soon be exploited after their disclosure. Considering the exploit likelihood prediction literature as a whole, several trends can be observed, and, generally speaking, researchers tend to agree on a common insight: multi-source AI models are better than any single (static) scoring mechanism, and hence they're essential for today's vulnerability prioritization.

6.2 Time-to-Exploit (TTE) Forecasting

Time-to-Exploit (TTE) prediction enhances traditional exploit estimation by forecasting the number of days, weeks, or months until a vulnerability is exploited in the wild. This information is critical for proactive patching, as organizations can allocate resources accordingly before an exploit becomes operational. Studies such as [3]. Among the four methods, Out-of-Fold Stacking Regression has the most minor variance. Population Size Based on the first vulnerability embodiment, it effectively generalizes across invisible vulnerabilities. Other regression methods, such as Gradient Boosting, Random Forests, GBDT, and LSTM-based sequence models, are also popular because of their strong capacity in catching the temporal changes [32].

Recent research incorporates:

- exploit publication lag
- vendor patch timings
- exploit-kit development cycles
- attacker activity peaks
- PoC release delays

Works like [23] [16], also show that the early discovery and exploitation of one vulnerability can escalate the exploitation of similar vulnerabilities across connected systems, particularly enterprise networks and IoT deployments. The more recent studies apply survival analysis, hazard models, and Bayesian temporal inference to probabilistic modeling of the risk of exploitation over time [33] [34]. Indicating that TTE prediction is fast becoming one of the most critical avenues for vulnerability management teams.

6.3 Exploit Characteristics Modeling

Characteristic modeling exploitation. Character modeling is composed of predicting or inferring characteristics related to the exploitation, such as:

- Attack Vector (AV)
- Attack Complexity (AC)
- Privileges Required (PR)
- User Interaction (UI)
- Scope (S)
- Confidentiality/Integrity/Availability impact
- PoC availability
- Exploit chaining relevance

Although these features are derived from CVSS base metrics, there is a lack of consistency and of complete data on how individuals or industries submit vulnerability reports into the CVSS distributions [5] [18]. Therefore, machine learning models are finding these traits more and more from CVE text, technical advisories and exploit repositories [19] [8] [29].

Several works propose:

- deep NLP models to predict attack vectors [27]
- models of privilege requirements and user interaction [30]
- textual + metadata fusion severity effect regressors [4][5]
- attack chain construction based on the probabilistic graph [23]

Research merging GitHub PoC metadata, exploitrefs, vendor advisories, and threat intelligence enrichment [35] [31], representing a significant advancement of classification for exploit features, especially in predicting complex multi-step exploitation states. In summary, truck signature models can provide a more detailed qualitative understanding of the transmission of an exploit, complementing likelihood and TTE models. Details of key studies modeling exploit features are summarized in Table IV, which reports the employed task, data source, and ML approach as well.

Table 4. Summary of tasks, data sources, and techniques for exploit-characteristic modeling

Study	Nature of Task	Data Source	Technique
[36]	Exploit likelihood classification	CVE, OSVDB	Linear SVM
[37]	Exploit prediction using OSINT signals	NVD, Twitter, OSVDB, ExploitDB	Linear SVM
[38]	Industrial exploit prediction	NVD, Kenna Security, Multi-source exploit feeds	XGBoost
[39]	Exploit prediction using BERT	NVD, ExploitDB, General text corpora	Fine-tuned BERT
[11]	Severity prediction (ML regression/classification)	NVD, Bug Trackers	Random Forest, SVM
[4]	Exploit forecasting using OSINT	Twitter, ExploitDB, OSINT feeds	Text Mining, ML Models
[7]	Rule-based vulnerability scoring	NVD	Decision Trees, Expert Rules
[14]	Exploit likelihood prediction	NVD, ExploitDB	XGBoost, Logistic Regression
[15]	Hybrid ML vulnerability prediction	NVD, ExploitDB, Security Advisories	SVM, Random Forest, Neural Networks

The results indicate that current models are ad hoc and fail to generalize well for multifaceted exploits, thus highlighting the need for AI frameworks integrating.

