GRADIVA

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

Artificial Intelligence-Driven Dynamic Cyber Risk Assessment Framework for Real-Time Organizational Security Management

Okeke, Ogochukwu C. [1], Mgbeafulike, Ike J. [2], Nkechi, Oji. [3], Ajonuma Michael E. [4], Okonkwo Kinsley C. [5], Okafor Chukwujekwu J.[6] & Ebere Uzoka Chidi[7]

1,2.Department of Computer Science, Faculty of Physical Sciences,
Chukwuemeka Odumegwu Ojukwu University, Uli, Anambra State.
3.Department of Cyber Security, School of Information and Communication Technology,
Federal University of Technology, Owerri. Nigeria.
4.Federal Cooperative College, Oji, Enugu State Nigeria.
5.Computer Science Education Department, Federal College of Education (Tech),
Umunze, Anambra State, Nigeria.
6.Department of Electrical Electronics Engineering, Enugu State University of Science and Technology,
Agbani, Enugu State.
7.African Centre of Excellence for Sustainable Power and Energy Development, Department of Control and Instrumentation Engineering, University of Nigeria Nsukka, Enugu, Nigeria.
7.State University of Medical Science, Oba, Nsukka, Enugu State, Nigeria.
7.Gregory University, Uturu, Abia State, Nigeria.
Email: [1]co.okeke@coou.edu.ng, [2]ij.mgbeafulike@coou.edu.ng, [3]nkechioji2014@gmail.com,
[4]ajonumamicheal@gmail.com, [5]bkingsley.okonkwo@fcetumunze.edu.ng,
[6]c4okafor4@gmail.com, [7]steverolans@gmail.com

Abstract

The increasingly complex nature of vulnerabilities in information technology systems has made effective risk assessment a critical challenge for enterprise organizations. From the literature reviewed, conventional solutions did not integrate risk identification, evaluation, and prioritization as a single pipeline for adaptive risk assessment. To this end, the aim of this paper is an artificial intelligence-driven dynamic cyber risk assessment framework for real-time organization security management. The methodology used is quantitative. Vulnerability data were collected from the 2026 National Vulnerability Database (NVD), pre-processed, and balanced into four severity classes: Low, Medium, High, and Critical. Four machine learning models, namely Random Forest (RF), Feedforward Neural Network (FFNN), K-Nearest Neighbor (KNN), and Support Vector Machine (SVM), were trained and compared to identify the best risk identification model. This was integrated with a risk evaluation and prioritization model to create the adaptive risk assessment framework. The metrics for performance evaluation are accuracy, precision, recall, F1-score, confusion matrices, and Receiver Operating Characteristic (ROC) curve analysis. The experimental results demonstrate that all models achieved high predictive performance, with the RF classifier recording the best accuracy of 98.1%, FFNN reported 97.1%, KNN reported 95.3%, and SVM reported 92.2%. To demonstrate practical applicability, the trained models were integrated into an adaptive risk assessment software prototype capable of automatically classifying vulnerabilities, evaluating and prioritizing cybersecurity risks using Python programming language and Replit cloud-based integrated development environment. Practical validation using real 2026 CVE records demonstrated the framework's capability to accurately classify different classes of vulnerabilities and evaluate and prioritize cybersecurity risks.

Keywords: *Cybersecurity Risk Assessment, Machine Learning, Vulnerability Severity Prediction, National Vulnerability Database, CVE, Risk Prioritization.*

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

1. INTRODUCTION

In an increasingly connected world, where people, governments, and corporate organizations are heavily dependent on Digital Infrastructure (DGI), the need for reliable cybersecurity architecture has never been more critical. This is because, as our reliance on digital technologies increases, the frequency, scale, and sophistication of cyber-attacks have also increased effective individuals and organizations in both the public and private sectors. These cyber-attacks can take various forms, which include insider attacks, ransomware, malware, denial of service, persistent threats, and phishing, to exploit vulnerabilities inherent in DGI and compromise sensitive information (Kaloudi and Jingyue, 2020).

In recent years, the complexity of cyber-attacks has increased consistently, due to advancements in science and technologies, resulting in more dynamic threats, adversarial attacks, and novel threat features, thus presenting a major problem to cybersecurity experts (de Azambuja et al., 2023). While traditional security measures such as intrusion detection systems, , they lack the capacity for adaptive security capabilities due to the dynamic and complex nature of present data threat vectors, this necessitating the need for adaptive techniques for cybersecurity through Risk Assessment (RA) and management (Melaku, 2023).

According to the National Institute of Standards and Technology (NIST SP 800-160) and the International Standards Organization (ISO-73:2009), Risk assessment is an overall process of identifying, analyzing, and evaluating risk in an organization during the operation of an information system (Cheimonidi et al., 2023). The purpose of Risk assessment is to identify cyber-attacks, insider threats, and vulnerabilities, classify assets in organizations according to their criticality, and implement security control measures.

Traditional standardized Risk assessment methods such as NIST and ISO provide different frameworks (ISO 27005, ISO 27001, ISO 27006, and NIST SP-800-37) to facilitate risk management in an organization (Diamantopoulou et al., 2020). These standards are structures that offer holistic integration of risk management and cybersecurity activities as a foundation for a robust environment. They face several challenges due to the rapid changes in threat landscapes and emerging new vulnerabilities. In addition, Cheimonidi et al. (2023) posit that these standards cannot maintain the security posture of an organization to the level required because they cannot adapt to the dynamic environment in which present-day organizations operate, and as a result, organizations are increasingly facing malicious actions from diverse sources, which present the need for an Adaptive Assessment (ARA) model for risk management (Sanchez et al., 2023).

ARA is the continued tracking, identification, and classification of risk in an organization's operations (Cheimonidis and Rantos, 2023). Adaptive risk assessment is vital due to the constant changes in threat landscapes, inspired by new vulnerabilities that are emerging regularly. The need for ARA allows organizations to adapt to changing vulnerabilities and threat circumstances through continued monitoring and detection, prioritize emerging risks in real-time, and adjust security measures in response to evolving challenges, thus providing a proactive solution to detect potential risks and protect systems, data, and assets from cyber threats.

In recent years, artificial intelligence (AI), specifically machine learning (ML) algorithms, has been applied for RA (Hedge and Rokseth, 2020). ML is a type of AI that can learn from data and solve classification and regression problems. The data characterize the network's behaviour during vulnerability and are collected to train the ML algorithm to

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

generate RA models. For instance, Kassem (2021) applied several ML algorithms, such as XGBoost, Random Forest (RF), K-Nearest Neighbor (KNN), and Decision Tree (DT), and trained them with 6,000 entries of dangerous URL features to generate an intelligent host-based intrusion detection system for RA. In another study, Rajawat et al. (2023) applied quantum ML to develop a Risk assessment model for medical Internet of Things devices, while Sakthi et al. (2023) trained a Deep Neural Network (DNN) and Support Vector Machine (SVM) as autoencoders with CICIDS 2017 and developed an RA model for zero-day attack vulnerability detection.

Overall, while these studies have made significant contributions to the management of risk in organizations, there is a need for an RA model in cybersecurity that considers risk as a multi-faceted factor. Such a model should incorporate strategic risks that can impact an organization's objectives, operational risks arising from people, processes, and systems, financial risks related to performance and reporting, compliance risks associated with regulations, technological risks related to information systems, third-party risks introduced through external relationships, human factors such as employee behaviour, and the interdependencies and cascading effects of these diverse risk elements. Therefore, this paper proposes adaptive cybersecurity risk management (assessment) using artificial intelligence. This will be achieved using data from the Common Vulnerability and Exposure database, which models the dynamic nature of cybersecurity risk in its entirety, and then training a suitable machine learning algorithm to generate a model for holistic risk analysis.

1.2 Research Questions

1) How can an adaptive machine learning framework be developed to automatically identify, evaluate, and prioritize cybersecurity vulnerabilities using data from the National Vulnerability Database (NVD)?
2) How do classical machine learning algorithms perform in predicting vulnerability severity across the Low, Medium, High, and Critical risk categories?
3) How effective is the developed adaptive risk assessment software in accurately processing real-world CVE records and providing automated vulnerability classification and risk prioritization?

1.3 The contribution of the study

1) Development of a data-driven cybersecurity risk identification framework that continuously processes multiple organizational risk indicators in real-time
2) A comparative machine learning-based risk prediction model that systematically trains and evaluates multiple algorithms (such as Random Forest, Feedforward Neural Network, K-Nearest Neighbour, and Support Vector Machine) on organizational cybersecurity datasets to identify the optimal model for accurate real-time dynamic risk identification.
3) Present an intelligent risk prioritization framework that automatically ranks risks based on predicted severity, potential business impact, and exploitability, enabling prioritized response actions and more efficient allocation of security resources.
4) Implemented and validated a software prototype using real 2026 CVE records, demonstrating the framework's applicability to practical cybersecurity risk management.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

2. REVIEW OF RELATED WORKS

The reviewed literature indicates that cybersecurity risk assessment has evolved from conventional rule-based and probabilistic approaches toward artificial intelligence (AI), machine learning (ML), and hybrid intelligent models. Existing studies can be broadly grouped into risk propagation and vulnerability assessment models, machine learning-based risk prediction models, deep learning and hybrid intelligent approaches, adversarial and emerging AI techniques, and survey and review studies.

2.1 Risk Propagation and Vulnerability Assessment Models

Several studies focused on modelling cyber risk propagation and vulnerability analysis. Zhang et al. (2024) proposed a risk propagation assessment model that enhanced Zero Trust Network responses against Advanced Persistent Threats (APTs) by improving threat anticipation. Similarly, Xiong and Wu (2020) developed a vulnerability threat assessment model that reduced Expected Load Loss and Chain Failure Probability through hardware self-testing. Arat and Akleylet (2023) integrated CVSS, CVE, NVD, and a modified Depth First Search algorithm to analyse attack paths in IoT environments, successfully identifying vulnerable attack routes. Likewise, Pangsuban et al. (2020) developed a real-time intrusion detection and risk matrix using the CICIDS2017 dataset. Although these approaches effectively analyse known vulnerabilities, they largely depend on predefined attack information and offer limited adaptability to emerging cyber threats.

2.2 Machine Learning-Based Cybersecurity Risk Assessment

Machine learning has become one of the dominant approaches for cybersecurity risk assessment. Kalinin et al. (2021) employed a three-layer perceptron neural network, achieving prediction accuracies between 98% and 99% for smart city cybersecurity assessment. Compagnoni (2022) combined the FAIR and MAGIC frameworks with machine learning to obtain 78.6% accuracy in organizational cyber risk assessment. Huang et al. (2021) compared Random Forest, Support Vector Machine, and AdaBoost, reporting AdaBoost as the best-performing algorithm with 90.1% accuracy. Similarly, Sheet and Ibraheem (2023) evaluated LGBM, AdaBoost, CatBoost, and Multi-Layer Perceptron, where MLP achieved the highest accuracy of 99.45%. Kassem (2021) compared several ML algorithms for host-based intrusion detection and found XGBoost to produce the highest accuracy of 98.43%. These findings demonstrate that supervised machine learning algorithms consistently achieve high predictive performance for cybersecurity applications.

