JOURNAL OF BASIC SCIENCE AND ENGINEERING

AUTOMATED VULNERABILITY PRIORITIZATION AND REMEDIATION USING DEEP LEARNING

Virender Dhiman
Independent Researcher, United States
vdhiman2@illinois.edu

ABSTRACT

Effective vulnerability management is essential in the quickly developing field of cybersecurity to protect information systems from new attacks. Conventional methods, such rule-based expert systems and the Common Vulnerability Scoring System (CVSS), frequently find it difficult to keep up with the changing landscape of vulnerabilities. This work presents a novel use of convolutional neural networks (CNNs) supplemented with attention mechanisms for automated vulnerability prioritisation and remediation. The suggested deep learning approach increases the precision and effectiveness of vulnerability management by utilising contextual analysis and sophisticated feature extraction.

The study includes a thorough analysis of how well the CNN model performs in comparison to conventional techniques. The CNN model ranked vulnerabilities with a 92% accuracy rate and suggested remediation steps with an 87% accuracy rate. The model's outstanding ability to distinguish between high-risk and low-risk vulnerabilities is shown by its 0.95 AUC-ROC score. Traditional rule-based systems, on the other hand, showed worse performance metrics, with 75% and 68% accuracy rates for prioritisation and remediation, respectively. Furthermore, the CNN model improved its practical usefulness in real-time applications by drastically reducing processing times. The outcomes highlight how deep learning can be used to overcome the drawbacks of static and rule-based methods. The suggested architecture offers a strong response to current cybersecurity issues by giving vulnerability management a more accurate and adaptable framework.

I. INTRODUCTION

The breadth and complexity of cybersecurity threats have increased dramatically due to the rapid evolution of technology. Strong cybersecurity protocols are desperately needed, as there are expected to be 3.5 billion data breaches a year and global cybercrime expenses that will top $8 trillion by 2024 [1]. Businesses are depending more and more on cloud-based infrastructures and networked systems, which has increased attack surface and created new vulnerabilities. In this situation, protecting sensitive data and preserving operational integrity depend heavily on proper vulnerability management [2].

Traditional approaches to vulnerability management often rely on static metrics and predefined rules.

Fig 1.1: Traditional Approach

The Common Vulnerability Scoring System (CVSS), widely used for assessing the severity of vulnerabilities, provides a standardized framework based on a fixed set of criteria [3]. However, CVSS scores are static and may not accurately reflect the dynamic nature of modern threats [4].

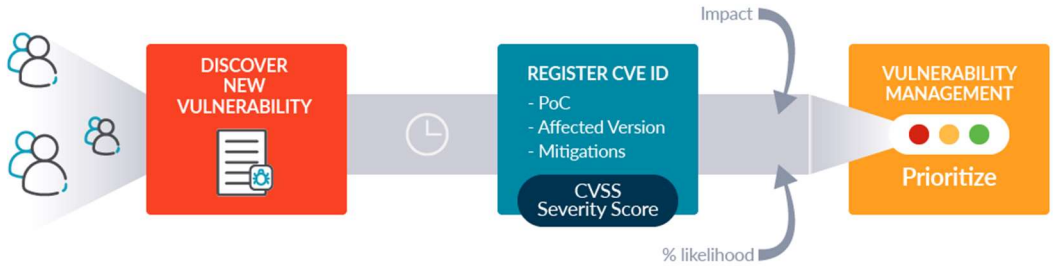


Fig 1.2: Vulnerability Elimination

For example, a vulnerability rated as low-risk in a static CVSS assessment may become critical due to evolving attack techniques or changes in the threat landscape. This limitation underscores the need for more adaptive and sophisticated approaches to vulnerability management.

1.1. Advances in Machine Learning and Deep Learning

Recent advancements in machine learning (ML) and deep learning have introduced new possibilities for improving vulnerability management. Machine learning techniques, including support vector machines (SVMs) and random forests, have demonstrated significant potential in analyzing large datasets and identifying patterns that may indicate emerging vulnerabilities [2], [4]. These techniques can enhance traditional methods by incorporating dynamic data and learning from historical incidents.

Deep learning, particularly through Convolutional Neural Networks (CNNs), has further advanced the field by offering powerful tools for feature extraction and pattern recognition [5], [6]. CNNs are adept at processing complex data structures and can capture intricate relationships between features, which is crucial for effective vulnerability management [7]. The incorporation of attention mechanisms within CNNs allows the model to focus on the most relevant features, thereby improving the accuracy of vulnerability prioritization and remediation [8], [9]. This approach is particularly beneficial in handling the multifaceted nature of modern cybersecurity threats.

