APTISI Transactions on Management (ATM)
Vol. 10, No. 1, January 2026, pp. 105∼116
E-ISSN: 2622-6804 | P-ISSN: 2622-6812, DOI: 10.33050

A Data Driven Information System for Cybersecurity Vulnerability Management

Qurotul Aini[1], Agung Rizky[2*], Suca Rusdian[3], Azwani Aulia[4], Archa Erica[5]
[1]Faculty of Information Technology, Satya Wacana Christian University, Indonesia
[2]Faculty of Sains and Technology, University of Raharja, Indonesia
[3]Department of Management, Yasa Anggana College of Economics, Indonesia
[4]Department of Accounting, Padjadjaran University, Indonesia
[5]Department of Management, Adi-Journal Incorporation, United States
[1]aini@raharja.info, [2]agungrizky@raharja.info,[3]sucarusdian@stieyasaanggana.ac.id, [4]azwaniaulia@gmail.com,
[5]archaca@adi-journal.org
***Corresponding Author**

Article Info

Article history:

Received January 04, 2026
Revised January 25, 2026
Accepted January 28, 2026

Keywords:

Information Systems
Predictive Analytics
Cybersecurity Vulnerability Management
Machine Learning

ABSTRACT

The rapid growth of digital infrastructures has amplified cybersecurity vulnerabilities, challenging organizations to manage risks effectively. Traditional vulnerability assessment methods, such as static scoring systems, often overlook dynamic threat information, leading to sub optimal prioritization. This study addresses the **gap** in existing vulnerability management approaches by introducing a data-driven framework that combines internal system data, public vulnerability databases, and external threat intelligence using predictive analytics. The proposed decision support information system employs machine learning as an analytical component to estimate the likelihood of vulnerability exploitation and support vulnerability prioritization decisions. The **novelty** of this approach lies in its ability to prioritize vulnerabilities not only based on technical severity but also considering the context of real-world threat activity. When bench marked against conventional methods, this approach demonstrates superior performance in identifying exploitable vulnerabilities, improving accuracy and recall, thus optimizing resource allocation. By adopting a proactive, risk-based strategy, the framework **prioritizes** the most critical vulnerabilities in complex IT environments. The **results** highlight the potential of predictive models in enhancing cybersecurity management and supporting sustainable infrastructure, driving a shift toward more efficient, data-driven decision-making.

Corresponding Author:

DOI: https://doi.org/10.33050/atm.v10i1.2600

1. INTRODUCTION

The rapid expansion of digital infrastructures and increased reliance on interconnected systems have intensified the cybersecurity threat landscape for modern organizations [1, 2]. The growing complexity of software architectures, frequent system updates, and the widespread adoption of cloud and distributed environments have resulted in an overwhelming number of vulnerabilities that must be continuously managed [3, 4]. In this context, effective vulnerability assessment and prioritization are essential to cybersecurity risk management [5, 6]. Organizations must identify which weaknesses pose the most immediate and severe threats to

operational continuity, making data-driven vulnerability assessment crucial [7, 8]. This research aligns with SDGs 9 on building resilient infrastructure and promoting sustainable industrial growth by advancing the technology needed for secure digital environments. Despite advancements in vulnerability assessment techniques, many organizations lack an information system that can integrate heterogeneous security data and support organizational decision-making for vulnerability prioritization. These methods often evaluate vulnerabilities in isolation, failing to incorporate contextual factors like asset criticality, data driven, network exposure, and evolving threat intelligence [9, 10]. As a result, data driven security teams may focus on vulnerabilities with high scores while neglecting lower-scored but actively exploited vulnerabilities, leading to inefficient patch management, increased costs, and prolonged exposure to risks. This issue relates to SDGs 16, which emphasizes the role of cybersecurity in strengthening institutions by ensuring secure digital systems that foster transparency and accountability.

Previous research has explored the use of data analytics and machine learning in cybersecurity; however, from an Information Systems perspective, limited attention has been given to vulnerability management as a decision support problem requiring system-level integration of data, models, and organizational context. However, many studies focus on isolated data sources or narrow analytical tasks, limiting support for comprehensive vulnerability prioritization [11]. This study proposes a novel data-driven framework that integrates diverse data sources and applies machine learning to predict vulnerability exploitability [12]. By factoring in contextual elements such as asset importance and network exposure, the framework generates a more accurate vulnerability score [13]. This approach contributes to cybersecurity management by demonstrating how data-driven, context-aware methods can enhance vulnerability prioritization and promote a proactive, risk-based strategy, aligning with SDGs 9 and SDGs 16 through improved digital security and risk management.