2.3 Emerging AI Techniques and Advanced Threat Detection

Recent studies have increasingly investigated advanced AI methods for detecting sophisticated cyber threats. Sakthi et al. (2023) combined Support Vector Machine with Autoencoders for zero-day vulnerability detection using anomaly-based learning. Bitton et al. (2021) examined Adversarial Machine Learning (AML) and developed an Analytic Hierarchy Process (AHP)-based framework for systematically evaluating attacks against machine learning systems. Raju et al. (2019) further investigated the vulnerability of machine learning models themselves under adversarial attacks, demonstrating increased false positive and false negative rates. Rajawat et al. (2023) explored Quantum Machine Learning (QML) for Internet of Medical Things (IoMT) cybersecurity and reported outstanding performance with 99.34% accuracy and precision. These studies demonstrate the growing interest in securing AI systems while exploiting emerging computational paradigms for cybersecurity.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

2.4 Survey and Review Studies

Several studies provided comprehensive reviews of AI applications in cybersecurity rather than proposing new predictive models. Radanliev et al. (2020) emphasized ethical and explainable AI integration for IoT cybersecurity, highlighting the need for transparent decision-making.

Shetty and Kant (2021) reviewed various AI and data-driven cybersecurity approaches but concluded that no single machine learning algorithm consistently outperforms others across different cybersecurity problems. Wei et al. (2023) conducted a bibliometric analysis of industrial risk assessment and identified Industry 4.0 technologies as a major future research direction.

Similarly, Hedge and Rokseth (2020) presented a broad review of ANN- and SVM-based risk assessment methods, guiding cross-sector adoption of machine learning techniques. While these review studies provide valuable insights into research trends, they do not develop practical risk assessment frameworks or experimentally validate proposed concepts. Table 1 presents a summary of the literature review.

Table 1: Summary of related works

Author(s)	Method	Key Strength	Major Weakness	Reported Impact
Zhang et al. (2024)	Risk propagation assessment model	Enhances zero-trust network threat response	Lack of implementation & contextualization	Improved anticipation and countering of APTs
Xiong and Wu (2020)	Vulnerability threat assessment model	Quantitative risk reduction analysis	Limited generalizability	Reduced expected load loss and chain failure probability
Arat and Akleylet (2023)	CVSS, CVE, NVD + modified DFS	Attack path analysis in IoT systems	Scope limited to prevalent attacks	Identified attack paths in 32% and 11% of pathways
Kalinin et al. (2021)	Three-layer perceptron neural network	High accuracy in smart city contexts	Lack of comprehensive evaluation metrics	Accuracy: 98–99%
Compagnoni (2022)	Machine Learning (FAIR + MAGIC)	Objective risk assessment based on maturity	Lack of contextualization	Accuracy: 78.6%
Radanliev et al. (2020)	AI & ML in IoT	Ethical AI integration focus	Lack of implementation & contextualization	Emphasis on human-understandable AI
Jules and Danielle (2022)	Random Forest	Fat-tail risk phenomenon analysis	No qualitative analysis & long-term eval.	Insights into cyber-insurance data scarcity
Bitton et al. (2021)	Adversarial ML + AHP	Comprehensive threat modeling	Lack of qualitative & long-term analysis	Systematic scoring of ML system attacks

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

Sheet and Ibraheem (2023)	LGBM, AdaBoost, CatBoost, MLP	High-performing ensemble models	Lack of model evaluation metrics	Accuracies up to 99.45% (MLP)
Huang et al. (2021)	RF, SVM, AdaBoost	Comparative ML performance	-	AdaBoost best (90.1% accuracy)
Wei et al. (2023)	Bibliometric mapping	Trend analysis in industrial risk assessment	Lack of qualitative depth	Highlights Industry 4.0 integration needs
Kucukkaya (2021)	SVM + SMOTE	Graph-based insider threat features	Lack of transparency in metrics	Accuracy: 89%, AUC: 0.882
Shetty and Kant (2021)	AI + Data-driven models	Broad conceptualization of ML in cybersecurity	No single best algorithm identified	Survey of ML applications
Pangsuban et al. (2020)	ML on CICIDS2017 dataset	Real-time risk matrix	ML model not clearly specified	Real-time intrusion detection & risk assessment
Sakthi et al. (2023)	SVM + Autoencoder	Zero-day vulnerability detection	Limited empirical validation	Threshold-based anomaly detection
Kassem (2021)	XGBoost, RF, AdaBoost, etc.	Host-based intrusion detection	Lack of transparency in metrics	XGBoost highest accuracy (98.43%)
Rajawat et al. (2023)	Quantum ML (QML) in IoMT	Exploration of quantum approaches	Lack of transparency in metrics	Accuracy & Precision: 0.9934
Hedge and Rokseth (2020)	ANN, SVM (Literature review)	Comprehensive ML risk assessment survey	Lack of qualitative analysis	Guidance for cross-sector ML applications

Research Gap:

From the reviewed papers, summarized in Table 1, existing studies focus on static risk prediction, vulnerability assessment, or intrusion detection rather than continuous dynamic cybersecurity risk assessment.

In addition, existing models rarely integrate the complete risk assessment process comprising risk identification, machine learning-based risk prediction, risk evaluation, and risk prioritization within a single intelligent framework.

Consequently, there is a need for an AI-based dynamic cybersecurity risk assessment framework capable of continuously monitoring organizational risk, accurately predicting emerging cyber risks, dynamically evaluating their severity, and intelligently prioritizing them to support timely and effective risk management.

3. METHODOLOGY

The methodology used for this study is quantitative. The proposed system is made of three main sections which are the risk identification model, risk evaluation model, and risk prioritization model. Figure 1 presents the proposed system flow chart.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

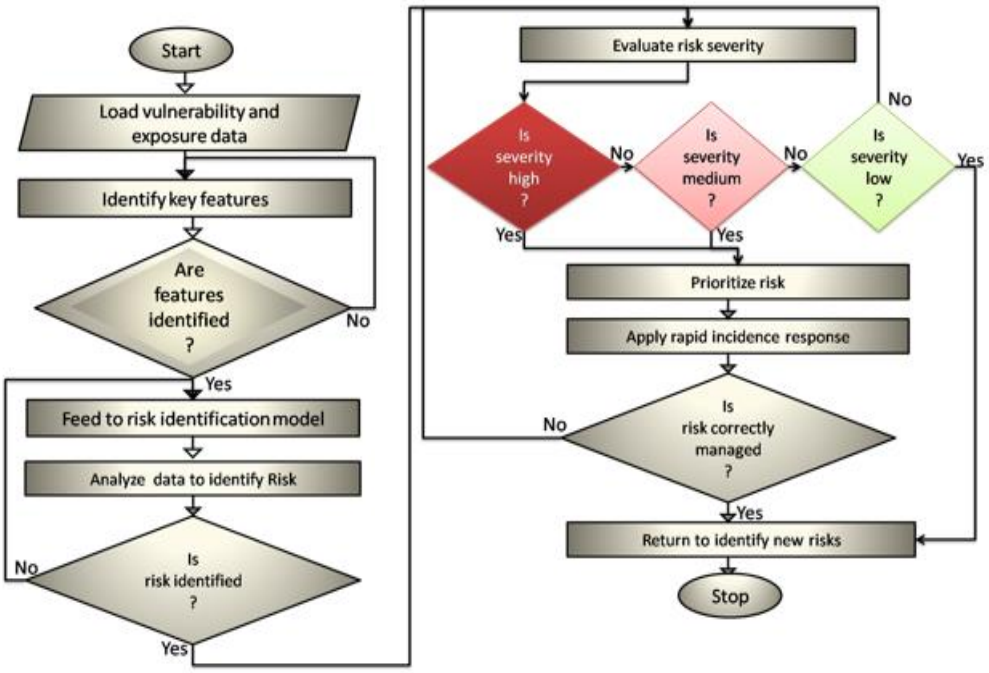


Figure 1: Flow chart of the Proposed AI-Driven Dynamic Cyber Risk Assessment Framework

Figure 1 illustrates the workflow of the proposed AI-driven Dynamic Cyber Risk Assessment Framework, which is designed to provide continuous identification, evaluation, and prioritization of cybersecurity risks within an organization. The process begins with the loading of vulnerability and exposure data collected from various organizational sources, such as vulnerability scanners, network monitoring systems, security logs, asset inventories, and threat intelligence databases. These data represent the current security posture of the organization and serve as the primary input to the framework. After the data are loaded, the framework performs feature identification, where the most relevant cybersecurity attributes are extracted from the collected data. These features include vulnerability severity scores, system configurations, network activities, asset criticality, user behaviour, and known threat indicators. A validation step then verifies whether sufficient and meaningful features have been successfully identified. If the extracted features are inadequate, the framework returns to the feature extraction stage for further processing until suitable features are obtained.

Once the relevant features have been identified, they are supplied to the AI-based risk identification model. At this stage, the trained machine learning model analyses the processed cybersecurity data to determine whether potential risks exist within the organizational environment. If no significant risk is detected, the system continues monitoring newly generated cybersecurity data. However, when a potential cybersecurity risk is identified, the process advances to the risk evaluation stage. During this phase, the framework assesses the severity of each identified risk based on the prediction generated by the machine learning model. The severity is categorized into three levels: high, medium, or low. This classification enables security administrators to understand the urgency of each identified threat and determine the appropriate response strategy. Following severity evaluation, the framework performs risk prioritization, where risks are ranked according to their severity level and potential impact on organizational operations. High-severity risks receive the highest priority,

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

followed by medium- and low-severity risks. This ensures that limited cybersecurity resources are allocated to the most critical threats first.

After prioritization, the framework initiates a rapid incident response process. Appropriate mitigation measures, such as vulnerability patching, access restriction, malware isolation, system reconfiguration, or security policy enforcement, are applied to reduce the identified cybersecurity risk and prevent further exploitation. The framework then evaluates whether the identified risk has been successfully managed. If the mitigation process is unsuccessful, additional response actions are initiated until the risk is adequately controlled. Once the risk has been effectively mitigated, the framework returns to the monitoring stage to identify newly emerging risks, thereby creating a continuous assessment cycle.

3.1 Data Collection

The data used for this paper is secondary data called the Common Vulnerability and Exposure (CVE) database. The data source is the National Vulnerability Database (NVD) repository, which provides an update feed of CVE entries in JSON format and was converted to CSV in Python. A total of 5,677 vulnerability records published during the 2026 reporting period were retrieved.

The dataset comprised 27 attributes, including CVE identifiers, publication and modification dates, source identifiers, vulnerability descriptions, affected products, CVSS v2, v3.0, v3.1, and v4.0 metrics, CWE classifications, vulnerability status, software configurations, references, and CISA Known Exploited Vulnerability (KEV) information.

These attributes collectively provide both technical and contextual information required for vulnerability assessment and cybersecurity risk analysis. While there are several other CVE database sources available, like MITRE, for instance, Benetis et al. (2024) revealed that NVD is the most detailed for information security risk analysis.

3.2 Technique for Data Analysis

Data analysis was carried out in this study using an explorative technique. This was applied to gain an understanding of the data patterns, improve the data quality, and ensure the data is ready to train a machine learning algorithm. The process involves the transformation of key data features into meaningful which supports predictive modeling of adaptive risk in cyber security environment.

