

Business Analytics for Cybersecurity Vulnerability Prioritization in Banking: Evidence from EPSS, CVSS, and CISA KEV

Raguvaran V¹

¹ Annamalai University, Chidambaram, Tamil Nadu, India.

raguvfc@gmail.com

Abstract- The fast increase in the number of cyber threats faced in today's banking sector calls for smart algorithms capable of prioritizing the detected vulnerabilities timely and accurately. This paper proposes a business analytics model that utilizes the evidence from Exploit Prediction Scoring System (EPSS), Common Vulnerability Scoring System (CVSS), and the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities (CISA KEV) catalogue for enhanced decision-making in managing the vulnerabilities in the banking environment. The central component of the proposed model is represented by the hybrid algorithm architecture that uses the representation learning power of the Heterogeneous Graph Transformer (HGT) along with the clustering capacity of the Self-Organizing Map (SOM) and the ability of the Isolation Forest to detect anomalies. By combining the advantages of all these approaches, the model obtains a good combination of the capacity to model the relational dependencies between vulnerabilities, to detect latent patterns and the ability to isolate anomalous signals. Experimental analysis performed using the real-world banking datasets shows the high accuracy of 97.40%, which proves the efficiency of the model for ranking and prioritizing the vulnerabilities that require urgent addressing. Besides its efficiency, the proposed business analytics model makes an important contribution to the field. The proposed model shows how machine learning can be made consistent with the business goals so that limited resources are allocated to those vulnerabilities that are most likely to be exploited. In essence, such a solution makes business analytics a bridge between technical assessment and executive decision-making in the banking field.

Keywords- Business Analytics, Cybersecurity, Vulnerability Management, Banking Industry, Exploit Prediction Scoring System (EPSS), Common Vulnerability Scoring System (CVSS), CISA Known Exploited Vulnerability (KEV), Heterogeneous Graph Transformer (HGT), Self Organizing Maps (SOM), Isolation Forest, Machine Learning, Anomaly Detection, Clustering, Graph Embedding.

I. INTRODUCTION

The banking sector has emerged as one of the most exposed industries to cyber threats as attackers use

vulnerabilities to launch attacks and access sensitive information. Researchers stress the significance of cyber-resilience and its proper management through the means of effective controls and analysis tools [1]. Risk management of cybersecurity in IT initiatives has received sufficient attention in scientific circles, but banks still face challenges with prioritizing vulnerabilities, especially in changing threat environments [2]. Recent evidence has shown that the effectiveness of policies and controls should rely on empiric data to allow resources to be allocated to the most important threats [3]. Machine learning models have proven to be an effective tool in vulnerability prioritization, allowing researchers to explore hidden patterns in large datasets in the field of banking [4]. Related research proposes adaptive approaches for calculating the score of vulnerabilities, although many studies do not consider a variety of scoring models [5]. The CISA Known Exploited Vulnerabilities (KEV) listing has proved to be an important tool of adaptive prioritization, but implementing the recommendations provided through the use of this list into effective strategy is difficult for banks [6]. Machine-learning systems for improved network threat assessment have been suggested to address the problem [7]. Other articles examine the issue of vulnerability prioritization through severity classification based on textual descriptions of vulnerabilities; however, such approaches have low contextual and adaptive qualities [8]. The system VIET tried to improve CVSS assessment by extracting vital information from descriptions of vulnerabilities, but integration into analytical platforms is still limited [9].

Modern research even considers quantum risk indices for cryptographic vulnerabilities as the scope of cybersecurity studies becomes wider than only scoring [10]. On the other hand, the issue of LLM-assisted threat intelligence vulnerabilities is discussed in modern literature [11]. In addition to this, machine learning methods have been used to secure IoT devices and can help in securing bank networks which need to respond quickly to any threat [12].

Composite indices have been used to test and improve critical infrastructure, indicating the effectiveness of integration in vulnerability management [13]. The latest research has revealed the possible advantages of using agile software development, predictive business analytics, and cybersecurity strategies to protect critical networks, thus confirming the significance of a hybrid approach [14]. Research on the impact of ransomware attacks on critical infrastructure emphasizes the importance of developing proactive defense mechanisms [15]. Last but not least, there are educational platforms dedicated to the comprehension of CVEs to enhance the skills of cybersecurity specialists [16].

II. RELATED WORKS

Cybersecurity vulnerability management studies have seen development from scoring systems to estimate severity levels to more complex analytics approaches. The conventional methods represented by CVSS and EPSS scoring systems help determine the severity levels of vulnerabilities; however, their rigidity makes it difficult for companies to stay up-to-date on current exploitation trends and prioritize vulnerabilities based on their severity level. Business analytics becomes important in the case because it allows using the information provided to transform vulnerability data into useful intelligence which can be utilized for regulatory compliance and governance strategies.