From an Information Systems perspective, cybersecurity vulnerability management represents a complex organizational decision-making problem rather than a purely technical security task. Accordingly, this study positions vulnerability assessment as a decision support information system that integrates heterogeneous security data, analytical models, and organizational context to support risk-based vulnerability prioritization.

2. LITERATURE REVIEW

Vulnerability assessment has traditionally relied on standardized scoring systems, penetration testing, and static code analysis to evaluate the severity of security weaknesses in information systems [14, 15]. Among these methods, the Common Vulnerability Scoring System (CVSS) is the most widely adopted due to its standardized metrics and ease of interpretation [16, 17]. CVSS allows organizations to rank vulnerabilities based on predefined severity criteria. However, prior studies have consistently highlighted its limitations in practical risk management [18, 19]. Specifically, CVSS evaluates vulnerabilities in isolation and fails to consider organizational context, exploit availability, or evolving threat conditions. This issue is particularly relevant in modern cybersecurity environments, where vulnerabilities are dynamic and context-dependent [20, 21]. As a result, vulnerabilities with high CVSS scores may not pose immediate risks, while those with lower scores that are actively exploited may be overlooked, leading to inefficient prioritization and remediation [22, 23].

To address these limitations, risk-based decision-making and predictive analytics frameworks have emerged as alternatives [24, 25]. These models emphasize the importance of contextual data, helping organizations better allocate resources to vulnerabilities with the highest likelihood of exploitation [26, 27]. This shift towards data-driven decision-making supports more adaptive and real-time assessment methods. The increasing availability of large-scale cybersecurity datasets has accelerated the use of machine learning techniques for threat detection and prediction [28, 29]. Models such as Random Forest, Gradient Boosting, and deep learning architectures have been applied to tasks including intrusion detection, malware classification, and exploit prediction [30, 31]. These algorithms can identify complex patterns that rule-based methods may miss. Machine learning also enables the detection of non-linear relationships between system vulnerabilities and exploitability, facilitating more precise prioritization. Several established cybersecurity frameworks, including the NIST Cybersecurity Framework and the MITRE ATT & CK framework, offer guidance for managing cyber risks and understanding adversary tactics and techniques [32, 33]. These frameworks are commonly used for strategic planning, threat modeling, and mapping security controls. However, they are not designed for quantitative vulnerability prioritization or predictive exploitability assessment.

While they provide valuable structure for understanding threats, they rely on external analytical tools for data-driven decision-making. Existing frameworks are not sufficient for real-time, risk-based vulnerability

management. The literature suggests that integrating predictive analytics with these frameworks could enhance their effectiveness, yet no solution has fully combined these elements into a unified, actionable vulnerability assessment system. This study fills this gap by proposing an integrated, data-driven framework that merges predictive analytics with contextual risk assessment, extending existing research to create a more effective approach to vulnerability prioritization. By combining internal system data, public vulnerability repositories, and external threat intelligence, the framework generates a more accurate vulnerability score that moves beyond static scoring systems.

From an Information Systems perspective, prior studies have largely emphasized technical models and analytical accuracy, with limited focus on vulnerability management as an organizational information system that supports managerial decision-making. This study extends the Information Systems literature by conceptualizing vulnerability prioritization as a decision support system that integrates data, analytical models, and organizational context into a unified decision-making framework.