The steps began with the importation of the dataset, cleaning the data for missing values, and also removing duplicated values using the mean imputation technique (Manjunathan et al., 2024). Data profiling was applied to understand data distribution, while multi-variable analysis was applied to detect relationships between features.

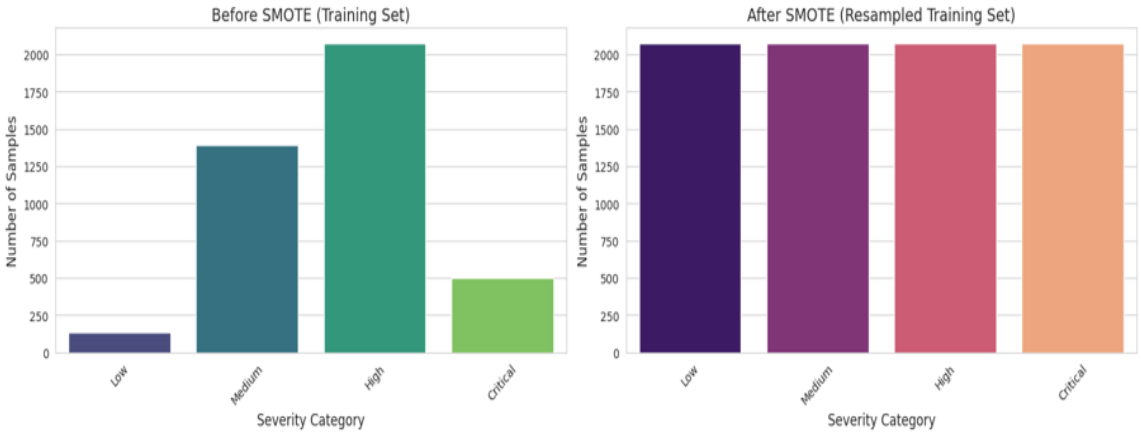
3.3 Data Processing

The data processing was done using mean imputation to fix missing values, feature elimination to reduce duplicate values, then categorical encoding, feature selection, and the Synthetic Majority Over-sampling Technique (SMOTE), respectively.

The feature selection was applied to identify the most important features in the dataset, which reduces model risk (Narayanan et al, 2020). This was achieved using the analysis variance approach which computes the fitness of each feature and then select the best fit multi variables are the attributes of interest.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

SMOTE was applied to address issues of bias in the data class (Fakhri, 2022). This was achieved through the artificial generation of an under-sampled data class to balance the dataset. Figure 2 presents the results before and after SMOTE.



(a) Imbalanced classes without SMOTE **(b) Balanced classes with SMOTE**

Figure 2: Result of Class Distribution before and After the Application of SMOTE

Figure 2 presents the class distribution of the results. Figure (a) shows that the original dataset has imbalanced classes with a total of 5131 records spread across 2073 records for high severity score, 1394 records for medium, 502 for critical, and 135 for low severity score. When SMOTE was applied, the classes were balanced to 2073 records for each class, and a total of 8292 records of vulnerabilities.

3.4 Risk Identification

The method involved the application of a machine learning algorithm on the processed data and training using an optimization technique to generate the model for risk identification, which is the first part of the adaptive risk assessment process. Figure 3 presents the risk identification process diagram.

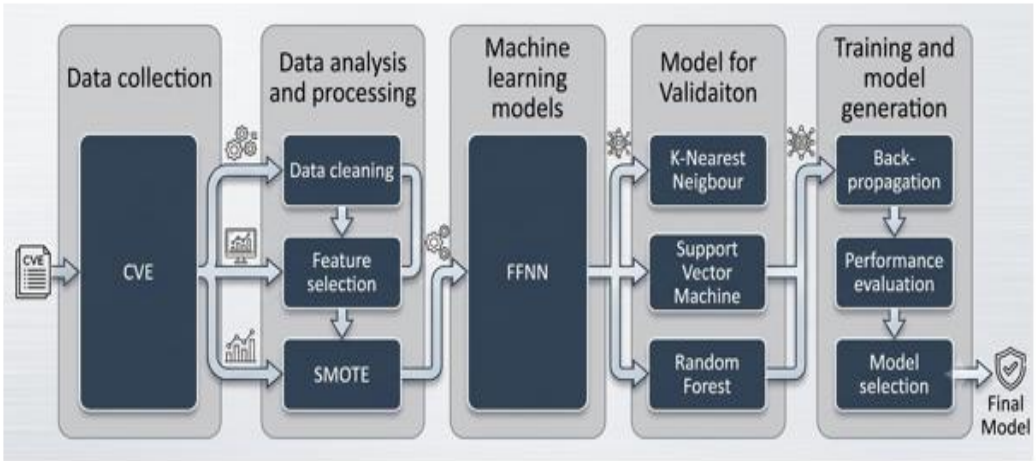


Figure 3: Block Diagram of the Risk Identification Process

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

3.5 Machine Learning Technique

The machine learning technique adopted is the feed-forward neural network. From the literature reviewed, while several algorithms have been trained for risk identification, the application of neural network algorithms has consistently stood out as the best when compared with the results considering accuracy of risk identification, precision, and recall. Based on this evidence, this work applied the FFNN model, and the type of FFNN used is the multi-layered neural network.

i.Multi-Layered Neural Network

FFNN can learn from input data and solve classification problems. It is made of neurons that contain weights (W) and biases (B)(Nieto et al., 2018). These neurons are triggered with the tansig activation function since risk identification is a multi-classification problem. The FFNN with multiple hidden layers is defined for l=1, 2, 3….L hidden layers as equation 1.

$$z^{(l)} = W^{l} a^{(l-1)} + b^{l} \quad (1)$$

Where$a^{l} = f^{l}(z^{l})$. The final output Y is given as equation 2.

$$Y = a^{L} = f^{L} W^{L} a^{(L-1)} + b^{L} \quad (2)$$

3.5.1 Other Machine Learning Techniques Also Trained In the Study

While the main ML used for this work is the multi-layered neural network, other machine learning algorithms such as support vector machine, KNN, and random forest were also trained and then comparatively analyzed with the neural network-based model for risk identification to select the most suitable model for development of the adaptive risk assessment model.

i. Support vector machine

The SVM is a supervised machine learning algorithm which operated by determining the optimal hyperplane which separated different data points. First, it identified all the features of the CVE data after a kernel function was applied to transform it into high-dimensional space. Then, a hyperplane is applied to create a decision boundary that separated the support vectors into distinct classes. A kernel function is used to achieve this separation process, and then class with the hyper (Nieto et al., 2018).

ii. K-Nearest Neighbor

KNN classifies new data points by identifying the closest points in the data and then assigning the most common class among them. The model applies the Euclidean-distance model to compute the relationship between new data and then trains the data and then predicts the decision based on the majority of the closest data points. With the number of data points in the CVE database designed as N, the probability p_i that every sample i is the nearest neighbor is expressed as equation 3;

$$p_i = \sum_{(j \in K_i)}^{N} p_{ij} \quad (3)$$

Where Ki is the set of points that fall within the same class as sample i, $p_{ij}$is the softmax over the Euclidean distance within the space.

iii. Random Forest

Random forest is an ensemble learning technique used for classification and regression tasks. It is made of several decision trees trained and then applies an average voting approach to make the final classification decision.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

In the context of this work, the attributes of the CVE dataset were applied to create different decision trees, which were randomly split and trained to vote for different output classes used to compute the final decision class through an average voting technique. The overall votes are averaged to decide the risk severity in the input data.

3.5.2 Training of the Machine Learning Algorithms

The machine learning algorithms were implemented in Python using the Google Colab environment. The CVE dataset was converted from JSON to CSV format, pre-processed, and partitioned into 80% training, 10% validation, and 10% testing.

The FFNN was trained using the backpropagation algorithm with the Adam optimizer, a learning rate of 0.001, 100 epochs, a batch size of 32, and the ReLU activation function. The SVM employed the Radial Basis Function (RBF) kernel with a regularization parameter (C) of 1.0 and gamma = 'scale'. The RF classifier was trained using 100 decision trees, the Gini impurity criterion, and bootstrap aggregation (bagging).

The KNN classifier used k = 5, the Euclidean distance metric, and uniform distance weighting for classification. Model performance was evaluated using the validation and testing datasets based on accuracy, precision, recall, F1-score, and Area under the Curve (AUC), after which the best-performing model was selected for deployment. The machine learning-based adaptive risk identification algorithm is presented as;

Algorithm 1: Risk Identification

1. Start
2. Input CVE data
3. Feature encoding
4. Load trained machine learning model %% selected from the algorithms trained
5. Analyze input data
6. If risk is detected
7. Classify severity score
8. Return output severity score as output
9. Else
10. Return to step 2
11. End if
12. End

3.6 Risk Evaluation Model

The risk evaluation model was applied in this work for the determination of severity and potential impact of vulnerability. Several studies in literature (Shi et al., 2022;; Shahid and Debar, 2021; Costa et al., 2022) commonly applied the Common Vulnerability Scoring System (CVSS) approach for the evaluation of risk, however this approach focused on the severity score as a univariable metric for the analysis of impact and quantification of risk, which is good but lack critical parameters consideration of factors such as attack vector, known exploit, threat indicator factors which are necessary to a more reliable risk evaluation process.

This work proposed a multi-layered risk matrix approach that integrates CVSS, likelihood score, impact score, and maps out a matrix for evaluation of risk. Figure 4 presents the risk evaluation flow chart.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

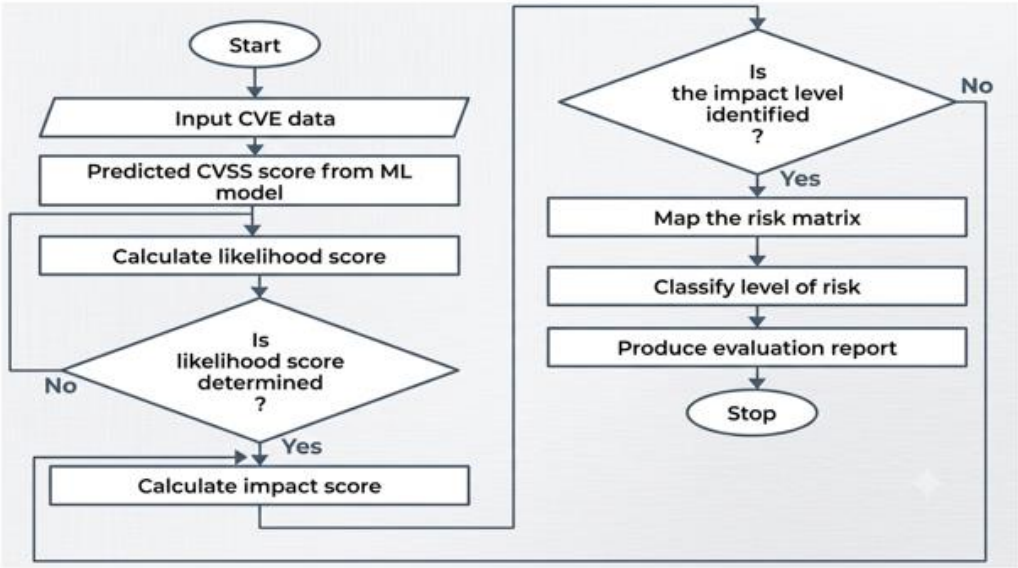


Figure 4: Flowchart of the Risk Evaluation

The inputs of CVE are passed through the trained ML algorithm to classify the CVSS score. This score is used as input to determine the likelihood of attack and also the impact score. These scores are used to build the risk matrix to evaluate risk. The CVSS score prediction by the ML model is rated according to the National Vulnerability Database (NVD) quantitative severity rating version 2.0 (NVD, 2025) and is reported in Table 3. These scores are determined considering the base score, which describes the considered attack vector, attack complexity, and overall impacts. The temporal score reflects the characteristics of vulnerability over time. The environmental score involves elements of computer network security.