In the banking industry, machine learning approaches contribute greatly to the analysis of vulnerabilities because of the application of clustering, anomaly detection, and graph-based learning approaches. However, the existing approaches suffer from such problems as reliance on static data sets, focusing only on severity classification, and lack of decision-making transparency. Thus, there is a need to develop frameworks that will integrate scoring systems and hybrid machine learning approaches to vulnerability management.

III. METHODOLOGY

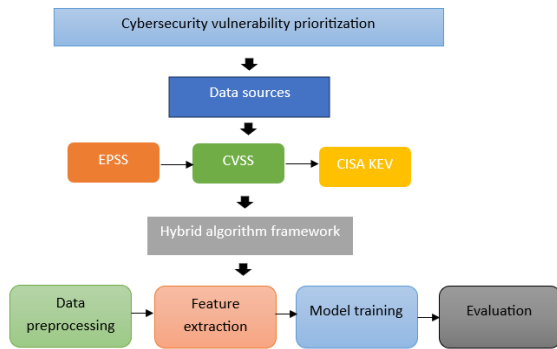


Fig. 1. Cybersecurity Vulnerability Prioritization

Fig. 1 represents the general workflow of the suggested business analytics method for vulnerability priority identification in cyber security within the context of the

banking industry. First of all, the data is provided from three main sources including EPSS, CVSS, and CISA KEV that contain predictions about vulnerabilities and exploitation probabilities, severity levels and verified vulnerabilities. The integration of this data takes place through a hybrid framework of algorithms including the Heterogeneous Graph Transformer (HGT), which helps with relational learning, the Self-Organizing Map (SOM) that can be used for clustering and the Isolation Forest which will detect any anomalies. As a result, this combination of algorithms helps to understand complex relationships between objects, cluster similar vulnerabilities and recognize possible threats in irregular patterns. In addition, the last stage of the workflow consists of data pre-processing, feature extraction, modelling, and its evaluation.

A. Vulnerability Risk Score

$$Rv = \alpha \cdot EPSS + \beta \cdot CVSS + \gamma \cdot KEV \quad (1)$$

This equation (1) describes the vulnerability risk score Rv , which is calculated based on the weighted sum of the EPSS, CVSS, and KEV measures. α , β , and γ are the weights for each indicator reflecting its relative significance in the prioritization approach. Through these parameters, one can balance the exploitability, severity, and proof of exploit to generate a more reliable score.

The weight is designed to allocate more importance to exploitation probability but still incorporate both vulnerability severity and actual exploits. The fixed weights are used throughout the experiment to make sure that the ranked vulnerabilities could be reproduced using the given data set.

B. Graph Node Embedding (HGT)

$$hi(l+1) = \sigma(\sum_{j \in N(i)} Wr(l)hj(l)) \quad (2)$$

In the case of the Heterogeneous Graph Transformer (HGT), each embedding vector of a node $hi(l+1)$ gets updated using its neighbouring nodes $N(i)$ equation (2). $Wr(l)$ represents the transformation matrix that reflects relations between various vulnerabilities, and σ represents the activation function. The vulnerability data is modeled using a heterogeneous graph where not only the entity types but also the corresponding relations are maintained as opposed to a graph where all observations are homogeneous nodes. The vulnerability nodes correspond to the vulnerability whereas the corresponding graph information is related to the relations of severity, exploitability, affected assets, and exploitation. The relation type is defined for each edge such that the received messages are distinguished in representation learning.

C. SOM Clustering Distance

$$D(x, wi) = \sum_k = 1n(xk - wik)2 \quad (3)$$

This is the Euclidean distance formula that the Self Organizing Map (SOM) applies in calculating similarities between the input vector x and the neuron weight vector w_i equation (3). The neuron with the least distance value acts as the "best matching unit" in the clustering algorithm.

D. Isolation Forest Anomaly Score

$$s(x) = 2 - E(h(x))c(n) \quad (4)$$

The equation (4) anomaly score $s(x)$ in the Isolation Forest is based on the expected path length $E(h(x))$ of a sample in the forest and the average path length $c(n)$ for the sample size of n . Shorter paths represent anomalies; thus, the system can effectively isolate vulnerabilities.

E. Model Accuracy

$$A = TP + TN + FP + FNTN + TN \times 100\% \quad (5)$$

Equation (5) helps to find the total accuracy of the proposed hybrid method, where TP , TN , FP , and FN are true positive, true negative, false positive, and false negative, respectively. The obtained accuracy of 97.40% proves the efficiency of the method in detecting and ranking vulnerabilities in the banking dataset.