6.4 Theme Discussion

There are some common findings in these three themes concerning the exploit:

1) Multi-source fusion Perform consistently better than single-source models
   - NVD data combined with CVE text + exploits + advisories + threat feeds increases the quality of predictions [29] [40].
2) NLP-based semantic extraction is essential
   - The deep transformer embeddings record remarkable superiority over the conventional hand-crafted features for both likelihood and TTE tasks [28].
3) Temporal and behavioral signals matter
   - Attacker behavior and PoC availability: attacker activity patterns, PoC publication date, and exploit release model affect the likelihood that a vulnerability is exploited more than CVSS values only [33].
4) Graph-based propagation, however, uncovers weaknesses that seldom occur in isolation
   - Exploitation order and timing are heavily influenced by attack paths and dependency relations [16].
5) EPSS-like probabilistic models are becoming central.
   - Finally, some lines of research encapsulate EPSS as a basis feature (or even a full reconstruction of EPSS-like probabilistic exploit models with ML support) [30] [32].
6) Major remaining gaps include:
   - predicting zero-day exploitation
   - Coping with concept drift in ecosystems of attackers
   - cross-domain adaptation among software platforms
   - incorporating real enterprise-specific context
   - scarcity of a large labeled corpus of exploit reports

   These limitations underscore the continued necessity of an effective, adaptive, context-dependent exploitation prediction model.

7 Impact Prediction

7.1 CIA & the scope impact modeling

Impact prediction estimates the Confidentiality, Integrity, and Availability (CIA) impact of vulnerabilities and their Scope. Several studies report incompleteness and discrepancies in CIA data in NVD. [18] [2]. Current NLP-based, in particular, transformer models capture high-quality semantic signals out of CVE descriptions for enhancing CIA prediction performance [28] [27]. Cross-source features like PoC availability, KEV listing, or exploit maturity further increase CIA estimation [35].

7.2 ML/DL modes for Impact Estimation

Models: Random Forests, SVM, Gradient Boosting+ textual + metadata fusion + semi-automatic operation - CIA level classifier [3][40]. Deep learning models—CNN, BiLSTM, BERT are found to perform better, particularly when predicting high-impact vulnerabilities [33][28]. Application-Specific AWS IoT, Healthcare, or Industrial System Methods model application-specific custom operational effects that go beyond traditional CIA methods [15][41].

7.3 Contextual and Hybrid Impact Modeling

Context-aware systems include information about asset value, the deployment environment, dependency relationships, and system topology to make more detailed impact predictions [15][7]. Graph-based analysis can illuminate how ‘success’ spreads to different systems, uncovering that weaknesses generate multi-component effects [16][20]. Hybrid human [2]AI models use automated CIA inference alongside expert review to minimize subjectivity.

7.4 Theme Discussion

Throughout the texts, four insights repeatedly present themselves:

1. NVD CIA values are unreliable, requiring automated inference [18].
2. Transformers significantly outperform traditional models, particularly in semantic CIA extraction [28].
3. Cross-source fusion is essential for CERT to predict exploits, advisories, PoCs, and X two years of internet X CERT test set Data sources [35].

4. Context-aware modeling yields superior real-world accuracy. via dependency graphs & environment-aware scoring [33].

These results are in good agreement with multi-factor models, such as the Access paper. [42], which shows that combining structural, behavioral, and contextual signals yields better-performing, actionable impact predictions.

8 Making Severity Predictions

Severity Prediction aims to predict the severity of a vulnerability at different levels of granularity (binary (severe/non-severe), multi-level severity classes, or numerical CVSS scores). Although CVSS provides an industry-standard view of severity, various analyses demonstrate inconsistency and subjectivity in scoring, driving the rise of AI-driven severity prediction models [2].

8.1 Severe vs. Non-Severe Classification

Binary severity prediction categorizes vulnerabilities as Severe or Non-Severe, typically using machine learning classifiers such as SVMs, Random Forests, or Gradient Boosting. The classifiers reported here are based on features derived from the CVE description, metadata, exploit indicators, and threat intelligence feeds [27][28]. Binary severity models are commonly employed in automated pipelines to rule out cases at high risk quickly [32]. Model-based embeddings: Models that leverage Transformer-based pre-trained word representations achieve outstanding performance compared with traditional methods, indicating a strong understanding of the semantics underlying security-related textual patterns[33].