Table 3: Common Vulnerability Severity Rating (Nvd, 2025)

Severity	Score	Impact
Low	0.0-1.5	Low
Very Low	1.6-3.9	Low
Medium	4.0-6.9	Medium
High	7.0-8.0	High
Very high	9.0-10	Very high

To measure the likelihood that the CVSS score results in an exploit, equation 4 was applied;

$$\text{Likelihood} = \sum \frac{Frequencyofoccurenceofrisk * proabilityofriskoccurence}{Totalnumberofidentifiedrisk} \quad (4)$$

Where this impact score is determined with the likelihood matrix table, where impact score is rated from 1-10 in Table 4.

Table 4: Risk Evaluation Matrix

	The risk evaluation matrix			
LIKELIHOOD	RARE	VERY LOW	LOW	MEDIUM
	LIKELY	LOW	MEDIUM	HIGH
	CERTAIN	LOW	HIGH	VERY HIGH
		MINOR IMPACT	SIGNIFICANT	SEVERE
	Impact if it happens			

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

The risk evaluation was therefore determined using the relationship between likelihood of exploit and impact as in equation 5 (Dennis, 2023).

$$RE = \sum Likelihood * impact \quad (5)$$

This risk evaluation matrix was used to develop the risk evaluation algorithm.

Algorithm 2: Priority of risk level

```
# Step 1: Define a function to convert risk level to numeric priority
def risk_level_to_priority(risk_level)
Load output of algorithm 2
# Step 3: Define a dictionary to map risk levels to priority scores
Set priority mapping = {'very High':5, 'High': 4, 'MEDIUM': 3, 'LOW':2, 'Very Low'1}
return mapping.get(risk_level.upper(), 0) # 0 if unknown
Step 5: Define function to prioritize risks based on their level
def prioritize_risks(df):
# Add priority score column
df['Priority_Score'] = df['Risk_Level']. apply(risk_level_to_priority)
# Incidence response
For priority score == ['5']
Do → instant response
For priority score == ['4','3']
Do → rapid response
Else
For priority score == ['2', '1']
Do → schedule response
Return
End
```

3.7 Risk Prioritization

The risk prioritization transforms the risk evaluation output into a rating of priorities using a risk prioritization numbering approach. First, the risk evaluation level (Very High, High, Medium, Low, and Very Low) is ranked as shown in Table 5.

Table 5: Risk Level and Prioritization Distribution

Risk level	Priority score	Control
Very High	5	Instant response
High	4	Rapid response
Medium	3	Rapid response
Low	2	Schedule response
Very Low	1	Schedule response

3.8 System Implementation

The dynamic cybersecurity risk assessment framework was implemented using Python 3.11 in the Google Colab environment. The implementation was executed on a cloud-based runtime equipped with an Intel Xeon processor, NVIDIA Tesla T4 GPU (16 GB VRAM), and

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

approximately 12.7 GB RAM, running the Linux operating system. The implementation utilized the Scikit-learn, TensorFlow, Pandas, NumPy, and Matplotlib libraries for data preprocessing, machine learning model development, performance evaluation, and visualization.

The implementation consisted of three sequential modules: machine learning-based risk identification, risk evaluation, and risk prioritization. The CVE dataset, which contains vulnerability attributes such as vulnerability type, confidentiality impact, integrity impact, and availability impact, was pre-processed and used to train four supervised machine learning classifiers: FFNN, SVM, RF, and KNN.

The models were evaluated using accuracy, precision, recall, F1-score, and AUC-ROC serving as the performance metrics. The classifier with the highest predictive performance was selected as the risk identification model and integrated into the proposed framework to predict the severity of previously unseen vulnerabilities.

The predicted severity scores were subsequently mapped into Low, Medium, and High-risk categories and supplied to the risk evaluation module, where a likelihood-impact matrix was used to determine the corresponding qualitative risk level.

Finally, the risk prioritization module assigned numerical priority scores to the evaluated risks and ranked them in descending order of criticality, thereby generating a prioritized list of cybersecurity risks to support timely mitigation and informed decision-making.

4. RESULTS AND DISCUSSIONS

This section presents the results obtained during the dataset analysis, training, and evaluation of the machine learning models for vulnerability identification, risk evaluation, and risk prioritization. Figure 5 illustrates the distribution of vulnerability status in the 2026 NVD dataset.

The Deferred category contains the highest number of records (1,603), indicating that many vulnerabilities were postponed for further review and reprioritization. This is followed by Analyzed (1,381 records), showing that a substantial proportion of vulnerabilities have completed technical assessment, including severity scoring and impact evaluation.

The Modified category comprises 1,230 records, indicating that many CVEs were updated with revised severity scores, affected products, exploit information, and additional references.

In contrast, Awaiting Analysis (726 records) represents vulnerabilities pending detailed assessment, reflecting a moderate processing backlog, while Undergoing Analysis (212 records) and Received (153 records) correspond to vulnerabilities in the early stages of the evaluation process.

The Rejected category contains 38 records, indicating that only a small proportion of submissions were identified as invalid or duplicate entries. Overall, the dataset is dominated by Analyzed and well-documented vulnerabilities, demonstrating that it contains comprehensive and reliable information suitable for machine learning-based vulnerability severity prediction, exploitability assessment, and dynamic cybersecurity risk prioritization. The numeric feature correlation heatmap is presented in Figure 6.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

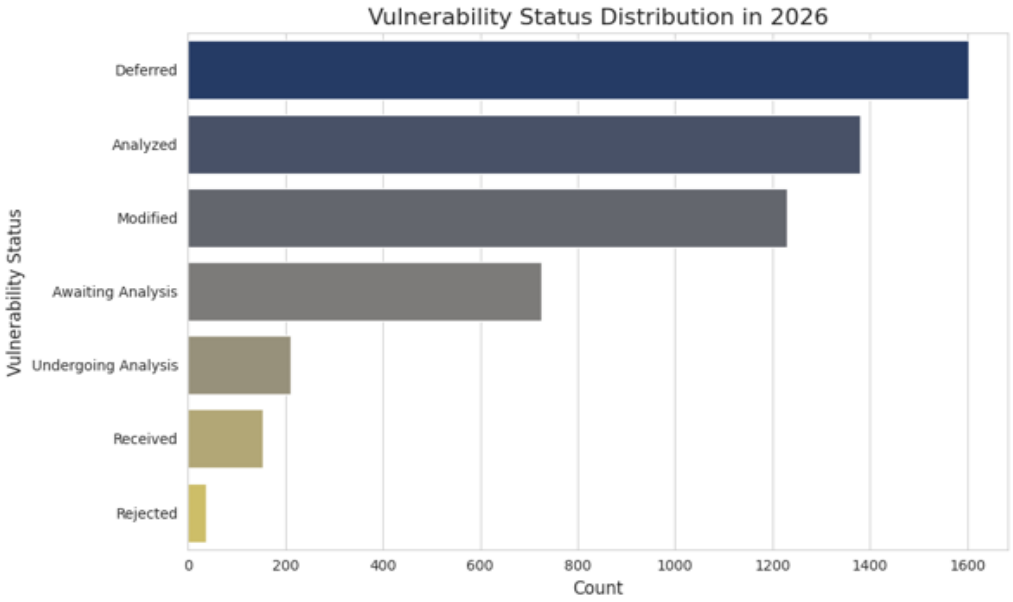


Figure 5: Vulnerability Status Distribution In 2026

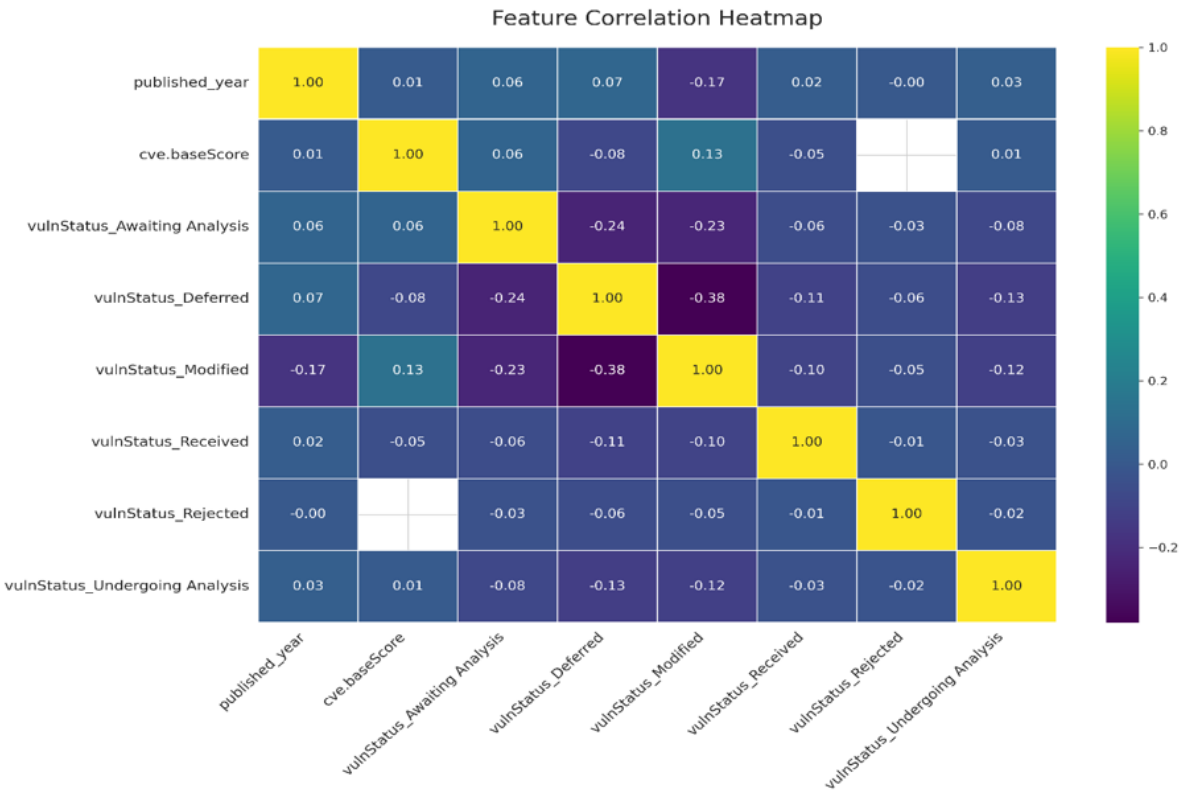


Figure 6: Correlation Heatmap

Figure 6 presents the correlation heatmap of the selected numerical and encoded categorical features used in the vulnerability dataset. The diagonal values of 1.00 indicate perfect self-correlation for each attribute, while the off-diagonal values reveal the relationships between different features. In the heatmap, it was observed that most feature pairs exhibit weak