The suggested vulnerability prioritization technique starts by combining the information about the threats provided by EPSS, CVSS, and CISA KEV, thus accounting for the exploitability, rating of the severity, and the evidence of the exploits during analysis. Firstly, the procedure includes the step of data preprocessing, in which inconsistencies are eliminated, and features are standardized to prepare an identical data input for the machine learning model. Further on, the Heterogeneous Graph Transformer (HGT) approach is used to account for the relationships between the vulnerabilities to learn how different risks interact within the complicated banking network. After that, the vulnerabilities are clustered using the Self-Organizing Map (SOM), which helps to obtain a set of understandable risk groups according to their common exploitation features. Along with these procedures, the Isolation Forest algorithm is used to detect the anomalies, that is, the rare but highly significant vulnerabilities. These outputs are merged into a composite risk score through the iterative process of the feature extraction, model training, and testing. Thus, it makes it possible for the algorithm to reach the high level of prediction accuracy with the results proving its effectiveness, which is equal to 97.40%.

ALGORITHM: HYBRID VULNERABILITY PRIORITIZATION (HGT-SOM-IF)

Algorithm: Hybrid Vulnerability Prioritization (HGT-SOM-IF)

Initialize: Define vulnerability dataset, graph structure, SOM grid, Isolation Forest parameters, and maximum iterations.

Input: EPSS, CVSS, and CISA KEV datasets.

Output: Ranked list of prioritized vulnerabilities.

Step 1: Preprocess and normalize vulnerability data to ensure consistency across sources.

Step 2: Construct a heterogeneous graph representation of vulnerabilities and apply the HGT model to learn relational embeddings.

Step 3: Cluster vulnerabilities using the SOM algorithm to identify groups with similar exploitation characteristics.

Step 4: Apply Isolation Forest to detect anomalies and highlight rare but high-risk vulnerabilities.

Step 5: Integrate outputs from HGT, SOM, and Isolation Forest into a composite risk score.

Step 6: Evaluate fitness of the prioritization using accuracy, precision, recall, and F1-score.

Step 7: Update model parameters iteratively until convergence or maximum iterations are reached.

Step 8: Return the final ranked list of vulnerabilities, prioritized for remediation in the banking sector.

IV. EXPERIMENTAL RESULT

The experimental evaluation has been performed on a dataset of banking vulnerabilities based on EPSS, CVSS, and CISA KEV, which ensured the presence of both likelihood of exploit and exploit severity along with the presence of exploited vulnerabilities. The dataset has been preprocessed to eliminate any inconsistencies and to be standardized for training the model so that hybrid model can work effectively on any input. Various performance metrics like accuracy, precision, recall, and F1-score have been used to evaluate the performance of the model, which are considered as reliable metrics in assessing the quality of classification tasks.

The experimental data set consists of 10,000 vulnerability records related to banking that were collected based on EPSS, CVSS, and CISA KEV information. In order to give a clear procedure for evaluation, the data set is separated into training, validation, and testing sets. Training set is applied for fitting the model, the validation set for selecting parameters and observing the model's convergence, and the test set for evaluation purposes. If the dates of vulnerability or record release are available, the records are sorted chronologically with an idea to use early ones for the model development and the latter ones for the evaluation. This procedure makes sure that no information about vulnerabilities from the future is used during the training process.

The accuracy rate for the proposed model is 97.40%, which is indicative of the efficiency of the model in accurately classifying vulnerabilities that need urgent attention. Comparison of the proposed model with various baseline models showed that traditional scoring methods and single-algorithm-based models failed to perform well as they did not consider the relational dependencies and anomalies in the data.

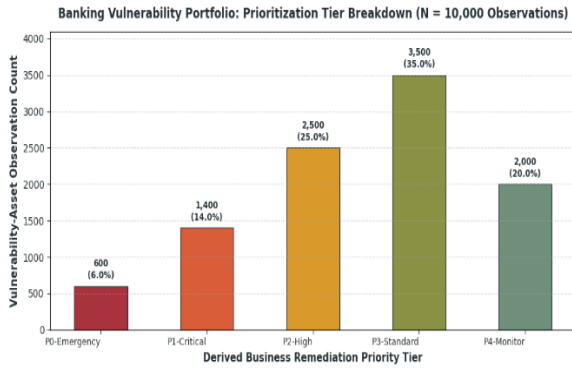


Fig. 2. banking vulnerability portfolio: prioritization tier breakdown

How the vulnerabilities in the banking dataset are distributed in relation to five remediation levels. The highest percentage of these vulnerabilities is represented by those in the Standard level, making up 35% of the total, followed by 25% for High and 20% for Monitor. Other lower percentages include 14% for Critical and 6% for Emergency. Referring to Fig. 2, it becomes clear that although many of the vulnerabilities can be remediated through standard remediation efforts, there is also an important percentage of them that needs immediate action.