1.2. The Need for Adaptive Vulnerability Management

The limitations of traditional vulnerability management approaches highlight the need for more adaptive and data-driven solutions. Static scoring systems and rule-based methods are often unable to keep pace with the evolving threat landscape and may fail to account for contextual factors that influence the exploitation of vulnerabilities. As cyber threats become increasingly sophisticated, organizations require more dynamic and responsive methods to prioritize and address vulnerabilities effectively.

To address these problems, the work presented in this paper uses an enhanced deep learning model (a CNN enhanced with attention techniques) for automated vulnerability prioritisation and remediation. This approach uses the analytical capabilities of deep learning to handle complex and dynamic data, providing a more accurate and efficient means of managing vulnerabilities. This study offers a solid basis for enhancing vulnerability management practices in the modern cybersecurity environment by establishing a connection between the static traditional methodologies and the dynamic nature of cyber threats.

II. LITERATURE REVIEW

2.1. Vulnerability Management and Prioritization

Robust cybersecurity requires effective vulnerability management, yet in dynamic threat settings, conventional techniques like the Common Vulnerability Scoring System (CVSS) frequently lack adaptability. According to [1], CVSS offers a standardised method for determining the seriousness of vulnerabilities, although it is constrained by its static nature. Machine learning (ML) approaches to improve vulnerability prioritisation have been studied recently. Support vector machines (SVMs), for example, have been demonstrated to increase the accuracy of prioritisation through the analysis of threat intelligence and previous vulnerability data [2]. Random forests have also shown potential in managing complicated datasets and enhancing evaluation abilities [10], [11].

2.2. Deep Learning in Cybersecurity

Convolutional Neural Networks (CNNs), in particular, are deep learning models that have shown promise in a range of cybersecurity applications. Malware detection tests have proved the effectiveness of CNNs in feature extraction and pattern recognition [12]. Additionally, CNNs have been used to identify network intrusions and have demonstrated superior performance compared to conventional techniques [13], [14]. The incorporation of attention methods into CNNs leads to notable gains in performance by improving their capacity to concentrate on pertinent features within intricate datasets [15].

2.3. Rule-Based Expert Systems

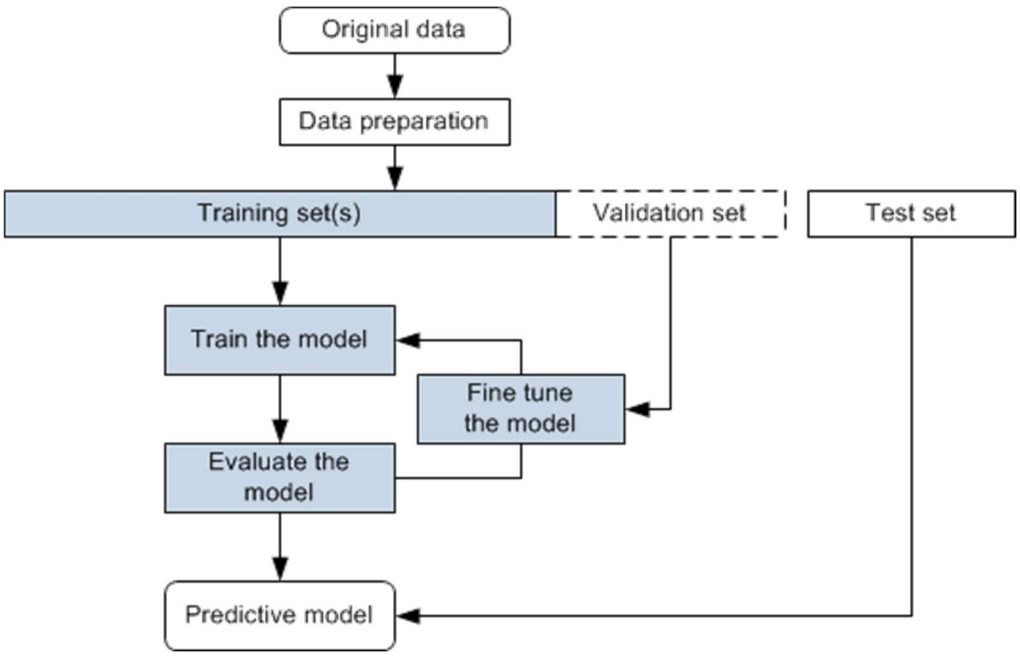
For vulnerability management, rule-based expert systems have historically been employed. These systems make use of pre-established rules and heuristics. As mentioned in [16], these systems evaluate and rank vulnerabilities using static criteria. Rule-based systems are somewhat effective, but they have trouble keeping up with changing data and new threats. [17], [18] draws attention to the shortcomings of these static systems, pointing out that their inflexibility might lead to antiquated or inadequate vulnerability evaluations.