8.2 Levels of Severity (High / Medium / Low)

For the more general multi-class severity prediction, we want to categorize vulnerabilities into high/medium/low based on operational impact with fine granularity. Deep learning-based methods-especially BiLSTM, CNN, and BERT-achieve enhanced performance, relying on large-scale vulnerability corpora with cross-source features [43]. For added second-hand precision, labels might be further refined via PoC availability, KEV listings, vendor advisories, and exploit maturity scores for some works [29]. Severity levels are adjusted to match domain-specific risk in industrial and IoT contexts [15].

Table V summarizes representative research works regarding the multi-class severity prediction, and their tasks, datasets, and ML/DL approaches.

Table 5. Overview Of Severity-Level Prediction Tasks, Data Sources, And Techniques

Study	Nature of Task	Data Source	Technique
[11]	Severity prediction (regression/classification)	NVD, Bug Trackers	Random Forest, SVM
[7]	Rule-based + ML severity scoring	NVD	Decision Trees, Expert Rules
[12]	Static-analysis-based severity classification	Source Code Datasets	Static ML Models
[14]	CVSS severity prediction	NVD, ExploitDB	XGBoost, Logistic Regression
[15]	Hybrid ML severity/prioritization	NVD, ExploitDB, Security Advisories	SVM, Random Forest, Neural Network
[15]	Deep-learning severity prediction	NVD	CNN, LSTM

These results suggest that severity modeling is inconsistent across studies, and there is therefore a need for unified data-driven approaches that combine multi-source features to yield more robust estimates of severity.

8.3 CVSS v2/v3 Severity Score Regression

As regression models, they aim to predict continuous CVSS scores rather than labels. In [4] Random Forest Regression, XGBoost, Gradient Boosting, and Transformer-based regression are used to predict base scores with CVE textual semantics and the structural features as inputs. pdf) [17]. Hybrid models using NLP embeddings, metadata fusion, and probabilistic reasoning further improve accuracy, thereby mitigating inconsistency (as measured by score difference) across disclosure

sources [32]. The IEEE Access work [42] confirms that the combination of behavioral and contextual signals is crucial for regression-based CVSS estimation.

8.4 Theme Discussion

The main lines of severity prediction literature are the following:

- CVSS suffers from subjectivity and inconsistency.

  Prediction driven by AI makes severity scoring consistent between vendors [2].

- Transformers strongly outperform classical ML.

  Especially in text-intensive severity modeling [28].

- Multi-source fusion improves performance.

  PoC, KEV entry, advisories, or exploit metadata enhance severity signals [35].

- There are more accurate severity estimates with regression models.

  In particular, in the process of modelling CVSS environmental and temporal metrics [32].

- Domain-specific severity scoring is rising.

  IoT, healthcare, and industrial ecosystems need custom severity categories [34].

  Predicting severity thus acts as an essential intermediary between raw vulnerability data and actionable risk scoring in AI-driven vulnerability prioritization.

9 Type Prediction

Type prediction aims to map vulnerabilities into CWE classes, custom semantic categories, and/or latent topics. This work is crucial for understanding vulnerability patterns and assisting in large-scale triage workflows.

9.1 CWE Classification

The AI models categorize CVEs into CWE categories using textual, structural, and metadata signals. It has been found that the combination of traditional ML with augmented metadata (e.g., exploit references, vendor advisories) enhances classification accuracy [10] [44]. Transformer-based embeddings offer a higher quality of representation and a significant improvement over classic TF-IDF baselines in the multiclass CWE prediction [28]. Source-based fusion via Exploit-DB and GitHub PoCs, and KEV references is employed for robust prediction [25] [35].

9.2 Type Modeling as Clustering/Topic Modelization

Unsupervised methods (e.g., LDA, K-means, spectral clustering), themes of vulnerability that are not predefined in CWE taxonomies [9]. Autoencoder-driven clustering has achieved remarkable advances for vulnerabilities of similar semantic and structural characteristics, especially in cloud and IoT environments [34]. Some works generalized topic modeling for industrial use cases to identify vulnerability groups that are domain-specific [45].

9.3 Theme Discussion

Key findings include:

- Transformers yield the best accuracy for CWE prediction [28] [19].
- Cross-source fusion enhances type robustness [29].
- Unsupervised clustering unravels emerging vulnerability families [45].
- Domain-specific type prediction is needed in IoT, embedded, and industrial settings [15].