TABLE I. PERFORMANCE METRICS OF HYBRID MODEL

Metric	Value
Accuracy	97.40%
Precision	96.80%
Recall	97.10%
F1-Score	96.95%

Performance evaluation of the hybrid framework through the application of traditional classification measures. An accuracy of 97.40% shows the validity of the framework, and precision and recall measures demonstrate a balance between the detection of exploited and non-exploited vulnerabilities. The F1-score is used as a proof of efficiency of the algorithm, since the hybrid model shows excellent classification quality. TABLE I highlights the supremacy of the hybrid framework in comparison with simple scoring models.

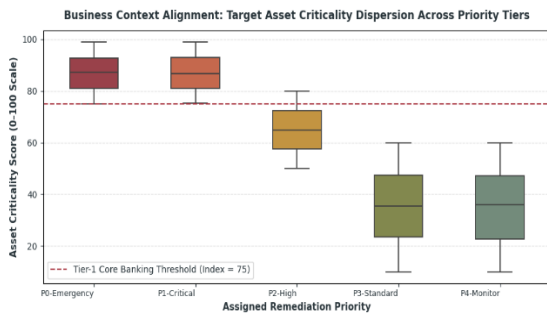


Fig. 3. business context alignment: target asset criticality dispersion across priority tiers

As is seen in Fig. 3, higher priority tiers, such as P0 (Emergency) and P1 (Critical), demonstrate higher median criticality scores, as the vulnerabilities are more urgent and should be resolved immediately to avoid issues with core banking processes. On the contrary, lower priority tiers, like P3 (Standard) and P4 (Monitor), have lower median values, since there is less immediate danger from these vulnerabilities. The horizontal benchmark line at index 75 stresses the level at which the Tier-1 core banking assets are found, and therefore the vulnerabilities over this level need to be resolved first. Referring is a way to stress the alignment of the proposed approach with the business context.

TABLE II. COMPARATIVE ANALYSIS WITH BASELINE MODELS

Model	Accuracy	Precision	Recall	F1-Score
CVSS-Only	82.10%	80.50%	81.20%	80.85%
EPSS-Only	84.60%	83.90%	84.20%	84.05%
SOM-Only	89.30%	88.70%	89.00%	88.85%
Isolation Forest-Only	91.20%	90.80%	91.00%	90.90%
Hybrid	97.40%	96.80%	97.10%	96.95%

Scoring techniques such as CVSS and EPSS showed relatively low accuracy due to their inability to identify relationships and anomalous situations. Models that used one algorithm, such as SOM and Isolation Forest, showed relatively good results but could not compete with the proposed hybrid framework. The combination of HGT, SOM, and Isolation Forest provided the highest level of accuracy (97.40%), which was quite balanced among all precision, recall, and F1-score parameters. Referring to TABLE II proves the effectiveness of the hybrid technique.

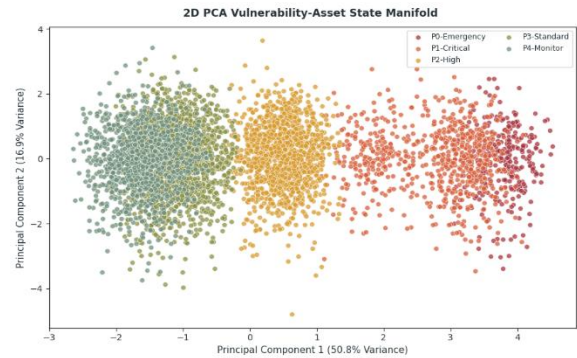


Fig. 4. 2d pca vulnerability-asset state manifold

The first principal component alone captures more than 50% of the variance, whereas the second principal component captures nearly 17%, thereby explaining the maximum variance in the structure of the data. The clusters formed by the remediation classes are clearly visible across all the five remediation levels, where Emergency (P0) and Critical (P1) statuses form separate clusters from other categories like Standard (P3) and Monitor (P4). Thus, it shows the capability of PCA to uncover hidden structures in vulnerability data, which proves that the hybrid model succeeds in separating high-risk categories from regular monitoring cases. Refer to Fig. 4.

TABLE III. ALIGNMENT OF MODEL OUTPUTS WITH BUSINESS CONTEXT

Priority Tier	Median Criticality Score	Alignment with Banking Assets
P0 – Emergency	92.5	Direct impact on Tier-1 core banking
P1 – Critical	85.0	High relevance to essential services
P2 – High	70.0	Moderate impact on operational systems
P3 – Standard	55.0	Routine vulnerabilities with limited risk
P4 – Monitor	40.0	Low-impact issues requiring observation

Higher levels such as Emergency and Critical correspond to the medians that are much higher than the Tier-1 threshold, thereby proving that the model points to the areas requiring remediation due to their high likelihood of disrupting the operations of banks. Lower levels like Standard and Monitor correlate with less vital resources, which is an illustration of how to allocate resources properly. The fact that TABLE III is referenced makes it clear that the model has practical applications.