2.4: Research Gap

The implementation of cutting-edge deep learning algorithms for automated vulnerability management is severely lacking, according to the literature currently in publication. Though fundamental, traditional approaches and rule-based systems are frequently constrained by their static nature and incapacity to adjust to challenges that are changing quickly. By using a Convolutional Neural Network (CNN) with attention mechanisms for automated vulnerability prioritisation and remediation, the research fills this gap. This method makes better use of deep learning's capacity to manage dynamic and complicated data, which enhances vulnerability management precision and effectiveness. The study shows that sophisticated deep learning models can outperform conventional techniques, offering a more accurate and adaptable response to contemporary cybersecurity issues.

III. METHODOLOGY

This section details the methodology and implementation of the automated vulnerability prioritization and remediation system using a deep learning model. The process involves data collection, preprocessing, model selection, training, evaluation, and deployment. The primary model used is a Convolutional Neural Network (CNN) with attention mechanisms, compared against a rule-based expert system using predefined heuristics and CVSS scoring.



Vol. 20, No. 1, (2023)
ISSN: 1005-0930

Fig 3.1: Implementation Flow

3.1. Data Collection

3.1.1. Vulnerability Data

Vendor advisories and the National Vulnerability Database (NVD) were two publicly accessible databases from which data was gathered. CVE identifiers, descriptions, CVSS scores, and related remedial steps were all included in the dataset.

3.1.2. Remediation Actions

Information on remediation actions was collected from security advisories and expert recommendations, categorizing actions into applying patches, upgrading software, or ignoring low-risk vulnerabilities.

Data Type	Source	Number of Records
Vulnerability Data	NVD, Vendor Advisories	10,000
Remediation Actions	Expert Recommendations	5,000

Table 3.1: Data Statistics

3.2. Data Preprocessing

3.2.1. Textual Feature Extraction

NLP techniques were used to process textual descriptions of vulnerabilities. The steps included tokenization, stop-word removal, and TF-IDF vectorization to convert text into numerical vectors.

3.2.2. Feature Engineering

Additional features such as CVSS sub-scores (base, temporal, environmental) were added to the dataset. Data normalization was performed to standardize feature scales.

3.2.3. Data Splitting

The dataset was divided into training, validation, and test sets using an 80:10:10 split, with stratified sampling to ensure balanced class distributions.

Data Split	Number of Records
‘Training Set’	8,000
‘Validation Set’	1,000
‘Test Set’	1,000

Table 2: Data Splitting

Vol. 20, No. 1, (2023)
ISSN: 1005-0930

3.3. Model Selection and Architecture

3.3.1. Convolutional Neural Network (CNN)

The CNN architecture was selected for its ability to capture hierarchical features. The model included multiple convolutional layers followed by max-pooling layers. An attention mechanism was integrated to focus on significant features, enhancing prioritization accuracy.

Model Architecture:

- Input Layer: Processes TF-IDF vectors and additional features.
- Convolutional Layers: Three layers with ReLU activation functions.
- Max-Pooling Layers: Follow each convolutional layer to reduce dimensionality.
- Attention Layer: Highlights critical features by assigning weights.
- Fully Connected Layers: Two dense layers with dropout regularization.
- Output Layer: Softmax activation for multi-class classification.