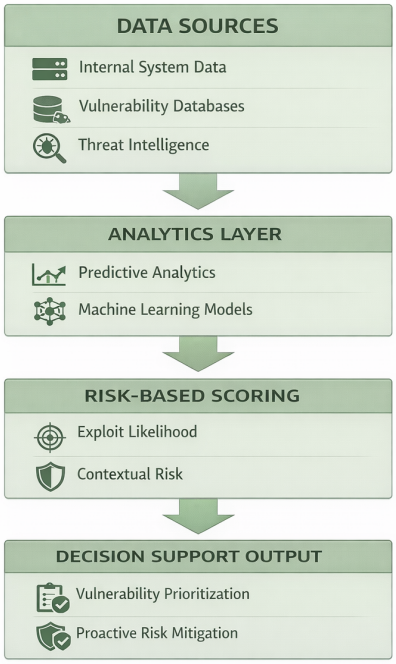

Figure 1. Data Driven Vulnerability Prioritization Framework

Figure 1 illustrates a high-level data-driven vulnerability prioritization framework that integrates multiple security data sources, including internal system data, vulnerability databases, and threat intelligence. Through an analytics layer based on predictive analytics and machine learning, the framework produces a risk-based scoring mechanism that evaluates vulnerabilities according to their likelihood of exploitation and contextual risk [34, 35]. This approach supports a proactive and context-aware decision-making process by enabling organizations to prioritize vulnerabilities more effectively and focus on those that pose the greatest potential risk. Rather than relying on reactive remediation, the framework emphasizes decision support for proactive risk mitigation in dynamic IT environments, contributing to more efficient and strategic vulnerability management [36, 37].

3. RESEARCH METHODOLOGY

3.1. Research Design

The study adopts a quantitative and data-driven research design aimed at developing and evaluating a comprehensive cybersecurity vulnerability assessment framework. This research focuses on the design and evaluation of a decision support information system for cybersecurity vulnerability management, where predictive analytics are embedded to support organizational decision-making. The experimental approach is employed to validate the framework's performance by comparing it with traditional methods using historical

cybersecurity incident data. To ensure robustness and generalizability, the design emphasizes the integration of both internal system data and external data sources. The framework's predictive accuracy and its ability to prioritize vulnerabilities are assessed to demonstrate its effectiveness in real-world applications. The methodology includes a comparative analysis between the newly proposed framework and traditional systems like the CVSS, which has historically been used to rank vulnerabilities. This allows the study to establish how the framework improves vulnerability prioritization and resource allocation compared to conventional methods.

3.2. Framework Architecture

From an Information Systems perspective, the proposed framework is conceptualized as a decision support information system designed to support organizational decision-making for cybersecurity vulnerability prioritization. In today rapidly evolving digital landscape, organizations face increasingly complex and diverse cybersecurity risks [38, 39]. A traditional, static vulnerability scoring system often fails to provide the actionable insights needed for effective prioritization. As a solution, this framework integrates a variety of data sources, advanced predictive analytics, and context-aware factors to offer a more accurate and dynamic method for identifying and prioritizing vulnerabilities that pose the greatest threat to an organization [40, 41].

Within the proposed decision support information system, collected data undergoes preprocessing and feature engineering to prepare analytical inputs for vulnerability prioritization decisions. This involves cleaning the data by removing incomplete or duplicate records, normalizing numerical features to standardize ranges, and encoding categorical variables into formats suitable for machine learning. The feature engineering process further refines the data by creating indicators such as exploit availability, vulnerability age, and historical attack frequency, which serve as key predictors for machine learning models. These engineered features are crucial for enhancing the predictive accuracy of the framework.

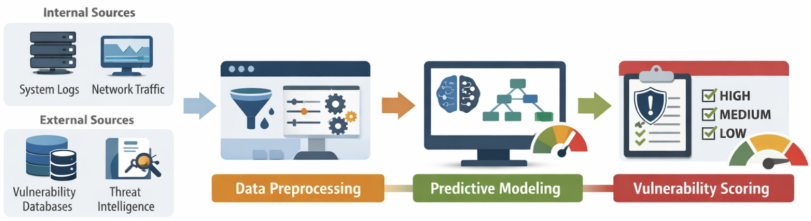

Figure 2. Cybersecurity Vulnerability Assessment Framework

Figure 2 above provides an overview of the framework used in this study. It is divided into four primary stages:

- Data Acquisition.
- Data Preprocessing.
- Predictive Modeling.
- Vulnerability Scoring.

The data acquisition stage focuses on gathering information from internal sources, such as system logs and network traffic, in addition to external sources like vulnerability databases and threat intelligence feeds. The preprocessing phase transforms raw data into structured features suitable for analysis by cleaning and normalizing the data, while feature engineering identifies key indicators like exploit availability and historical attack frequency. These features are crucial for feeding into the machine learning model, which predicts the likelihood of vulnerability exploitation. Finally, the framework's predictive modeling uses machine learning techniques, such as Random Forest, to estimate the exploitability of vulnerabilities. The output from this model is integrated with contextual factors such as asset criticality and network exposure, producing a comprehensive vulnerability score.