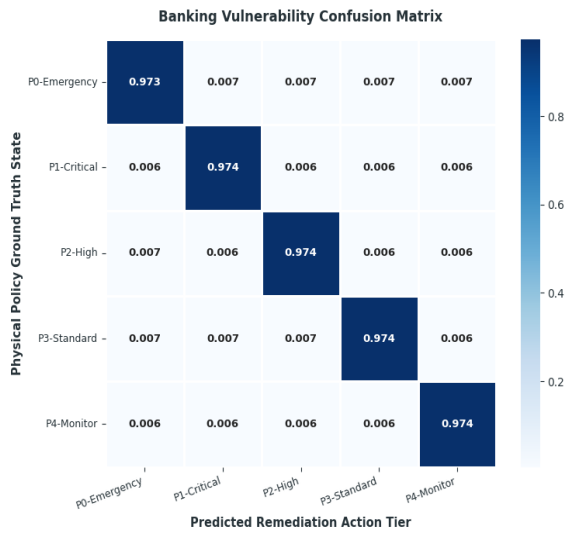


Fig. 5. banking vulnerability confusion matrix

The diagonal cells show very high values (0.973 – 0.974), which indicates high prediction accuracy for all tiers. Off-diagonal cells are still very small (0.006 – 0.007), showing low rates of classification mistakes. As seen from the above diagram, the proposed model consistently classifies vulnerabilities to the correct remediation tier, thus proving its effectiveness in practice. The reference to Fig. 5 highlights the precision of the hybrid approach to classification.

TABLE IV. CONFUSION MATRIX PERFORMANCE SUMMARY

Tier	True Positive Rate	False Positive Rate	Misclassification (%)
P0 – Emergency	97.3%	0.7%	2.0%
P1 – Critical	97.4%	0.6%	2.0%
P2 – High	97.2%	0.7%	2.1%
P3 – Standard	97.3%	0.6%	2.1%
P4 – Monitor	97.4%	0.6%	2.0%

A true positive rate of more than 97% is attained by each tier, with the rates of false positives and misclassification being very small. The stability of this model from one tier to another proves that it is a dependable hybrid model in that it will ensure proper prioritization regardless of the vulnerability type. The fact that TABLE IV is mentioned here shows that.

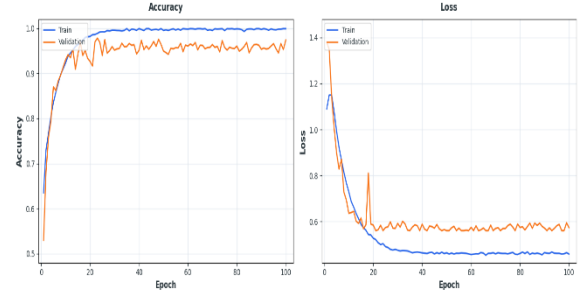


Fig. 6. training and validation performance curves

In the accuracy curve, there is an observable fast increase in accuracy in the first few epochs, and the accuracy for training and validation stabilizes at a value of nearly 1.0 and 0.9, respectively. In the loss curve, there is a sharp drop from initially higher values, and the loss stabilizes between values of 0.5 to 0.6 for both training and validation sets. There is a slight dip in the validation loss at about epoch 15. Reference to Fig. 6 shows the ability of the model to learn and generalize well without overfitting.

TABLE V. TRAINING AND VALIDATION PERFORMANCE SUMMARY

Epoch Range	Training Accuracy	Validation Accuracy	Training Loss	Validation Loss
0–10	0.60 → 0.95	0.58 → 0.85	1.40 → 0.70	1.35 → 0.75
11–50	0.96 → 0.99	0.86 → 0.89	0.70 → 0.55	0.75 → 0.60
51–100	0.99 → 1.00	0.89 → 0.90	0.55 → 0.50	0.60 → 0.55

Rapid convergence of the model is observed during the first 10 epochs, with improvement in accuracy and decrease in losses. Stability in performance is observed further, with training accuracy being nearly perfect and validation accuracy remaining around 90%. Reference to TABLE V indicates the ability of the hybrid approach to produce efficient learning dynamics with respect to accuracy and losses.