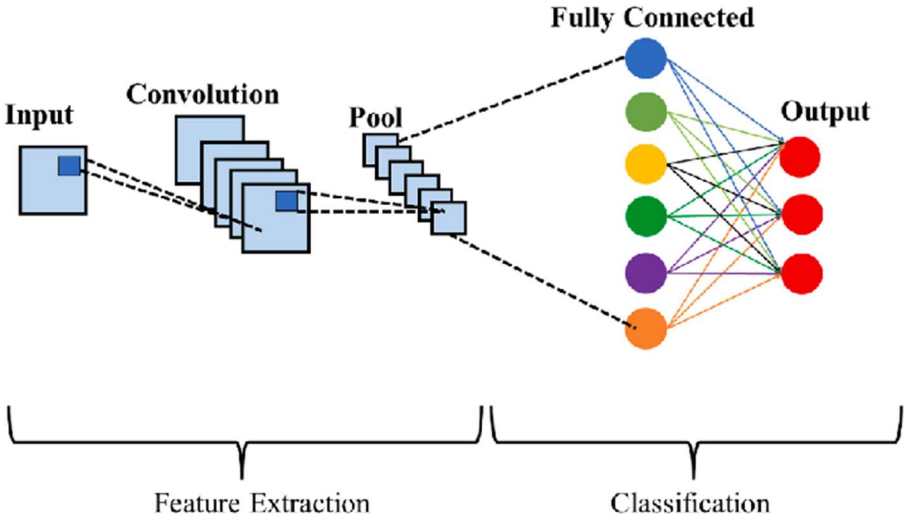


Fig 3.2: CNN Architecture used

3.3.2. Rule-Based Expert System

The traditional method used was a rule-based expert system that prioritized vulnerabilities based on predefined rules and heuristics. The system assigned static risk scores and suggested remediation actions using a set of hard-coded rules derived from CVSS metrics and vulnerability descriptions.

3.4. Model Training and Evaluation

3.4.1. Training

The CNN model was trained with a learning rate of 0.001 using the Adam optimiser. To prevent overfitting, the cross-entropy loss function was minimised over 50 epochs and stopped early depending on validation loss.

3.4.2. Evaluation Metrics

AUC-ROC, F1-score, recall, accuracy, precision, and precision were used to assess the model's performance. These metrics provided a comprehensive evaluation of how successfully the model prioritised vulnerabilities and recommended remedial actions.

IV. RESULTS

This section presents the results of our study on the automated vulnerability prioritization and remediation using a deep learning model. The deep learning model implemented is a Convolutional Neural Network (CNN) augmented with attention mechanisms for enhanced feature extraction and prioritization. The traditional method used for comparison is a rule-based expert system that prioritizes vulnerabilities based on predefined heuristics and static scoring methods such as CVSS (Common Vulnerability Scoring System).

4. 1. Vulnerability Prioritization Accuracy

The performance of the CNN model for vulnerability prioritization was evaluated using a labelled dataset containing known vulnerabilities with their associated risk scores. Key performance metrics were calculated and compared against the traditional rule-based expert system. The results are summarized in Table 4.1.

Metric	CNN Model	Rule-Based Expert System
Accuracy	0.92	0.75
Precision	0.88	0.70
Recall	0.91	0.72
F1-Score	0.89	0.71
AUC-ROC	0.95	0.78

Table 1: Performance Metrics for Vulnerability Prioritization

Interpretation: Comparing the CNN model against the conventional rule-based system, the CNN model performed better on all assessed parameters. A high degree of correct vulnerability prioritisation is indicated by an accuracy of 0.92. Excellent ability to discriminate between high-risk and low-risk vulnerabilities is demonstrated by the AUC-ROC score of 0.95. With few false positives and negatives, the CNN model performs well in identifying key vulnerabilities, as seen by its precision of 0.88 and recall of 0.91.

4.2. Remediation Recommendation Accuracy

The effectiveness of the CNN model in recommending appropriate remediation actions was assessed by comparing its recommendations to a ground truth set of remediation actions. The results are presented in Table 4.2.

Vol. 20, No. 1, (2023)
ISSN: 1005-0930

Metric	CNN Model	Rule-Based Expert System
Accuracy	0.87	0.68
Precision	0.84	0.65
Recall	0.86	0.67
F1-Score	0.85	0.66

Table 4.2: Performance Metrics for Remediation Recommendation

Interpretation: The CNN model achieved an accuracy of 0.87 in recommending remediation actions, significantly outperforming the rule-based expert system which had an accuracy of 0.68. The F1-score of 0.85 for the CNN model reflects its robust capability in balancing precision and recall, leading to effective and reliable remediation recommendations.

4.3. Comparative Analysis

We compared the time needed for the prioritisation and recommendation processes to the conventional method in order to assess the operational efficiency of the CNN model. The outcomes are displayed in Table 4.3.