3.3. Data Collection and Preprocessing

The data collection process combines both internal and external sources, creating a rich dataset that enhances vulnerability assessment. Internal data is collected from sources such as system logs and network

traffic records, offering critical insights into system activities, potential weaknesses, and the organization's overall exposure. These internal sources provide context for understanding the existing infrastructure, helping identify and prioritize vulnerabilities [42]. Meanwhile, external data from sources like vulnerability databases (e.g., CVE, NVD) and threat intelligence feeds provide a broader perspective on emerging risks and real-time updates on known threats, exploits, and attacks.

Following the data collection phase, preprocessing is essential to prepare the dataset for analysis. This phase involves data cleaning, such as removing incomplete or duplicate records, ensuring that the dataset is reliable and accurate [43]. Normalization of numerical features (e.g., severity scores, frequency of attacks) standardizes the data, while categorical variables (e.g., system type, vulnerability class) are encoded to make them compatible with machine learning models. These preprocessing steps ensure that the dataset is consistent and ready for effective analysis.

In the feature engineering stage, relevant indicators are extracted from the data, such as vulnerability age, exploit availability, asset exposure level, and historical attack frequency. These features are crucial for assessing the likelihood of vulnerabilities being exploited, which feeds directly into the machine learning model. By refining the dataset, this phase improves the predictive capabilities of the framework, enabling it to make more accurate assessments and prioritize vulnerabilities for remediation effectively. To further improve data quality, a consistency check is applied across internal and external sources to resolve discrepancies in vulnerability identifiers and timestamps. Records referring to the same vulnerability from different sources are merged using standardized identifiers, ensuring that each vulnerability instance is represented accurately. This integration process reduces redundancy and enhances the completeness of the dataset, allowing the framework to capture both technical characteristics and real-world threat context in a unified representation.

In addition, basic statistical analysis is conducted during preprocessing to examine data distribution and detect potential class imbalance between exploited and non-exploited vulnerabilities. When imbalance is observed, resampling techniques are applied to prevent model bias toward majority classes assessment framework. This step ensures that the predictive model is trained on balanced and representative data, thereby strengthening its ability to generalize across different vulnerability scenarios and improving the reliability of subsequent prioritization results.

Table 1. Main Data and Data Collection Process

Data Type	**Source**	**Description**
Internal Data	System Logs	Records system activities, providing insights into system vulnerabilities and organizational exposure.
	Network Traffic Records	Offers information on data flows and communication patterns, highlighting potential network risks.
External Data	Vulnerability Databases	Provides detailed information on known vulnerabilities (e.g., CVE, NVD), offering a broader view of global threats.
	Threat Intelligence Feeds	Provides real-time updates on emerging threats, exploits, and attacks, helping assess potential risks.

The combination of internal and external data sources, as shown in Table 1, plays a pivotal role in creating a well-rounded view of cybersecurity vulnerabilities. These diverse data inputs allow for a more dynamic and informed approach to vulnerability prioritization, ensuring that resources are allocated effectively to mitigate the most pressing risks. The preprocessing and feature engineering steps further ensure that the dataset is structured and ready for machine learning, significantly enhancing the accuracy and efficiency of the vulnerability assessment framework process.

3.4. Predictive Model Development

The predictive model is developed using the Random Forest classifier, chosen for its ability to handle high dimensional data and its robustness to noisy inputs. The model predicts the likelihood of a vulnerability being exploited based on features such as exploit availability and historical attack frequency [44]. This

approach allows for probabilistic scoring of vulnerabilities, aiding in prioritization. Hyperparameter tuning is performed using cross-validation to optimize model performance and reduce overfitting. This ensures the model performs well across different datasets and remains generalizable to various cybersecurity environments. Cross-validation helps to fine-tune the model by evaluating its performance on different subsets of the data. The model's effectiveness is evaluated using accuracy, precision, recall, and F1-score, with an emphasis on recall, which is crucial in identifying high-risk vulnerabilities. These metrics offer insights into the model's ability to correctly identify vulnerabilities that pose a significant threat to organizational security.