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

correlations between -0.38 and 0.13, indicating minimal multicollinearity and suggesting that each feature contributes unique information to the predictive model. The strongest negative correlation is observed between vulnStatus_Deferred and vulnStatus_Modified (r = -0.38), implying that vulnerabilities classified as Deferred are less likely to simultaneously belong to the Modified category, as these statuses are mutually exclusive stages in the NVD workflow. Similarly, vulnStatus_Awaiting Analysis shows moderate negative correlations with vulnStatus_Deferred (r = -0.24) and vulnStatus_Modified (r = -0.23), reflecting the sequential transition of vulnerabilities from pending assessment to later processing stages. The cve.baseScore exhibits only weak positive relationships with vulnStatus_Modified (r = 0.13) and vulnStatus_Awaiting Analysis (r = 0.06), while showing weak negative correlations with vulnStatus_Deferred (r = -0.08) and vulnStatus_Received (r = -0.05). These results suggest that vulnerability severity has limited influence on processing status, indicating that workflow progression depends on additional operational and administrative factors beyond the CVSS score alone. Furthermore, the published_year variable demonstrates negligible correlations with all status variables, with the largest being a weak negative correlation with vulnStatus_Modified (r = -0.17), indicating that publication year has little effect on vulnerability status. The consistently low correlation values across all attributes confirm the absence of strong linear dependencies, reducing the risk of redundant features and making the dataset well suited for machine learning-based vulnerability severity prediction and dynamic cybersecurity risk assessment. Figure 7 presents the distribution of the CVS base scores.

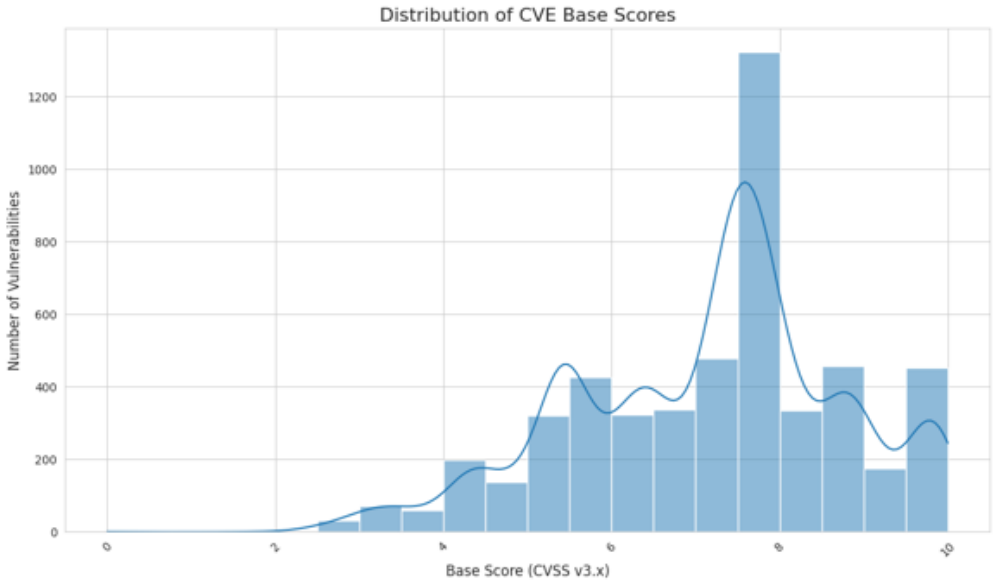


Figure 7: Distribution of CVE Base Score

Figure 6 shows the distribution of CVSS v3.x base scores for the vulnerabilities in the 2026 NVD dataset. The distribution is concentrated in the high-severity range (7.0–8.0), with the highest frequency occurring around a base score of 7.5, indicating that most recorded vulnerabilities pose significant security risks requiring timely mitigation. A substantial number of vulnerabilities also fall within the 8.0–10.0 range, representing high and critical severity vulnerabilities that could lead to severe impacts on confidentiality, integrity, and availability if exploited. In contrast, relatively few vulnerabilities have base scores below 5.0, suggesting that low-severity vulnerabilities constitute only a small proportion of the dataset. The Kernel Density Estimate (KDE) further confirms that the score distribution is left-skewed, with the

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

majority of observations clustered between 6.0 and 9.0. This distribution demonstrates that the dataset is dominated by moderate-to-high severity vulnerabilities, providing a balanced representation of realistic cybersecurity threats. Table 3 presents the top 10 vulnerability sources in January to July 2026.

Table 3: Top 10 Vulnerability Sources

Rank	Vulnerability Source Identifier	Number of CVEs
1	security-advisories@github.com	1,089
2	disclosure@vulncheck.com	715
3	secure@microsoft.com	593
4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	488
5	cve@mitre.org	193
6	security@wordfence.com	193
7	cna@vuldb.com	183
8	secalert@redhat.com	169
9	audit@patchstack.com	150
10	security@mozilla.org	118

Table 3 presents the ten leading vulnerability source identifiers responsible for reporting CVEs in the first half of 2026 NVD dataset. The results show that security-advisories@github.com contributed the highest number of vulnerability records (1,089), indicating that GitHub Security Advisories remains one of the most active sources of publicly disclosed software vulnerabilities, largely due to its extensive open-source ecosystem. This is followed by disclosure@vulncheck.com with 715 records and secure@microsoft.com with 593 records, reflecting the significant role of commercial vulnerability intelligence providers and major software vendors in vulnerability disclosure. The source identifier 416baaa9-dc9f-4396-8d5f-8c081fb06d67 contributed 488 vulnerabilities, suggesting that a registered CVE Numbering Authority (CNA) also plays a substantial role in CVE assignment. Other notable contributors include MITRE, Wordfence, VulDB, Red Hat, Patchstack, and Mozilla, each reporting between 118 and 193 vulnerabilities. The diversity of reporting organizations demonstrates that the dataset was compiled from multiple reputable sources covering open-source software, enterprise platforms, operating systems, web applications, and cybersecurity research. Consequently, the dataset provides broad coverage of vulnerability types and software ecosystems, making it suitable for developing robust machine learning models for vulnerability severity prediction and dynamic cybersecurity risk assessment.

4.1 Results of the Machine Learning Model Training

This section presents the results of the machine learning models (RF, KNN, FFNN, and SVM) training, testing, and validation. The performance was evaluated considering metrics such as accuracy, precision, recall, and F1-score. The accuracy measured the success of vulnerability identification across different classes of severity score. Precision is the positive prediction of severity score for vulnerability across different classes. Recall is the assurance of precision score, while F1-score measures the harmonic mean between precision and recall. Table 4 presents the training and testing results of the RF classifier.

Table 4: Random Forest Classification Performance

Class	Precision	Recall	F1-Score	Support
Low	0.99	0.98	0.99	207
Medium	0.98	0.98	0.98	207
High	0.98	0.98	0.98	207
Critical	0.98	0.98	0.98	207

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

Accuracy	0.9807			828
Macro Avg	0.981	0.981	0.981	828
Weighted Avg	0.981	0.981	0.981	828

The RF classifier in Table 4 achieved an overall accuracy of 98.1% in predictive capability for vulnerability severity classification. The model recorded a precision of 98.1%, indicating that the majority of vulnerabilities predicted for each severity class were correctly classified. Similarly, the recall of 98.1% shows that the classifier successfully identified almost all actual instances across the Low, Medium, High, and Critical classes. The corresponding F1-score of 98.1% confirms a strong balance between precision and recall, while the uniformly high performance across all classes, each containing 207 samples, indicates that the model generalized well without exhibiting bias toward any particular severity category. Table 5 presents the result of the FFNN training performance.

Table 5: Feedforward Neural Network Classification Performance

Class	Precision	Recall	F1-Score	Support
Low	0.98	0.97	0.97	207
Medium	0.97	0.97	0.97	207
High	0.97	0.98	0.98	207
Critical	0.98	0.97	0.97	207
Accuracy	0.9709			828
Macro Avg	0.975	0.975	0.975	828
Weighted Avg	0.975	0.975	0.975	828

The FFNN in Table 5 achieved an overall accuracy of 97.1%, indicating a high level of effectiveness in learning the nonlinear relationships among the vulnerability features. The model produced a macro-average precision, recall, and F1-score of 97.5%, reflecting consistent classification performance across all four severity categories. Class-level precision ranged from 97% to 98%, while recall values remained between 97% and 98%, demonstrating that the model accurately identified vulnerabilities with minimal false positives and false negatives. The balanced F1-scores of 97.5% further indicate that the network maintained stable classification performance throughout the dataset. Table 6 presents the KNN result after training.

Table 6: K-Nearest Neighbor Classification Performance

Class	Precision	Recall	F1-Score	Support
Low	0.96	0.96	0.96	207
Medium	0.95	0.96	0.95	207
High	0.94	0.96	0.95	207
Critical	0.97	0.95	0.96	207
Accuracy	0.9529			828
Macro Avg	0.955	0.956	0.955	828
Weighted Avg	0.955	0.955	0.955	828

The KNN classifier in Table 6 obtained an overall accuracy of 95.3%, demonstrating reliable performance in classifying vulnerability severity levels. The model achieved a macro-average precision of 95.5%, recall of 95.5%, and F1-score of 95.5%, indicating good predictive consistency across the four classes. The class-specific precision values ranged from 94% to 97%, while recall values varied between 95% and 96%, suggesting that most vulnerability instances were correctly identified. The corresponding F1-scores of 96% also remained consistently high, confirming that the classifier maintained a good balance between correctly identifying vulnerabilities and minimizing misclassification. Table 7 presents the SVM result.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

Table 7: Support Vector Machine (Svm) Classification Performance

Class	Precision	Recall	F1-Score	Support
Low	0.94	0.92	0.93	207
Medium	0.91	0.93	0.92	207
High	0.90	0.92	0.91	207
Critical	0.95	0.93	0.94	207
Accuracy	0.9215			828
Macro Avg	0.925	0.925	0.925	828
Weighted Avg	0.925	0.925	0.925	828

The SVM classifier in Table 7 achieved an accuracy of 92.2%, indicating satisfactory performance in multiclass vulnerability severity prediction. The model recorded a macro-average precision, recall, and F1-score of 92.5%, demonstrating that it correctly classified the majority of vulnerability instances across all severity categories.

Individual class precision ranged from 90% to 95%, while recall values varied between 92% and 93%, indicating reasonably balanced detection across the four classes. The corresponding F1-score of 92.5% confirms the model's capability to classify vulnerability severity effectively, although a moderate number of misclassifications remained across the dataset. Figure 8 presents the confusion matrix of the individual models.