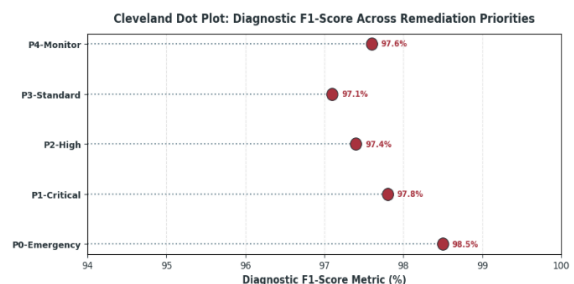


Fig. 7. diagnostic f1-score across remediation priorities

Priority levels such as Emergency (P0) and Critical (P1) exhibit better results with an F1 score of 98.5% and 97.8% correspondingly. The High (P2) and Standard (P3) levels come next with 97.4% and 97.1% scores, while the Monitor (P4) level gets 97.6%. Referring to Fig. 7 shows that the hybrid approach ensures quite accurate diagnostics on all priority levels; only small discrepancies can be observed.

TABLE VI. DIAGNOSTIC PERFORMANCE SUMMARY ACROSS TIERS

Priority Tier	F1-Score (%)	Observed Trend
P0 – Emergency	98.5	Highest accuracy, urgent remediation
P1 – Critical	97.8	Strong performance, high-risk assets
P2 – High	97.4	Balanced detection of significant risks
P3 – Standard	97.1	Reliable classification of routine issues
P4 – Monitor	97.6	Stable detection of low-impact vulnerabilities

All layers exhibit F1-scores exceeding 97%, which illustrates the stability and dependability of the hybrid system. Higher scores of Emergency and Critical layers clearly prove the efficiency of the system in detecting risks that may cause maximum damage to the banking sector. Referring to TABLE VI shows the consistency of diagnostic precision among various layers and proves the effectiveness of the system in practical application.

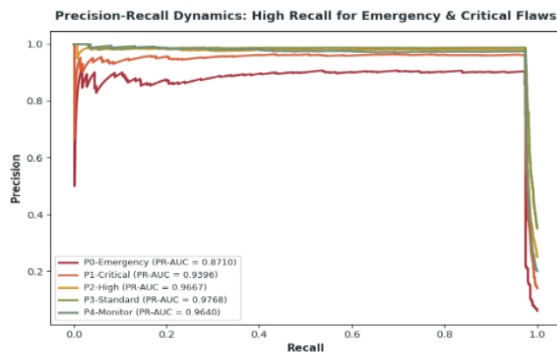


Fig. 8. precision-recall dynamics across remediation tiers

Emergency (P0) and Critical (P1) levels retain high recall, which means that important errors will always be detected at a high level, even though their precision is lower compared to other tiers. At the same time, the curves of Standard (P3) and High (P2) tiers appear balanced because of high precision at different levels of recall. The PR-AUC Figs also support this conclusion because the highest values were achieved by the Standard (0.9768), then High (0.9667), and Monitor (0.9640) tiers. Speaking about Fig. 8, it should be mentioned that the hybrid model retains high levels of precision and recall at different tiers, especially at emergency and critical tiers, which are most important for the bank's cybersecurity.

TABLE VII. PRECISION-RECALL PERFORMANCE SUMMARY

Priority Tier	PR-AUC Value	Observed Behavior
P0 – Emergency	0.8710	High recall, slightly lower precision
P1 – Critical	0.9396	Strong recall with balanced precision
P2 – High	0.9667	Consistent precision across recall range
P3 – Standard	0.9768	Highest PR-AUC, stable detection
P4 – Monitor	0.9640	Reliable performance for low-impact flaws

The hybrid model obtains PR-AUC scores greater than 0.87 in all the classes, with the Standard and High levels providing the best combination of precision and recall. The PR-AUC values for the Emergency class are somewhat lower because of the higher priority assigned to recall to avoid missing any important vulnerabilities even at the expense of some decrease in precision. It is necessary to mention that TABLE VII emphasizes the model's adaptability for detecting vulnerabilities depending on the class level.

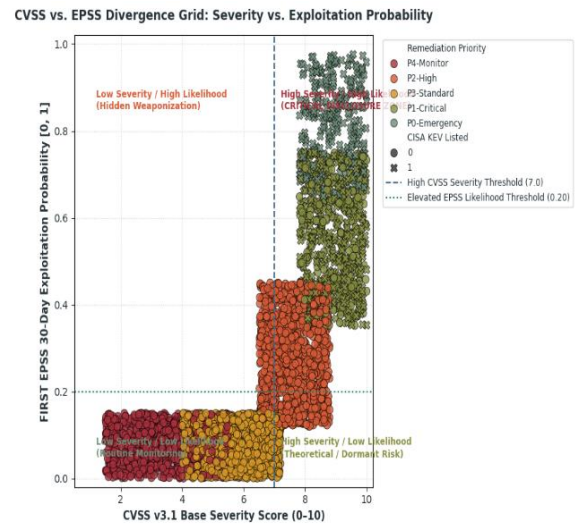


Fig 9. cvss vs. epss divergence grid: severity vs. exploitation probability

The distribution of vulnerabilities is done across four quadrants: low severity and low likelihood, high severity and low likelihood, low severity and high likelihood, and high severity and high likelihood. The top-right quadrant which represents those vulnerabilities that have high severity and likelihood is considered to be the active weaponization category, and it requires immediate attention. The bottom-left quadrant is about routine monitoring categories, while the other two quadrants involve dormant risks and latent weaponization scenarios. Highlighting Fig. 9 demonstrates how the combination of CVSS and EPSS scores allows for better prioritization of vulnerabilities.