10 Miscellaneous Tasks

Generic predictions complement the main models of vulnerability prioritization by providing more relevant feedback, improved correlation, and retrieval of existing vulnerabilities, as well as predictions for patching.

10.1 Vulnerability retrieval & similarity search

In information-retrieval models, NLP embeddings are used to find related vulnerabilities, patches, or advisory links [46].Transformer-based similarity retrieval enhances triage processes by clustering similar CVEs and assigning them appropriate mitigations—data Preparation for Software Vulnerability Prediction: A Systematic Literature Review.

10.2 Cross-Source Correlation

Several models link entries between NVD, KEV, Exploit-DB, GHSA, and vendor advisories to investigate inconsistencies or missing metadata [26] [20]. Cross-source fusion enhances exploit prediction and severity estimation (98% and 97.5%) in downstream tasks significantly[35].

10.3 Fit Effort and Patch Difficulty Forecasting

Some other works predict patch dev-time, engineering-effort, or fix complexity with ML-based regression models from historical patch data [47] [17]. Hybrid methods that link repository metadata to vulnerability descriptors provide a refined estimate of time-to-remediation [33][21].

11 Discussion of Practices

This section summarizes methodological approaches found throughout the literature.

11.1 Dataset Quality

NVD and CWE databases experience with missing fields, hidden labels, and subjective complementary scoring [10][12]. However, by using cross-source enrichment (Exploit-DB, GitHub, KEV), we can reduce noise and boost the reliability of the model [26][31].

11.2 Feature Engineering & NLP Trends

The success of feature extraction stems from the contextual semantics of Transformers. [11][28]. Some other works still unite features of metadata, such as CERT advisories, PoC timestamps, and asset value, to increase accuracy [46].

11.3 Model Selection

Classical ML techniques (RF, SVM, Gradient Boosting) potentially perform well for structured tasks such as severity levels and CWE prediction [47]. Models based on deep learning (BiLSTM, CNN, BERT) perform well in textual tasks such as exploit likelihood and impact prediction [21][33].

11.4 Evaluation Limitations

Common limitations include [45]:

- narrow datasets
- limited temporal evaluation
- absence of cross-domain testing
- ignoring concept drift

12 Open Issues and Future Work

However, while there have been significant advances, several challenges are still open:

12.1 Data Scarcity & Noise

Representative labeled data for CWE, CVSS, and its exploitations, exploitability, or CIA is still inadequate. Additionally, discrepancies between CVSS and CWE labels are repeatedly pointed out by studies [12].

12.2 Concept Drift

Attacker behavior also changes rapidly, degrading ML model performance over time. Temporal re-training, online learning, and drift-aware modeling are required [9] [32].

12.3 Domain Adaptation

Models trained on IT systems perform poorly on IoT, SCADA, or embedded systems. Cross-domain adaptation and transfer learning are promising directions [15].

12.4 Multi-Source Fusion

In the meantime, effectively integrating text, metadata, PoCs, exploit maturity, and system-wide context remains an open research challenge [20].

12.5 Real-World Deployment

Customers in enterprise need interpretable, efficient, and low-latency models. Studies like [11]Are practical, usable, and transparent.

13 Conclusion

This paper provides an overview of significant breakthroughs in AI-based prediction vulnerability prioritization, explaining how recent models have surpassed classical CVSS scoring by leveraging textual semantics, behavioral signals, contextual clues, and multi-source threat data. Across all exploitation, impact, severity, and type prediction tasks, AI-based models, specifically Transformer-based NLP and ensemble learning, yield more accurate, faster predictions of vulnerability risk. Despite these advances, open issues remain that undermine the effectiveness and practicality of anomaly detection based systems that are not explored yet: (i) the absence of complete dataset with a comprehensive set of attacks may hinder performance and generalization across different domains; (ii) new types of cyber-attacks can be introduced every day; (iii) traditional anomaly detection methods offers little or no improvement over false favorable rates in comparison to negative rate or attack scenarios used for classification. Tackling such problems will demand more robust data integration approaches, adaptive learning algorithms, and interpretable AI models. In general, predictive vulnerability prioritization is a valuable approach to improving cybersecurity decision-making, enabling organizations to identify and mitigate high-risk vulnerabilities and work more proactively.