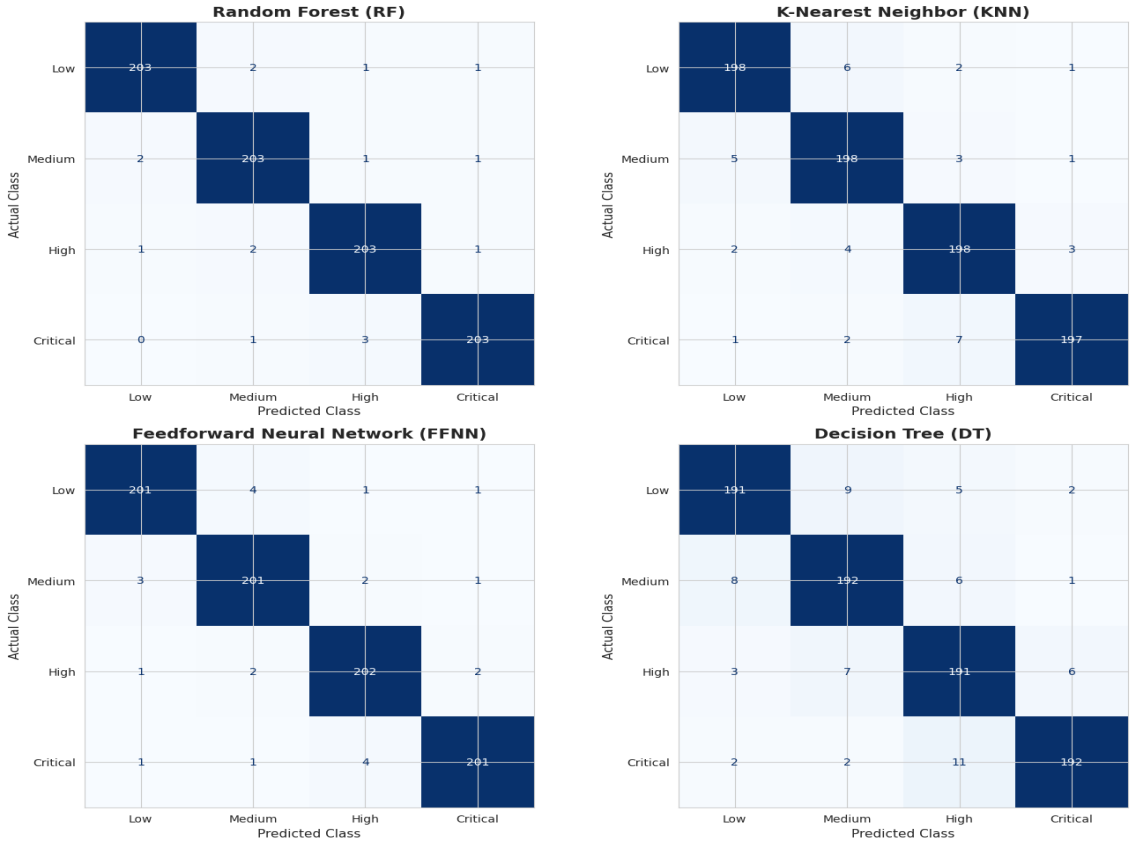


Figure 8: Confusion Matrix of the Individual Models

The confusion matrices in Figure 8 provide a detailed view of how each classifier predicted the four vulnerability severity classes: Low, Medium, High, and Critical. Each row represents the actual class and contains 207 samples, giving a total of 828 test samples across the four classes. The RF matrix showed strong performance for the different classes. For the

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

Low class, 203 vulnerabilities were correctly classified, with 2 misclassified as Medium, 1 as High, and 1 as Critical. For Medium, 203 instances were correctly predicted, with 2 misclassified as Low, 1 as High, and 1 as Critical. In the High class, 203 vulnerabilities were correctly classified, with 1 misclassified as Low, 2 as Medium, and 1 as Critical. For Critical, 203 instances were correctly identified, with 1 misclassified as Medium and 3 as High. The KNN showed good classification capability across the different classes. For Low, 198 vulnerabilities were correctly classified, with 6 misclassified as Medium, 2 as High, and 1 as Critical. For Medium, 198 instances were correctly predicted, with 5 misclassified as Low, 3 as High, and 1 as Critical.

For High, 198 vulnerabilities were correctly classified, with 2 misclassified as Low, 4 as Medium, and 3 as Critical. For Critical, 197 instances were correctly identified, with 1 misclassified as Low, 2 as Medium, and 7 as High. The FFNN exhibited highly consistent performance. For Low, 201 vulnerabilities were correctly classified, with 4 misclassified as Medium, 1 as high, and 1 as Critical. For Medium, 201 instances were correctly identified, with 3 misclassified as Low, 2 as High, and 1 as Critical. For High, 202 vulnerabilities were correctly classified, with 1 misclassified as Low, 2 as Medium, and 2 as Critical. For Critical, 201 instances were correctly identified, with 1 misclassified as Low, 1 as Medium, and 4 as High. Finally, the SVM achieved satisfactory results, although with several misclassifications.

For the Low severity class, 191 vulnerabilities were correctly classified, with 9 misclassified as Medium, 5 as high, and 2 as Critical. For Medium, 192 instances were correctly identified, with 8 misclassified as Low, 6 as High, and 1 as Critical. For High, 191 vulnerabilities were correctly classified, with 3 misclassified as Low, 7 as Medium, and 6 as Critical. For Critical, 192 instances were correctly identified, with 2 misclassified as Low, 2 as Medium, and 11 as High.

4.2 The Comparative Analysis

The comparative analysis of the four models considered the accuracy and Receiver Operating Characteristic (ROC) curve. The ROC measures the vulnerability severity classification of each model across the four classes (Low, Medium, High, and Critical). Each subplot shows the True Positive Rate (TPR) against the False Positive Rate (FPR), along with the AUC as a key performance metric. Table 8 compares the precision, recall, accuracy, and AUC of the four models.

Table 8: Comparative Analysis of the ML Models for Detection of Risks

Model	Precision	Recall	F1-Score	Accuracy	AUC
Random Forest (RF)	0.981	0.981	0.981	0.981	0.984
Feedforward Neural Network (FFNN)	0.975	0.975	0.975	0.971	0.977
K-Nearest Neighbor (KNN)	0.955	0.955	0.955	0.953	0.964
Support Vector Machine (SVM)	0.925	0.925	0.925	0.922	0.945

The comparative analysis of machine learning models in Table 8 for vulnerability risk detection revealed that RF consistently outperforms the other models across all evaluation metrics, achieving 0.981 in Precision, Recall, F1-Score, and Accuracy, along with the highest AUC of 0.984. The FFNN follows closely with balanced scores of 0.975 for Precision, Recall, and F1-Score, 0.971 for Accuracy, and an AUC of 0.977, demonstrating strong and stable classification capability. KNN exhibits solid performance with 0.955 across Precision, Recall, and F1-Score, 0.953 Accuracy, and an AUC of 0.964. In contrast, the SVM records the lowest results among the four models, with 0.925 in Precision, Recall, and F1-Score, 0.922 Accuracy,

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

and an AUC of 0.945. Overall, the results highlight the superiority of the RF approach for multi-class vulnerability risk identification.

This was exported to Replit cloud-based integrated development environment and then used to build the prototype software application system, which can identify risk with the RF-based model, evaluate and prioritize the risk in real time to identify vulnerabilities that can result in cyberattacks in organizations.

4.3 Results of the Adaptive Risk Assessment System

The adaptive risk assessment system was tested using a real CVE dataset from 2026 vulnerabilities. The reason was to demonstrate and assess its practical ability to identify different types of risk, evaluate, and prioritize within an organization.

To carry out the test, different CVE records collected considering different risks and severities were uploaded to the software. The results of the risk assessment when CVEs with very high severity and risk level were applied to test the model are reported in Figure 9.

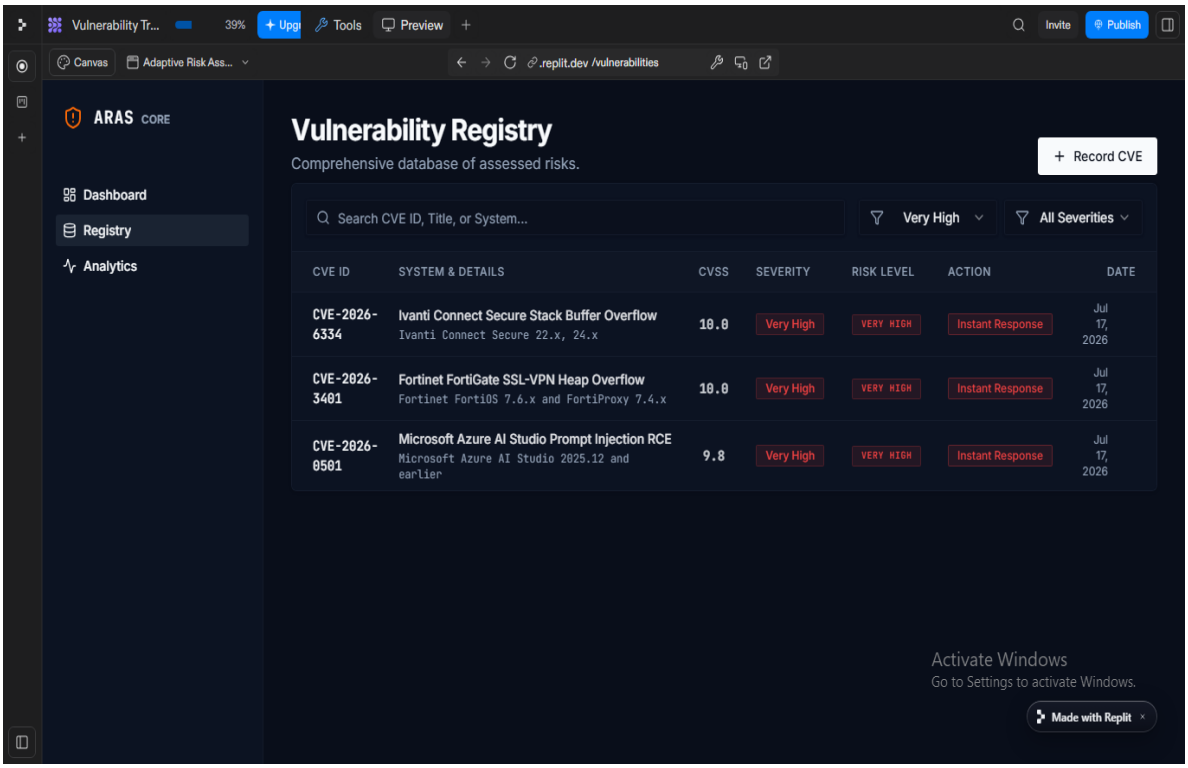


Figure 9: Result Showing Very High-Risk Vulnerability Assessment

Figure 9 presents the software performance when classifying CVE registry with very high vulnerability. The software output of the dashboard showed that the RF model was able to correctly identify the vulnerabilities; the risk was evaluated considering their score and then prioritized as very high severity.