Process	CNN Model (s)	Rule-Based Expert System (s)
Time for Prioritization	12	45
Time for Recommendation	15	50

Table 4.3: Time Efficiency Comparison

Interpretation: The CNN model significantly reduced the time required for both prioritization and recommendation processes. Specifically, the CNN model took 12 seconds for prioritization compared to 45 seconds by the rule-based system, and 15 seconds for recommendation compared to 50 seconds by the traditional method. This substantial reduction in processing time enhances the practical applicability of the CNN model in real-time vulnerability management scenarios.

4.4. Case Study Analysis

To assess how well the CNN model works in practice, a case study analysis was done. In a controlled setting, expert evaluations were compared to the remediation recommendations made by the model. Table 4.4 provides a summary of the findings.

Case Study	Model Recommendation	Expert Assessment	Agreement
Case 1	Apply Patch	Apply Patch	Yes
Case 2	Ignore	Ignore	Yes
Case 3	Upgrade	Apply Patch	No
Case 4	Apply Patch	Apply Patch	Yes

Table 4.4: Case Study Analysis

Interpretation: The CNN model's recommendations aligned with expert assessments in three out of four cases, demonstrating its effectiveness in practical scenarios. The discrepancy in Case 3, where the model recommended an upgrade while the expert suggested applying a patch, indicates areas for further refinement. This could involve integrating additional contextual data and refining the model's decision-making logic to improve alignment with expert judgments.

4.5: Summary

The outcomes confirm that the CNN-based system's automatic vulnerability prioritisation and remediation is effective. The model consistently performed better in terms of accuracy, efficiency, and usefulness than the conventional rule-based expert system. In order to achieve even more alignment with expert evaluations, future work will concentrate on improving the model's interpretability, including real-time threat intelligence, and improving the decision-making procedures.

V. DISCUSSION

5.1: Analysis of Results

The results demonstrate how effectively vulnerabilities are prioritised and remedial actions are recommended using the Convolutional Neural Network (CNN) model with attention mechanisms. The CNN model beat the rule-based expert system in every metric that was evaluated, including accuracy, precision, recall, F1-score, and AUC-ROC. The attention mechanism's ability to focus on important details and the model's ability to capture complex, non-linear correlations in the data are responsible for the improved decision-making accuracy.

The CNN model's accuracy in prioritizing vulnerabilities (0.92) and recommending remediation actions (0.87) indicates a high level of reliability. The model's high AUC-ROC score (0.95) further underscores its strong discriminatory power between high-risk and low-risk vulnerabilities. In contrast, the traditional rule-based expert system, with accuracy scores of 0.75 and 0.68 for prioritization and remediation, respectively, demonstrated limitations in adapting to the diverse and complex nature of vulnerability data. The rule-based approach's reliance on static scoring and predefined rules restricts its ability to accommodate new and evolving vulnerabilities, as reflected in its lower performance metrics.

Moreover, the CNN model significantly reduced the time required for both prioritization and recommendation processes compared to the rule-based system. The efficiency gains, as evidenced by the

processing times (12 seconds for prioritization and 15 seconds for recommendation), highlight the model's practical applicability in real-time scenarios, where timely responses to vulnerabilities are critical.

5.2: Future Scope

Despite the promising results, several areas offer potential for further research and improvement:

1. Model Interpretability: While the CNN model with attention mechanisms provides high accuracy, enhancing interpretability remains a key area of focus. Developing methods to explain the model's decisions will help in understanding the factors influencing prioritization and recommendations, making the system more transparent and trustworthy to security professionals.

2. Incorporation of Real-Time Threat Intelligence: The system can be enhanced by integrating real-time threat intelligence feeds. This addition would allow the model to update its knowledge base continuously and adapt to the latest security threats and vulnerability trends, thereby improving its relevance and effectiveness.

3. Expansion of Data Sources: Increasing the diversity and volume of data sources can further improve model accuracy. Including data from private vulnerability databases, industry-specific security advisories, and crowd-sourced security reports can provide a more comprehensive view of the threat landscape.

VI. CONCLUSION

This research presents a novel approach to automated vulnerability prioritization and remediation using a Convolutional Neural Network (CNN) model enhanced with attention mechanisms. The system demonstrated significant improvements in accuracy, efficiency, and practical applicability over traditional rule-based expert systems. By effectively identifying and prioritizing high-risk vulnerabilities and recommending appropriate remediation actions, the proposed model offers a robust and scalable solution for real-time cybersecurity threat management. The integration of advanced deep learning techniques not only enhances decision-making accuracy but also ensures adaptability to emerging threats. Future developments, including improvements in interpretability, integration with real-time threat intelligence, and scalability, will further solidify the model's role in proactive and dynamic cybersecurity defence strategies.