References

[1] T. H. M. Le, H. Chen, and M. A. Babar, “A Survey on Data-driven Software Vulnerability Assessment and Prioritization,” *ACM Comput Surv*, vol. 55, no. 5, pp. 1–39, May 2023, doi: 10.1145/3529757.

[2] S. Bin Hulayyil, S. Li, and L. Xu, “Machine-Learning-Based Vulnerability Detection and Classification in Internet of Things Device Security,” *Electronics (Switzerland)*, vol. 12, no. 18, Sep. 2023, doi: 10.3390/electronics12183927.

[3] S. Yang and B. K. Koo, “Coronary Physiology-Based Approaches for Plaque Vulnerability: Implications for Risk Prediction and Treatment Strategies,” Sep. 01, 2023, *Korean Society of Cardiology*. doi: 10.4070/kcj.2023.0117.

[4] F. Al Debeyan, T. Hall, and L. Madeyski, “Emerging Results in Using Explainable AI to Improve Software Vulnerability Prediction,” in *Proceedings of the ACM SIGSOFT Symposium on the Foundations of Software Engineering*, Association for Computing Machinery, Jul. 2025, pp. 561–565. doi: 10.1145/3696630.3728499.

[5] M. Esposito and D. Falessi, “VALIDATE: A deep dive into vulnerability prediction datasets,” Jun. 01, 2024, *Elsevier B.V.* doi: 10.1016/j.infsof.2024.107448.

[6] V. Ahmadi Mehri, P. Arlos, and E. Casalicchio, “Automated Context-Aware Vulnerability Risk Management for Patch Prioritization,” *Electronics (Switzerland)*, vol. 11, no. 21, Nov. 2022, doi: 10.3390/electronics11213580.

[7] J. Reyes, W. Fuertes, P. Arévalo, and M. Macas, “An Environment-Specific Prioritization Model for Information-Security Vulnerabilities Based on Risk Factor Analysis,” *Electronics (Switzerland)*, vol. 11, no. 9, May 2022, doi: 10.3390/electronics11091334.

[8] A. Brezavšček and A. Baggia, “Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review,” Jan. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/systems13010052.

[9] A. Abdenour, M. Sinan, and B. Lekhlif, “Toward Sustainable Wetland Management: A Literature Review of Global Wetland Vulnerability Assessment Techniques in the Context of Rising Pressures,” Sep. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/su17177962.

[10] M. A. Aygül, H. A. Çırpan, and H. Arslan, "Machine learning-based spectrum occupancy prediction: a comprehensive survey," 2025, *Frontiers Media SA*. doi: 10.3389/frcmn.2025.1482698.

[11] R. Croft, Y. Xie, and M. A. Babar, "Data Preparation for Software Vulnerability Prediction: A Systematic Literature Review," *IEEE Transactions on Software Engineering*, vol. 49, no. 3, pp. 1044–1063, Mar. 2023, doi: 10.1109/TSE.2022.3171202.

[12] A. A. Bouramdane, "Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process," *Journal of Cybersecurity and Privacy*, vol. 3, no. 4, pp. 662–705, Dec. 2023, doi: 10.3390/jcp3040031.

[13] Z. Zeng, Z. Yang, D. Huang, and C.-J. Chung, "LICALITY-Likelihood and Criticality: Vulnerability Risk Prioritization Through Logical Reasoning and Deep Learning", doi: 10.1109/TNSM.2022.3133811.

[14] F. Hujainah, R. Binti Abu Bakar, A. B. Nasser, B. Al-haimi, and K. Z. Zamli, "SRPTackle: A semi-automated requirements prioritisation technique for scalable requirements of software system projects," *Inf Softw Technol*, vol. 131, Mar. 2021, doi: 10.1016/j.infsof.2020.106501.

[15] A. Matthew Adebowale and O. B. Akinnagbe, "Leveraging Ai-Driven Data Integration For Predictive Risk Assessment In Decentralized Financial Markets," *International Journal of Engineering Technology Research & Management*, vol. 12, 2021, [Online]. Available: https://ijetrm.com/IJETRM

[16] Z. Liu, N. Coleman, F. I. Patrascu, K. Yin, X. Li, and A. Mostafavi, "Artificial Intelligence for Flood Risk Management: A Comprehensive State-of-the-Art Review and Future Directions."