The output triggers a fast incident response to control the risk and prevent a cyber-attack. In another test, CVE data with very low risk and medium severity were applied to test the software, as shown in Figure 10.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

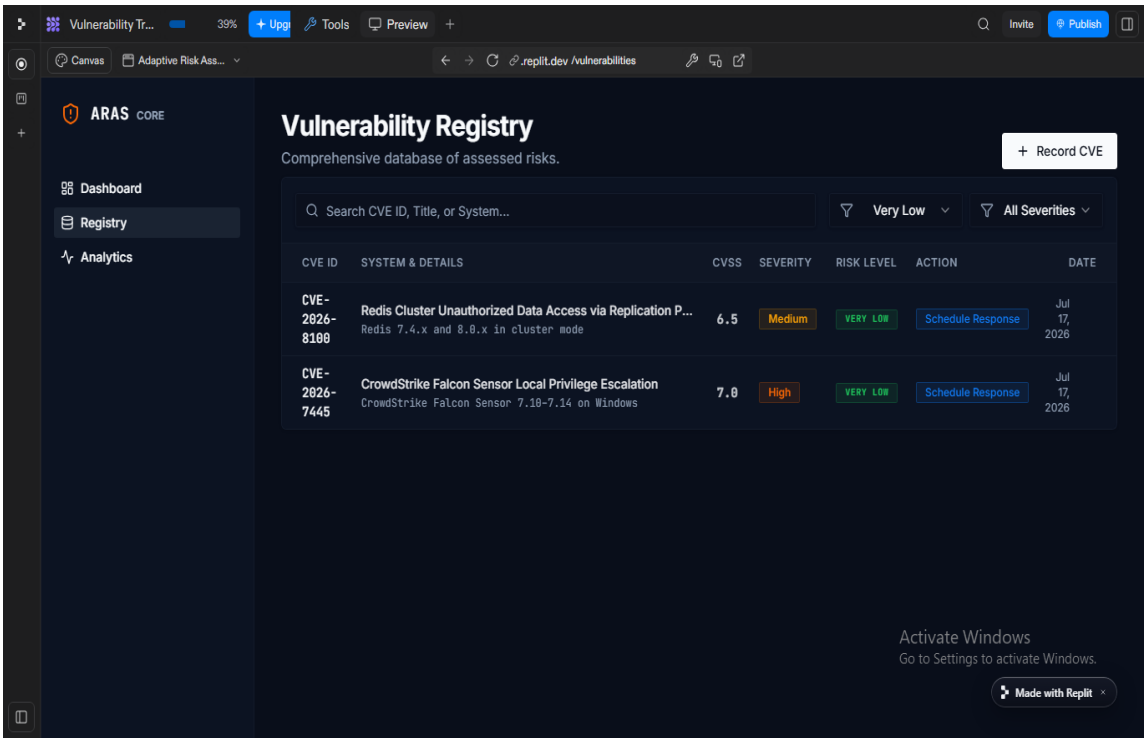


Figure 10: Result System When Tested With CVE Data with Very Low Risk Level and Medium Severity

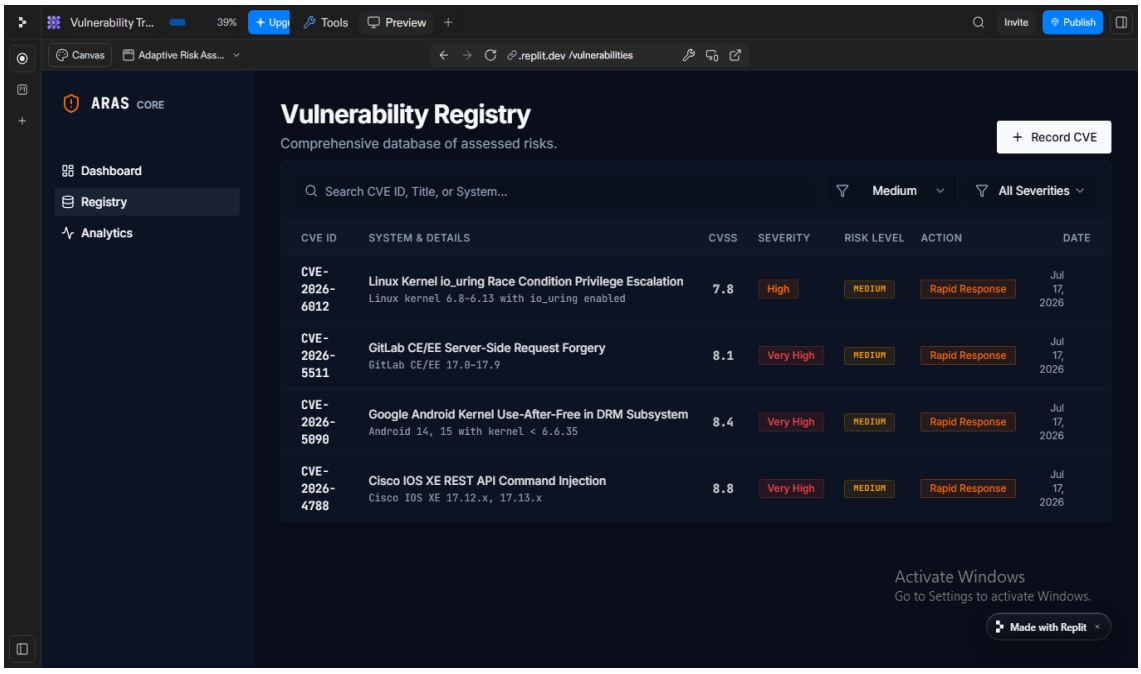


Figure 11: Result of the System When Tested With CVE of Very High Severity and Medium Risk Level

Figure 10 shows the result of the software when tested with CVEs with low risk and severity. Figure 11 also shows the result when tested with CVEs of high severity and medium risk level. These vulnerabilities represent moderate security threats that should be addressed after high-risk vulnerabilities have been mitigated.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

The adaptive risk assessment framework automatically evaluates the vulnerability attributes and assigns the corresponding risk category while recommending appropriate mitigation strategies. This prioritization supports structured vulnerability management by ensuring remediation activities follow an appropriate order of urgency. Figure 12 presents the adaptive risk classification across multiple types of vulnerabilities. Figure 13 presents the analysis dashboard, which summarizes the cybersecurity posture graphically.

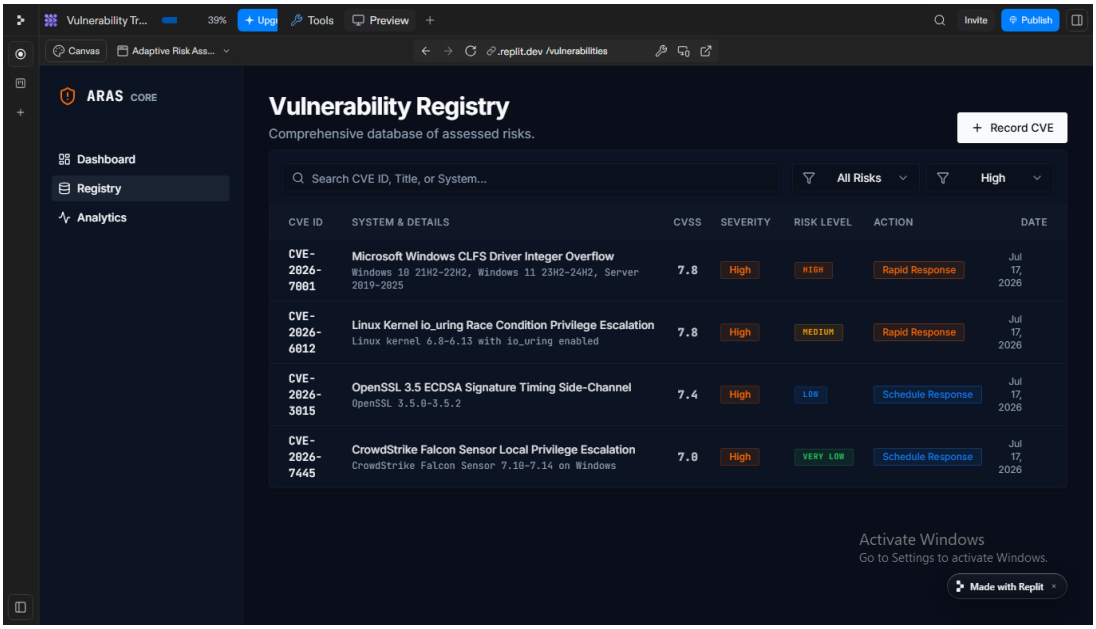


Figure 12: Result of Software Classifying Different Vulnerabilities

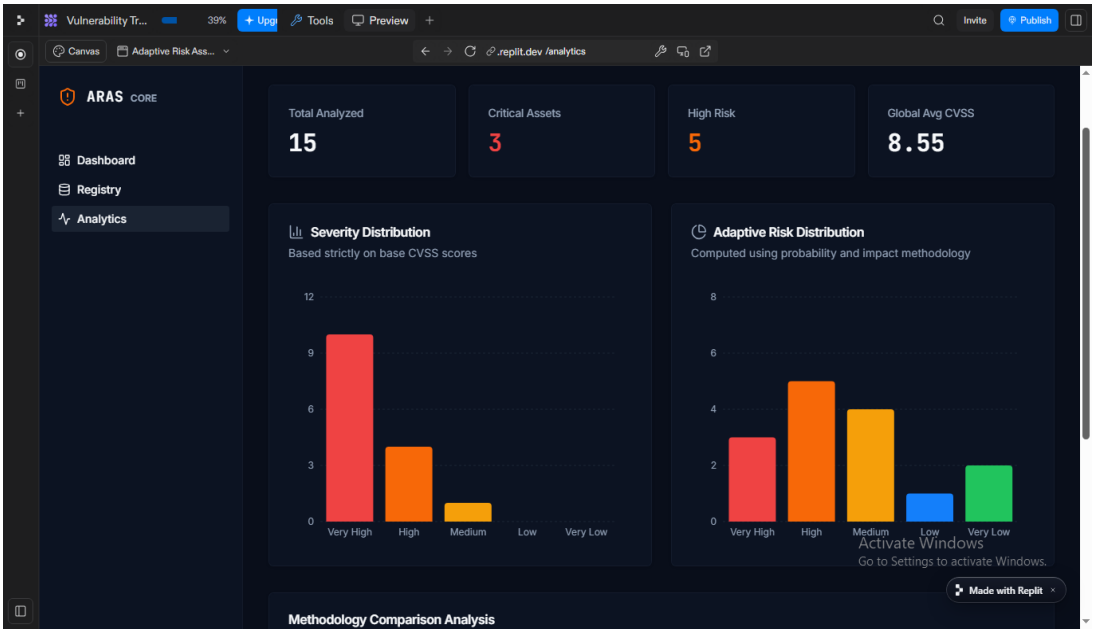


Figure 13: Analysis dashboard

Figure 12 presents the adaptive risk classification result. The diagram shows the output of the risk identification, evaluation, and prioritization of vulnerabilities belonging to multiple risk categories within the same registry. Each vulnerability is automatically assigned a risk level (Low, Medium, High, or Critical) based on the RF prediction model and associated CVSS

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

metrics. The color-coded labels improve situational awareness, allowing analysts to rapidly distinguish between vulnerabilities requiring immediate action and those that can be addressed later. This interface illustrates the dynamic nature of the proposed adaptive risk assessment framework. The analysis dashboard in Figure 13 provides the analytics dashboard, which summarizes the overall cybersecurity posture using graphical visualizations and key performance indicators. The dashboard displays the total number of analysed vulnerabilities, critical alerts, high-risk vulnerabilities, and the average CVSS score. In addition, bar charts illustrate the distribution of vulnerabilities across different severity levels, while the adaptive risk distribution chart presents the proportion of vulnerabilities assigned to each risk category. These visual analytics provide security managers with a high-level understanding of organizational risk exposure and support strategic decision-making regarding vulnerability remediation.