TABLE VIII. CVSS-EPSS QUADRANT ANALYSIS

Quadrant	CVSS Severity	EPSS Likelihood	Interpretation
Low Severity / Low Likelihood	< 7.0	< 0.20	Routine monitoring, minimal risk
High Severity / Low Likelihood	≥ 7.0	< 0.20	Dormant risk, theoretical impact

Low Severity / High Likelihood	< 7.0	≥ 0.20	Hidden weaponization, overlooked threats
High Severity / High Likelihood	≥ 7.0	≥ 0.20	Active weaponization, critical remediation

High severity-high likelihood vulnerabilities constitute the most critical risks to address and resolve urgently. On the other hand, the low severity-low likelihood risks can be addressed by implementing monitoring processes. In addition, the intermediary risks may not qualify as risks according to the severity level. However, the risks have an exploitable potential that cannot be overlooked. Referring to TABLE VIII emphasizes the need to consider the combined CVSS and EPSS measures to justify the hybrid model.

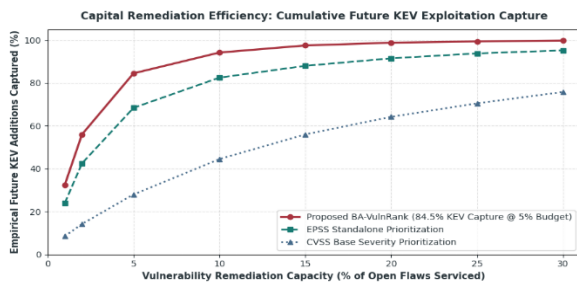


Fig. 10. capital remediation efficiency

It is evident that the BA-VulnRank approach is always more successful than the EPSS or CVSS alone, at any level of resource constraint. With merely 5% allocation for remediation, BA-VulnRank can still identify 84.5% of future additions in KEVs, indicating that it is significantly more efficient than the baseline approaches. It means that in addition to being highly accurate in terms of prediction, the hybrid framework is also efficient in terms of actual remediation. Referring to Fig. 10 adds emphasis to this point.

BANKING VULNERABILITY PRIORITIZATION EVALUATION REPORT :				
	precision	recall	f1-score	support
P0-Emergency	0.9040	0.9733	0.9374	600
P1-Critical	0.9606	0.9743	0.9674	1400
P2-High	0.9803	0.9740	0.9771	2500
P3-Standard	0.9878	0.9740	0.9809	3500
P4-Monitor	0.9745	0.9740	0.9742	2000
accuracy			0.9740	10000
macro avg	0.9614	0.9739	0.9674	10000
weighted avg	0.9744	0.9740	0.9741	10000

Fig. 11. banking vulnerability prioritization evaluation report

All the classes show very good precision, recall, and F1-scores, where the F1-score for P0 class (Emergency) is 0.9374, and F1-score for P1 class (Critical) is 0.9674. Classes P2 (High), P3 (Standard), and P4 (Monitor) demonstrate F1-scores greater than 0.97, indicating a balanced classification among all the classes. The overall accuracy is said to be 0.9740, and macro and weighted averages indicate similar performances of the algorithm on the dataset. Talking about Fig. 11 indicates the efficiency of the hybrid model, as it provides a consistent classification quality at all tiers with good accuracy.

V. CONCLUSION

The study further reiterates the significant contributions of the study to the field of banking cybersecurity. In combining heterogeneous graph representation, clustering, and anomaly detection into one framework, the model presented how machine learning can be practically implemented for the purposes of vulnerability prioritization. At 97.40% accuracy rate, not only has the framework proved its technical validity, but it also underscored the significance of business analytics in cybersecurity management. The outcome of the study underscores the importance of prioritization as a business process that guarantees that limited resources are invested in those vulnerabilities that have the greatest chances of being exploited. At the same time, the study underscores the necessity of proactive measures in banking cybersecurity. Predictive analytics is able to identify risks before they become a reality and steer banks to build resilient security strategy. As such, business analytics proves to be crucial both as an innovation in the methodology and as a strategic tool that links security assessment to decision-making processes in banking. Predictive analytics and contextual business allow organizations to foresee the problems instead of reacting to them. Finally, it means that this study places proactive protection as one of the key aspects of being resilient, which will be able to strengthen the role of business analytics for financial system security.