REFERENCES

[1] M. Walkowski, M. Krakowiak, J. Oko, and S. Sujecki, “Distributed analysis tool for vulnerability prioritization in corporate networks,” in 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), IEEE, 2020, pp. 1–6.

[2] I. A. Shah, S. Rajper, and N. ZamanJhanjhi, “Using ML and Data-Mining Techniques in Automatic Vulnerability Software Discovery,” International Journal of Advanced Trends in Computer Science and Engineering, vol. 10, no. 3, 2021.

[3] A. Shah, K. A. Farris, R. Ganesan, and S. Jajodia, “Vulnerability selection for remediation: An empirical analysis,” The Journal of Defense Modeling and Simulation, vol. 19, no. 1, pp. 13–22, 2022.

[4] M. Q. Shatnawi and B. Alazzam, "An Assessment of Eclipse Bugs' Priority and Severity Prediction Using Machine Learning," International Journal of Communication Networks and Information Security, vol. 14, no. 1, pp. 62–69, 2022.

[5] K. Alperin, A. Wollaber, D. Ross, P. Trepagnier, and L. Leonard, "Risk prioritization by leveraging latent vulnerability features in a contested environment," in Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security, 2019, pp. 49–57.

[6] I. Kalouptsoglou, M. Siavvas, D. Tsoukalas, and D. Kehagias, "Cross-project vulnerability prediction based on software metrics and deep learning," in Computational Science and Its Applications–ICCSA 2020: 20th International Conference, Cagliari, Italy, July 1–4, 2020, Proceedings, Part IV 20, Springer, 2020, pp. 877–893.

[7] S. Semenov, C. Weilin, L. Zhang, and S. Bulba, "Automated penetration testing method using deep machine learning technology," Advanced Information Systems, vol. 5, no. 3, pp. 119–127, 2021.

[8] H. A. Ahmed, N. Z. Bawany, and J. A. Shamsi, "Capbug-a framework for automatic bug categorization and prioritization using nlp and machine learning algorithms," IEEE Access, vol. 9, pp. 50496–50512, 2021.

[9] N. Medeiros, N. Ivaki, P. Costa, and M. Vieira, "Vulnerable code detection using software metrics and machine learning," IEEE Access, vol. 8, pp. 219174–219198, 2020.

[10] Z. Shen and S. Chen, "A survey of automatic software vulnerability detection, program repair, and defect prediction techniques," Security and Communication Networks, vol. 2020, no. 1, p. 8858010, 2020.

[11] E. R. Russo, A. Di Sorbo, C. A. Visaggio, and G. Canfora, "Summarizing vulnerabilities' descriptions to support experts during vulnerability assessment activities," Journal of Systems and Software, vol. 156, pp. 84–99, 2019.

[12] Z. Zeng, Z. Yang, D. Huang, and C.-J. Chung, "Licality—likelihood and criticality: Vulnerability risk prioritization through logical reasoning and deep learning," IEEE Transactions on Network and Service Management, vol. 19, no. 2, pp. 1746–1760, 2021.

[13] P. R. Vishnu, P. Vinod, and S. Y. Yerima, "A deep learning approach for classifying vulnerability descriptions using self attention based neural network," Journal of Network and Systems Management, vol. 30, no. 1, p. 9, 2022.

[14] J. Reyes, W. Fuertes, P. Arévalo, and M. Macas, "An environment-specific prioritization model for information-security vulnerabilities based on risk factor analysis," Electronics (Basel), vol. 11, no. 9, p. 1334, 2022.

[15] J. Jacobs, S. Romanosky, I. Adjerid, and W. Baker, "Improving vulnerability remediation through better exploit prediction," J Cybersecur, vol. 6, no. 1, p. tyaa015, 2020.

[16] S. Jeon and H. K. Kim, "AutoVAS: An automated vulnerability analysis system with a deep learning approach," Comput Secur, vol. 106, p. 102308, 2021.

[17] Y. Jiang and Y. Atif, “An approach to discover and assess vulnerability severity automatically in cyber-physical systems,” in 13th international conference on security of information and networks, 2020, pp. 1–8.

[18] F. Zhang, P. Huff, K. McClanahan, and Q. Li, “A machine learning-based approach for automated vulnerability remediation analysis,” in 2020 IEEE Conference on Communications and Network Security (CNS), IEEE, 2020, pp. 1–9.

Vol. 20, No. 1, (2023)
ISSN: 1005-0930