In addition to model selection and tuning, feature importance analysis is conducted to better understand the contribution of each input variable to the prediction results. By examining the relative influence of features such as exploit availability, vulnerability age, and historical attack patterns, the model provides interpretability regarding which factors most strongly affect exploitation likelihood. This analysis supports transparency in decision making and helps security analysts validate whether the model's predictions align with known threat behaviors. Moreover, understanding feature relevance enables further refinement of the framework by eliminating redundant variables and improving computational efficiency without sacrificing predictive accuracy. To enhance robustness, the predictive model is also tested under different data distribution scenarios to evaluate its stability in practical environments. Sensitivity analysis is applied to assess how changes in input features influence the predicted exploitation probability.

3.5. Vulnerability Scoring Mechanism

The vulnerability scoring mechanism integrates the output of the predictive model with contextual risk factors. These factors include asset criticality, network exposure, and organizational impact, ensuring that the prioritization process accounts for both technical severity and the potential operational consequences of an exploited vulnerability. By weighting the predicted exploit probability against the contextual factors, the framework generates a composite vulnerability score that offers a dynamic and context-aware approach to vulnerability prioritization. This method ensures that vulnerabilities with high exploitability and significant organizational impact are given higher priority, allowing for more effective use of security resources. The framework is designed to go beyond static scoring systems like CVSS, which do not incorporate contextual information. The inclusion of dynamic factors ensures that vulnerabilities are ranked based on both technical and real-world operational risk, providing a more comprehensive vulnerability prioritization system.

4. RESULT AND DISCUSSION

Performance of the Predictive Model From an Information Systems perspective, the performance of the proposed decision support system was evaluated in terms of its ability to improve decision quality in vulnerability prioritization using a hold-out test dataset composed of historical vulnerability exploitation records. Standard classification metrics, such as Accuracy, Precision, Recall, and F1-Score, were employed to assess the model's predictive effectiveness. From an Information Systems perspective, the system demonstrates its ability to improve decision quality by prioritizing vulnerabilities that are more likely to be exploited in real-world contexts. This indicates the model's ability to accurately identify vulnerabilities that are likely to be exploited.

The high recall value is particularly significant in cybersecurity, as it highlights the model's capacity to detect exploitable vulnerabilities, thus minimizing the risk of false negatives. Missing high-risk vulnerabilities is a critical issue in cybersecurity, as it may lead to severe security incidents. The strong precision also indicates that the model is capable of reducing false positives, thereby ensuring that the vulnerabilities flagged as critical truly represent potential security risks.

Table 2. Model Demonstrates

Metric	Value
Accuracy	0.91
Precision	0.89
Recall	0.93
F1-Score	0.91

Table 2 above, while the accuracy of 0.91 is promising, further analysis is required to understand the model's performance under various operational conditions. For instance, the model's ability to perform on imbalanced datasets or datasets containing rare vulnerabilities should be explored further. This is particularly

important in real-world cybersecurity scenarios, where such data conditions are common. Additionally, it is essential to investigate the generalizability of the model across different types of organizational environments. The current results are based on a specific set of cybersecurity incidents, and their performance might vary when applied to datasets from different industries or organizations. Thus, validating the model on more diverse datasets will strengthen its practical application. Finally, the ability of the Random Forest model to capture complex, non-linear relationships between vulnerability characteristics and exploitation likelihood sets it apart from simpler rule-based systems. This advantage allows the framework to perform better in identifying vulnerabilities that may be overlooked by traditional methods like CVSS, which rely on static scoring mechanisms.

4.1. Comparison with Traditional CVSS-Based Prioritization

To assess the practical effectiveness of the proposed framework, vulnerability prioritization results were compared with the rankings generated using the traditional CVSS-based scoring system. The comparison revealed that the proposed framework outperformed CVSS by successfully identifying a higher proportion of vulnerabilities that were exploited in real-world incidents. This is particularly evident in the top-ranked vulnerabilities, where the proposed framework identified 8 out of the top 10 vulnerabilities as exploited, compared to only 5 identified by the CVSS approach.