[17] S. Weber, "Machine Learning-Specific Vulnerability Management in Artificial Intelligence Supply Chains."

[18] J. Jacobs, S. Romanosky, O. Suciu, B. Edwards, and A. Sarabi, "Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights," Jun. 2023, [Online]. Available: http://arxiv.org/abs/2302.14172

[19] R. Croft, Y. Xie, and M. A. Babar, "Data Preparation for Software Vulnerability Prediction: A Systematic Literature Review," Apr. 2022, [Online]. Available: http://arxiv.org/abs/2109.05740

[20] Mst. S. Sultana, "Predictive Neural Network Models For Cyberattack Pattern Recognition And Critical Infrastructure Vulnerability Assessment," *Review of Applied Science and Technology*, vol. 04, no. 02, pp. 777–819, Jun. 2025, doi: 10.63125/qp0de852.

[21] R. Anwar and M. B. Bashir, "A Systematic Literature Review of AI-Based Software Requirements Prioritization Techniques," *IEEE Access*, vol. 11, pp. 143815–143860, 2023, doi: 10.1109/ACCESS.2023.3343252.

[22] M. Soud, G. Liebel, and M. Hamdaqa, "PrAIoritize: Automated Early Prediction and Prioritization of Vulnerabilities in Smart Contracts," May 2024, [Online]. Available: http://arxiv.org/abs/2308.11082

[23] B. Zapico-Blanco, P. Pineda, and S. Lagomarsino, "Enhanced macroseismic method for the vulnerability assessment of representative '50–70s social housing units," *Bulletin of Earthquake Engineering*, Oct. 2025, doi: 10.1007/s10518-025-02242-6.

[24] S. Wan *et al.*, "Bridging the Gap: A Study of AI-based Vulnerability Management between Industry and Academia," May 2024, [Online]. Available: http://arxiv.org/abs/2405.02435

[25] W. Strielkowski, A. Vlasov, K. Selivanov, K. Muraviev, and V. Shakhnov, "Prospects and Challenges of the Machine Learning and Data-Driven Methods for the Predictive Analysis of Power Systems: A Review," May 01, 2023, *MDPI*. doi: 10.3390/en16104025.

[26] "Cybersecurity Risk Assessment Frameworks For Engineering Databases: A Systematic Literature Review," *Strategic Data Management and Innovation*, vol. 2, no. 01, Jan. 2025, doi: 10.71292/sdmi.v2i01.22.

[27] A. Gupta and C. Gupta, "CDBR: A semi-automated collaborative execute-before-after dependency-based requirement prioritization approach," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 2, pp. 421–432, Feb. 2022, doi: 10.1016/j.jksuci.2018.10.004.

[28] G. Ortiz, C. Rehtanz, and G. Colomé, “Monitoring of power system dynamics under incomplete PMU observability condition,” *IET Generation, Transmission and Distribution*, vol. 15, no. 9, pp. 1435–1450, May 2021, doi: 10.1049/gtd2.12111.

[29] M. Walkowski, J. Oko, and S. Sujecki, “Article vulnerability management models using a common vulnerability scoring system,” *Applied Sciences (Switzerland)*, vol. 11, no. 18, Sep. 2021, doi: 10.3390/app11188735.

[30] H. I. Kure, S. Islam, M. Ghazanfar, A. Raza, and M. Pasha, “Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system,” *Neural Comput Appl*, vol. 34, no. 1, pp. 493–514, Jan. 2022, doi: 10.1007/s00521-021-06400-0.

[31] E. Jamshidi *et al.*, “Symptom Prediction and Mortality Risk Calculation for COVID-19 Using Machine Learning,” *Front Artif Intell*, vol. 4, Jun. 2021, doi: 10.3389/frai.2021.673527.

[32] Fu and C. Tantithamthavorn, “LineVul: A Transformer-based Line-Level Vulnerability Prediction,” *19th International Conference on Mining Software Repositories (MSR ’22), May 23â•fi24, 2022, Pittsburgh, PA, USA*, vol. 1, 2022, doi: 10.1145/3524842.