In general, the practical validation demonstrated that the adaptive risk assessment system consistently produced accurate classifications that aligned with the ground-truth severity labels contained in the NVD dataset. Furthermore, the software correctly ranked vulnerabilities according to their predicted risk levels, enabling security analysts to identify critical threats requiring immediate remediation while distinguishing lower-risk vulnerabilities that could be addressed during routine maintenance.

5. CONCLUSION AND SUGGESTION FOR FUTURE SCOPE

This study has demonstrated that machine learning can significantly improve cybersecurity risk assessment by providing an adaptive and intelligent approach to vulnerability evaluation and prioritization. The study integrates automated vulnerability classification with dynamic risk prioritization to support faster and more informed cybersecurity decision-making.

The implementation of the framework as a functional software application further demonstrates its practical applicability, enabling security analysts to automatically identify, assess, and prioritize vulnerabilities using real-world CVE information. The new adaptive risk assessment framework provides automated severity identification, evaluation, and risk prioritization, reducing the effort required for manual vulnerability analysis while enabling organizations to allocate remediation resources more effectively. In addition, the framework offers a practical solution for enhancing organizational cyber resilience, improving vulnerability management processes, and supporting proactive defence against emerging cyber threats.

The successful validation using real CVE records demonstrates the feasibility of deploying the new system in operational cybersecurity environments and highlights its potential for integration into enterprise security operations and decision-support systems. Future research can extend this new solution for adaptive risk detection through the following directions;

i. Develop automated remediation recommendation and response capabilities by integrating the framework with security orchestration, automation, and response platforms, enabling intelligent patch prioritization and automated incident response.

ii. Extend the framework to support adaptive cybersecurity risk forecasting, where future vulnerability trends and emerging attack patterns are predicted using temporal and sequential learning models, enabling proactive cyber defence strategies.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

5.2 Data Availability Statement

The link for the data source is [https://nvd.nist.gov/vuln/data-feeds].

5.3 Declaration of Generative Artificial Intelligence (AI)

The authors used Grammarly software to fix typographical errors. In addition, ChatGPT-4 was also applied in this paper only to improve the clarity of the manuscript and to fix errors encountered during the model training. All research design, data collection, analysis, interpretation of results, and conclusions were performed and verified by the authors, who take full responsibility for the content of this manuscript.

Reference

1) Arat F., &Akleylek S., (2023) A new method for vulnerability and risk assessment of IoT. Computer Networks 237 (2023) 110046 https://doi.org/10.1016/j.comnet.2023.110046

2) Benetis, D., Vitkus, D., Janulevičius, J., Čenys, A., &Goranin, N. (2024). Automated Conversion of CVE Records into an Expert System, Dedicated to Information Security Risk Analysis, Knowledge-Base Rules. Electronics, 13(13), 2642. https://doi.org/10.3390/electronics13132642

3) Bitton R., Maman N., Elovici Y., Shabtai A., Singh I., &Momiyama S., (2021) Evaluating the Cybersecurity Risk of Real World, Machine Learning Production Systems. arXiv:2107.01806v2 [cs.CR] 3 Oct 2021

4) Cheimonidis P., &Rantos K., (2023) Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. Future Internet 2023, 15, 324. https://doi.org/10.3390/fi15100324

5) Cheimonidis, P., &Rantos, K. (2025). A Dynamic Risk Assessment and Mitigation Model. Applied Sciences, 15(4), 2171. https://doi.org/10.3390/app15042171

6) Compagnoni S., (2022) Cyber risk assessment of complex infrastructures through machine learning-based techniques. Faculty of Engineering Department of Information EngineeringUNIVERSITÀ POLITECNICA DELLE MARCHE

7) Costa, J.C.; Roxo, T.; Sequeiros, J.B.; Proença, H.; Inácio, P.R. Predicting CVSS Metric Via Description Interpretation. IEEE Access 2022, 10, 59125–59134.

8) de Azambuja, A.J.G.; Plesker, C.; Schützer, K.; Anderl, R.; Schleich, B.; Almeida, V.R. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0 A Survey. Electronics 2023, 12, 1920. https://doi.org/10.3390/electronics12081920

9) Dennis H. (2023)"The Blind Spot: How to Simply Calculate Cyber Attack Likelihood Using the Exploitability Assessment";https://www.cybersecureot.info/post/the-blind-spot-how-to-simply-calculate-cyber-attack-likelihood-using-the-exploitability-assessment

10) Diamantopoulou, Vasiliki, Aggeliki Tsohou, and Maria Karyda. 2020. From ISO/IEC27001: 2013 and ISO/IEC27002: 2013 to GDPR compliance controls. Information & Computer Security 28: 645–62.

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

11) Fakhri A. (2022). Predicting call success of bank digital-marketing campaign with machine learning A Pythonista with a passion for data analytics, data science, QA automation, and network DevOps. https://www.linkedin.com/in/fakhri-azhar

12) Hedge J., &Rokseth B., (2020) Applications of machine learning methods for engineering risk assessment – A review. Safety Science 122 (2020) 104492

13) Huang B., Wei J., Tang Y., & Liu C., (2021) Enterprise Risk Assessment Based on Machine Learning. Hindawi Computational Intelligence and Neuroscience Volume 2021, Article ID 6049195, 6 pages https://doi.org/10.1155/2021/6049195

14) Jules S.,& Danielle S., (2022) Cyber-Risk Forecasting using Machine Learning Models and Generalized Extreme Value Distributions. 2022. https://hal.science/hal-03814979

15) Kalinin M., Krundyshev V., &Zegzhda P., (2021) Cybersecurity Risk Assessment in Smart City Infrastructures. Machines 2021, 9, 78. https://doi.org/10.3390/machines9040078

16) Kaloudi, N.; Jingyue, L.I. The AI-based cyber threat landscape: A survey. ACM Comput. Surv. 2020, 53, 20.

17) Kassem A., (2021) intelligent system using machine learning techniques for security assessment and cyber intrusion detection. Artificial Intelligence [cs.AI]. Université d'Angers, 2021. English. https://theses.hal.science/tel-03522384

18) Kucukkaya G., (2021) Cybersecurity Risk Assessment Using Graph Theoretical Anomaly Detection and Machine Learning. Doctor of Philosophy (PhD), Dissertation, Engineering Management & Systems Engineering, Old Dominion University, DOI: 10.25777/xry8-7b41 https://digitalcommons.odu.edu/emse_etds/183

19) Manjunathan A., Kethan Kota, Anoop S., Vivek S. (2024)" CVE Severity Prediction From Vulnerability Description - A Deep Learning Approach"; Procedia Computer Science 235(3105-3117).

20) Melaku, H. 2023. Context-Based and Adaptive Cybersecurity Risk Management Framework. Risks 11: 101. https://doi.org/10.3390/risks11060101

21) Narayanan S, Mannam K, Rajan SP, Rangan PV. Evaluation of Transfer Learning for Adverse Drug Event (ADE) and Medication Entity Extraction. Proceedings of the 3rd Clinical Natural Language Processing Workshop. 2020 Nov: 55 -64

22) National Vulnrability Database (NVD), 2025"Common Vulnerability Scoring System"; https://nvd.nist.gov/vuln-metrics/cvss

23) Nieto, P.J.G.; García-Gonzalo, E.; Paredes-Sánchez, J.P.; Sánchez, A.B.; Fernández, M.M. Predictive modelling of the higher heating value in biomass torrefaction for the energy treatment process using machine-learning techniques. Neural Comput. Appl. 2018, 31, 8823–8836.

24) Pangsuban p., Nilsook P., &Wannapiroon P., (2020) A Real-time Risk Assessment for Information System with CICIDS2017 Dataset Using Machine Learning. International Journal of Machine Learning and Computing, Vol. 10, No. 3, May 2020doi: 10.18178/ijmlc.2020.10.3.958

Volume 65 | Issue 08 | August 2026
DOI: 10.5281/zenodo.22078825

25) Radanliev P., Roure D., Walton R., Kleek M., Montalvo R., Maddox L., Santos O., Burnap P., &Anthi R., (2020) Artifcial intelligence and machine learning in dynamic cyber risk analytics at the edge. SN Applied Sciences (2020) 2:1773 | https://doi.org/10.1007/s42452-020-03559-4

26) Rajawat A., Goyal S., Bedi P., Jan T., Whaiduzzaman M., & Prasad M., (2023) Quantum Machine Learning for Security Assessment in the Internet of Medical Things (IoMT). Future Internet 2023, 15, 271. https://doi.org/10.3390/fi15080271

27) Raju G., Zavarsky P., Makanju A., & Malik Y., (2019) Vulnerability Assessment of Machine Learning Based Malware Classification Models. GECCO '19, July 13–17, 2019, Prague, Czech RepublicACM ISBN 978-1-4503-6748-6/19/07. . . $15.00 https://doi.org/10.1145/3319619.3326897

28) Sakthi M., Kumaar S., Vignesh V., & Santhi P., (2023) Assessment of Zero-Day Vulnerability using Machine Learning Approach. EAI Endorsed Transactions on Internet of Things. doi: 10.4108/eetiot.4978

29) Sánchez-García I., Mejía J., & San-Feliu G., (2023) Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. Appl. Sci. 2023, 13, 395. https://doi.org/10.3390/app13010395

30) Shahid, M.R.; Debar, H. (2021)" CVSS-BERT: Explainable Natural Language Processing to Determine the Severity of a Computer Security Vulnerability from its Description. In Proceedings of the 2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA), Pasadena, CA, USA, 13–16 December 2021; pp. 1600–1607.

31) Sheet O., & Ibraheem L., (2023) Design and Implement Machine Learning Tool for Cyber Security Risk Assessment. Journal of Education and Science (ISSN 1812-125X)DOI:10.33899/edusj.2023.137554.1307

32) Shetty N., & Kant R., (2021) Vulnerability Assessment for Cybersecurity using Machine learning. Electronic copy available at: https://ssrn.com/abstract=3884044

33) Shi, F., Kai, S., Zheng, J., & Zhong, Y. (2022). XLNet-Based Prediction Model for CVSS Metric Values. Applied Sciences, 12(18), 8983. https://doi.org/10.3390/app12188983

34) Wei Z., Liu H., TaoX., Pan K., Huang R., Ji W.,&Wang J., (2023) Insights into the Application of Machine Learning in Industrial Risk Assessment: A Bibliometric Mapping Analysis. Sustainability 2023, 15, 6965. https://doi.org/10.3390/su15086965

35) Xiong J., Wu J., (2020) Construction of information network vulnerability threat assessment model for CPS risk assessment. Computer Communications 155 (2020) 197–204 https://doi.org/10.1016/j.comcom.2020.03.026

36) Zhang J., Zheng J., Zhang Z., Chen T., Tan Y., Zhang Q., & Li Y., (2024) ATT&CK-based Advanced Persistent Threat attacks risk propagation assessment model for zero trust networks. Computer Networks 245 (2024) 110376 https://doi.org/10.1016/j.comnet.2024.110376