Table 3. Based Scoring System

Scoring Approach	Exploited Vulnerabilities Top 10	Precision
CVSS-Based Ranking	5	0.50
Proposed Framework	8	0.80

Table 3 demonstrates this improvement in precision. The CVSS-based ranking yielded a precision score of 0.50, while the proposed framework achieved 0.80, indicating a more accurate prioritization of vulnerabilities based on their actual exploitation history. The framework's ability to leverage threat intelligence and contextual risk factors significantly improved its performance over the traditional static approach. The comparison also highlighted that several vulnerabilities with moderate CVSS scores, but which were actively exploited, were ranked higher by the proposed framework. This shift is a direct result of the framework's dynamic prioritization mechanism, which factors in real-time threat intelligence and asset criticality, offering a more relevant and actionable score than CVSS alone. Moreover, the CVSS system failure to account for organizational-specific data, such as network exposure or asset importance, makes it less effective in real-world settings. In contrast, the proposed framework context-aware scoring ensures that vulnerabilities critical to an organization operations are prioritized, even if they receive moderate CVSS scores [45, 46]. This comparative analysis also reinforces the idea that static scoring systems like CVSS may mislead security teams into focusing on vulnerabilities that, while severe, are less likely to be exploited in the near future [47, 48]. The proposed framework incorporation of dynamic threat intelligence and contextual awareness ensures more proactive, risk-based vulnerability management, which is crucial for modern cybersecurity strategies.

4.2. Interpretation of Findings

The superior performance of the proposed framework can be attributed to its ability to integrate predictive exploitability analysis with contextual risk information. Unlike CVSS, which provides a static severity score based on predefined criteria, the proposed approach evaluates vulnerabilities dynamically, considering real-world threat activity and the organization's exposure. By incorporating asset criticality, network exposure, and threat intelligence, the framework ensures that vulnerabilities with the highest likelihood of exploitation are prioritized. One of the key advantages of the proposed framework is its capacity to capture complex, non-linear relationships between vulnerability characteristics and exploitation likelihood. This is a critical step forward, as traditional rule-based systems cannot easily represent these relationships. The use of machine learning models like Random Forest allows the framework to adapt to new, unseen patterns, ensuring that vulnerability prioritization remains accurate and relevant over time.

Additionally, the framework benefits from the ability to continuously learn and incorporate new data, ensuring that vulnerability prioritization stays up-to-date with emerging threats. This is in stark contrast to traditional systems, which are limited by their static nature and fail to account for changes in the threat landscape or an organization's operational context. As cybersecurity threats evolve, the ability of the framework to integrate live threat intelligence allows for a more responsive and agile approach to vulnerability management.

Another significant improvement is the ability to assess exploitability in the context of organizational risk. By considering not only the likelihood of exploitation but also the impact of a vulnerability on the organization's assets and operations, the proposed framework aligns vulnerability prioritization with overall cybersecurity strategy and risk management goals. This makes it a more effective tool for For Chief Information Security Officers (CISOs) who need to allocate limited resources to the most critical vulnerabilities [49, 50].

From a practical perspective, the proposed framework offers several advantages that allow organizations to shift from reactive vulnerability management to a proactive, risk-based strategy. By incorporating dynamic threat intelligence and contextual risk factors, security teams can allocate resources more effectively, focusing on vulnerabilities with the highest likelihood of exploitation and greatest potential impact on organizational operations. This proactive approach also allows organizations to stay ahead of emerging threats, rather than responding only when a vulnerability is actively exploited. For example, vulnerabilities that may have gone unnoticed using traditional methods like CVSS could be flagged by the proposed framework due to the integration of threat intelligence, giving organizations a head start on patching or mitigating potential risks before an attack occurs. CISOs and other decision-makers, the framework provides a data-driven decision-support tool that enhances situational awareness. This tool enables security teams to make informed decisions about which vulnerabilities to address first, reducing the likelihood of a breach and improving overall cyber resilience. However, there are several limitations to the study. First, the dataset used for evaluation is limited to specific data sources and time periods, which may affect its applicability to different industries or threat environments. The framework's effectiveness also depends on the quality and timeliness of threat intelligence feeds, which can vary across organizations. Future research should aim to expand the dataset and explore real-time data integration to further test the framework's scalability. Lastly, while the framework demonstrates strong performance, it is important to recognize that no system is perfect. The model may still face challenges with certain types of vulnerabilities, particularly those that are newly discovered or rarely exploited. Future research should focus on enhancing the model's ability to handle such edge cases and improve its robustness in diverse operational contexts.