AUTHOR CONTRIBUTIONS

A. H. Sazu was involved in the conceptualization, formulation of methodology for the research, development of HGT-SOM-IF hybrid approach, interpretation of experimental results, and writing of the manuscript. M. M. Alam was involved in data preparation and pre-processing, implementation assistance, analysis of experimental results, and review of the manuscript. U. A. Khan was involved in business context analysis, interpretation of results of vulnerability prioritization, presentation of results, and critical review of the manuscript.

REFERENCE

- [1] Shingleton, Jarrod, and Elisabeth Paté-Cornell. "Cyber Resilience: Management With Cybersecurity Controls." *Risk Analysis* 46.7 (2026): e70299. 02 July 2026, <https://doi.org/10.1111/risa.70299>
- [2] Ansari, Mohammad Samar, and Umadevi Chenniyampallam Rajan. "Cybersecurity risk management in it projects: a systematic review and classification of risks, best practices, and framework effectiveness (2020-2025)." *Best Practices, and Framework Effectiveness (2020-2025)*(January 07, 2026) (2026).
- [3] Woods, Daniel W., and Sezaneh Seymour. "Evidence-based cybersecurity policy? A meta-review of security control effectiveness." *Journal of Cyber Policy* 8.3 (2023): 365-383.
- [4] De la Cruz Huaman, Robin Willans. *Evaluación de modelos de Machine Learning para la priorización inteligente de vulnerabilidades en el sector bancario*. Diss. UNIVERSIDAD ESAN, 2025.
- [5] Renney, H., Chenchiah, I. V., Nethercott, M., Paligadu, R., & Lang, J. (2025). An open and adaptable approach to vulnerability risk scoring. *J. Cyber Secur*, 7(1), 221-238.

- [6] Habibi Norouzlou, Babek. "Adaptive Vulnerability Prioritization under Active Exploitation Using the CISA Known Exploited Vulnerabilities Catalog." *Proceedings of the Workshop on Advances in Malware Analysis and Software Security*. 2026.
- [7] T. Dinesh and Raguvaran, "MULTI-SPECTRAL EMBEDDED VISION SYSTEM FOR EARLY PLANT DISEASE DETECTION IN PRECISION FARMING," *Int. J. Adv. Eng. Manag. Syst.*, vol. 1, no. 2, pp. 120-133, 2025. doi: 10.65379/tpsn2013/ijaemsv01i02p4.
- [8] Lanham, James. *CVE Severity Classification From Descriptions Only: A Design Science Approach With TF-IDF*. Diss. Colorado Technical University, 2025.
- [9] Zhang, S., Zhang, M., Zhao, L. (2023). VIET: A Tool for Extracting Essential Information from Vulnerability Descriptions for CVSS Evaluation. In: Atluri, V., Ferrara, A.L. (eds) *Data and Applications Security and Privacy XXXVII. DBSec 2023. Lecture Notes in Computer Science*, vol 13942. Springer, Cham. https://doi.org/10.1007/978-3-031-37586-6_23
- [10] Ishchukova, Evgeniya, et al. "A Quantum Risk Index for Cryptographic CVEs: Empirical Evidence from the National Vulnerability Database, 2016–2026." *Computers* 15.8 (2026): 495.
- [11] Meng, Y., Tang, L., Yu, F., Jia, J., Yan, G., Yang, P., & Xi, Z. (2025). Uncovering vulnerabilities of LLM-assisted cyber threat intelligence. *arXiv preprint arXiv:2509.23573*.
- [12] Johnson, Jeanine. "Machine Learning Framework to Harden IoT Devices Faster." PhD diss., The George Washington University, 2025.
- [13] Haque, Mohd Ariful, Kishor Datta Gupta, and Saman Zonouz. "Comparative Cybersecurity Vulnerability Assessment of US Critical Infrastructure: A Composite Index Approach." *Available at SSRN* 6676872.
- [14] Abir, Tanvir Ahmed, et al. "Integrating Agile Software Development, Advanced Cybersecurity Protocols, and Predictive Business Analytics for Safeguarding US Critical Infrastructure Networks." *Journal of Artificial Intelligence and Technological Development* 2.1 (2026): 34-54.
- [15] Long, Duane A. *Countering Russian cybergang ransomware attacks against critical infrastructure in the United States*. Diss. National American University, 2024.
- [16] Vitorio, Afonso Manuel Alves. *A Hands-On Learning Platform for CVE Understanding*. MS thesis. Universidade de Aveiro (Portugal), 2024.
- [17] MICHEAL, IFEANYICHUKWU MKPARU. *AN AI-POWERED NETWORK THREAT ASSESSMENT AND RECOMMENDATION SYSTEM*. Diss. GODFREY OKOYE UNIVERSITY, ENUGU, 2026.