[33] Sunday Adeola Oladosu, Adebimpe Bolatito Ige, Christian Chukwuemeka Ike, Peter Adeyemo Adepoju, Olukunle Oladipupo Amoo, and Adeoye Idowu Afolabi, “Next-generation network security: conceptualizing a Unified, AI-Powered Security Architecture for Cloud-Native and On-Premise Environments,” *International Journal of Science and Technology Research Archive*, vol. 3, no. 2, pp. 270–280, Dec. 2022, doi: 10.53771/ijstra.2022.3.2.0143.

[34] Adebunmi Okechukwu Adewusi, Njideka Rita Chiekezie, and Nsisong Louis Eyo-Udo, “The role of AI in enhancing cybersecurity for smart farms,” *World Journal of Advanced Research and Reviews*, vol. 15, no. 3, pp. 501–512, Sep. 2022, doi: 10.30574/wjarr.2022.15.3.0889.

[35] C. I. Kithulgoda, R. Vaithianathan, and D. P. Culhane, “Predictive Risk Modeling to Identify Homeless Clients at Risk for Prioritizing Services using Routinely Collected Data,” *J Technol Hum Serv*, vol. 40, no. 2, pp. 134–156, 2022, doi: 10.1080/15228835.2022.2042461.

[36] Bharat. Rao, Balaji. Krishnapuram, A. . Tomkins, and Qiang. Yang, *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining : Washington, DC, USA, July 25-28, 2010*. Association for Computing Machinery, 2010.

[37] C. Sabottke, O. Suciu, T. Dumitraş, and T. Dumitras, *Vulnerability Disclosure in the Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits*. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/sabottke

[38] J. Jacobs, S. Romanosky, B. Edwards, I. Adjerid, and M. Roytman, “Exploit Prediction Scoring System (EPSS),” *Digital Threats: Research and Practice*, vol. 2, no. 3, Jun. 2021, doi: 10.1145/3436242.

[39] Y. Dong, W. Guo, Y. Chen, X. Xing, Y. Zhang, and G. Wang, “Towards the Detection of Inconsistencies in Public Security Vulnerability Reports.” [Online]. Available: https://github.com/pinkymm/inconsistency_detection

[40] Abisoye and J. I. Akerele, “A High-Impact Data-Driven Decision-Making Model for Integrating Cutting-Edge Cybersecurity Strategies into Public Policy, Governance, and Organizational Frameworks,” *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 2, no. 1, pp. 702–716, 2021, doi: 10.54660/.ijmrge.2021.2.1.702-716.

[41] L. Romeo and E. Frontoni, “A Unified Hierarchical XGBoost model for classifying priorities for COVID-19 vaccination campaign,” *Pattern Recognit*, vol. 121, Jan. 2022, doi: 10.1016/j.patcog.2021.108197.

[42] A. Ali, Y. Hafeez, S. Hussain, and S. Yang, “Role of Requirement Prioritization Technique to Improve the Quality of Highly-Configurable Systems,” *IEEE Access*, vol. 8, pp. 27549–27573, 2020, doi: 10.1109/ACCESS.2020.2971382.

[43] A. Bagheri and P. Hegedűs, “Application of Advanced AI Methods for Precise Vulnerability Detection.”

[44] K. Bennouk, D. Mahouachi, N. Ait Aali, Y. El Bouzekri El Idrissi, B. Sebai, and A. Z. Faroukhi, “Dynamic Data Updates and Weight Optimization for Predicting Vulnerability Exploitability,” *IEEE Access*, vol. 13, pp. 65266–65284, 2025, doi: 10.1109/ACCESS.2025.3558990.

[45] A. Mehrzad, M. Darmiani, Y. Mousavi, M. Shafie-Khah, and M. Aghamohammadi, "A Review on Data-Driven Security Assessment of Power Systems: Trends and Applications of Artificial Intelligence," 2023, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2023.3299208.

[46] M. I. Khan, "Managing Threats In Cloud Computing: A Cybersecurity Risk Mitigation Framework," *international journal of advanced research in computer science*, vol. 16, no. 5, pp. 37–43, Oct. 2025, doi: 10.26483/ijarcs.v15i5.7347.

[47] J. Dąbrowski, E. Letier, A. Perini, and A. Susi, "Analysing app reviews for software engineering: a systematic literature review," *Empir Softw Eng*, vol. 27, no. 2, Mar. 2022, doi: 10.1007/s10664-021-10065-7.