5. MANAGERIAL IMPLICATIONS

5.1. Proactive Vulnerability Management

The proposed decision support information system represents a significant shift from reactive to proactive vulnerability management by enhancing managerial situational awareness and supporting evidence-based cybersecurity decision-making. By leveraging predictive analytics and contextual risk factors, the framework enables organizations to identify vulnerabilities that are most likely to be exploited in the near future rather than relying solely on static severity scores. This allows security teams to anticipate potential threats and address critical weaknesses before they escalate into serious security incidents, thereby strengthening overall organizational preparedness.

CISOs and cybersecurity practitioners, adopting this proactive approach supports timely mitigation of high-risk vulnerabilities and enhances cyber resilience. The framework also contributes to improved operational continuity by reducing exposure windows and minimizing the likelihood of disruptive attacks. In an increasingly dynamic threat landscape, the ability to act in advance of exploitation is essential for maintaining stable and secure digital operations.

5.2. Efficient Resource Allocation

One of the key managerial benefits of the proposed framework lies in its ability to improve resource allocation through risk-based prioritization. By ranking vulnerabilities according to both their probability of exploitation and the potential operational impact, the framework provides a more accurate basis for decision making compared to traditional systems that rely only on severity scores. Factors such as asset criticality and network exposure ensure that the most sensitive and vulnerable systems receive immediate attention.

Through its decision support capabilities, the proposed information system enables organizations to concentrate limited remediation resources on areas that pose the highest risk, increasing the overall efficiency of cybersecurity investments. Decision makers can allocate security budgets more strategically and avoid unnecessary remediation efforts on low-impact vulnerabilities. As a result, organizations can achieve better risk reduction outcomes while maintaining cost-effective cybersecurity operations.

5.3. Integration with Existing Cybersecurity Frameworks

Another important implication of this framework is its compatibility with existing cybersecurity strategies and governance models. Many organizations already adopt established frameworks such as NIST or MITRE ATT & CK to structure their security practices. The proposed framework complements these approaches by incorporating predictive modeling and real-time threat intelligence into vulnerability prioritization processes, thereby enhancing their analytical depth.

From a managerial perspective, this integration allows organizations to strengthen current security programs without replacing existing policies or architectures. Managers can continue to rely on familiar standards while benefiting from more adaptive and data-driven prioritization mechanisms. This alignment supports a holistic cybersecurity strategy that integrates technical controls, risk management objectives, and operational continuity requirements within a unified decision-support structure.

6. CONCLUSION

This study contributes to the Information Systems literature by proposing and evaluating a data-driven decision support system that enhances cybersecurity vulnerability management in organizational contexts. This contribution positions cybersecurity vulnerability management not merely as a technical security function, but as a core organizational information system that enhances managerial decision-making and risk governance. Motivated by the limitations of traditional vulnerability assessment approaches that rely on static and context-independent scoring mechanisms, the proposed framework integrates heterogeneous cybersecurity data sources with machine learning-based predictive analytics to support more accurate and actionable vulnerability prioritization. By combining internal system data, public vulnerability repositories, and external threat intelligence, the framework captures both technical severity and real-world threat dynamics.

The empirical evaluation demonstrates that the proposed framework outperforms conventional CVSS-based prioritization methods in identifying vulnerabilities that are likely to be exploited. The machine learning model achieved strong predictive performance, particularly in terms of recall, which is critical for minimizing missed high-risk vulnerabilities. Furthermore, the integration of contextual risk factors, such as asset criticality and network exposure, enables the framework to align vulnerability prioritization with organizational risk and operational impact, thereby enhancing the effectiveness of cybersecurity decision-making.

From a theoretical perspective, this study contributes to the cybersecurity and risk management literature by bridging predictive exploitability modeling and contextual risk assessment within a unified framework. Practically, the proposed approach supports a shift from reactive patch management toward a proactive, risk-based vulnerability management strategy, enabling organizations to allocate security resources more efficiently. Despite these contributions, the study is subject to limitations related to data scope and dependency on threat intelligence quality. Future research should explore the incorporation of real-time data streams, alternative machine learning models, and automated remediation recommendations to further enhance the adaptability and scalability of the framework. Overall, this study highlights the critical role of data-driven and context-aware approaches in strengthening organizational cyber resilience in an increasingly dynamic threat landscape.

7. DECLARATIONS

7.1. About Authors

Qurotul Aini (QA) https://orcid.org/0000-0002-7546-5721
Agung Rizky (AR) https://orcid.org/0009-0006-7046-8639
Suca Rusdian (SR) https://orcid.org/0009-0008-4805-1524
Azwani Aulia (AA) https://orcid.org/0000-0003-1333-9057
Archa Erica (AE) https://orcid.org/0009-0007-5667-7853

7.2. Author Contributions

Conceptualization: QA and AR; Methodology: SR; Software: AA and AE; Validation: AR and QA; Formal Analysis: SR and AA; Investigation: AE; Resources: QA; Data Curation: AA; Writing Original Draft Preparation: AE and SR; Writing Review and Editing: AA and QA; Visualization: SR. All authors, QA, AR, AA and AE, have read and agreed to the published version of the manuscript.

REFERENCES

[1] Y. Cheng, Z. Zhang, Y. Gao, Z. Chen, S. Guo, Q. Zhang, R. Mei, S. Nepal, and Y. Xiang, "Meltdown-type attacks are still feasible in the wall of kernel page-table isolation," *Computers & Security*, vol. 113, p. 102556, 2022.

[2] K. Charmanas, N. Mittas, and L. Angelis, "Exploitation of vulnerabilities: a topic-based machine learning framework for explaining and predicting exploitation," *Information*, vol. 14, no. 7, p. 403, 2023.

[3] P. Majocco, P. Mosch, and R. Obermaier, "Digital transformation under uncertainty–market value effects of early industry 4.0 innovation projects," *Procedia Computer Science*, vol. 232, pp. 232–241, 2024.

[4] R. Parla, "Efficacy of epss in high severity cves found in kev," *arXiv preprint arXiv:2411.02618*, 2024.

[5] U. Rahardja, Q. Aini, A. S. Bist, S. Maulana, and S. Millah, "Examining the interplay of technology readiness and behavioural intentions in health detection safe entry station," *JDM (Jurnal Dinamika Manajemen)*, vol. 15, no. 1, pp. 125–143, 2024.

[6] Y. Jiang, N. Oo, Q. Meng, H. W. Lim, and B. Sikdar, "A survey on vulnerability prioritization: Taxonomy, metrics, and research challenges," *arXiv preprint arXiv:2502.11070*, 2025.

[7] V. Koscinski, M. Nelson, A. Okutan, R. Falso, and M. Mirakhorli, "Conflicting scores, confusing signals: An empirical study of vulnerability scoring systems," in *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, 2025, pp. 1904–1918.

[8] I. Naseer, "Machine learning applications in cyber threat intelligence: a comprehensive review," *The Asian Bulletin of Big Data Management*, vol. 3, no. 2, pp. 190–200, 2023.

[9] E. D. Lonergan and J. Schneider, "The power of beliefs in us cyber strategy: The evolving role of deterrence, norms, and escalation," *Journal of Cybersecurity*, vol. 9, no. 1, p. tyad006, 2023.

[10] T. Hidayat, D. Manongga, Y. Nataliani, S. Wijono, S. Y. Prasetyo, E. Maria, U. Raharja, I. Sembiring *et al.*, "Performance prediction using cross validation (gridsearchcv) for stunting prevalence," in *2024 IEEE International Conference on Artificial Intelligence and Mechatronics Systems (AIMS)*. IEEE, 2024, pp. 1–6.

[11] N. I. of Standards, T. (US), N. I. of Standards, and T. (US), *NIST Cybersecurity Framework 2.0: Quick-start Guide for Creating and Using Organizational Profiles*. US Department of Commerce, National Institute of Standards and Technology, 2024.

[12] M. Santana, V. V. Cogo, and A. O. de Sá, "Secscore: Enhancing the cvss threat metric group with empirical evidences," *arXiv preprint arXiv:2405.08539*, 2024.

[13] N. Shimizu and M. Hashimoto, "Vulnerability management chaining: An integrated framework for efficient cybersecurity risk prioritization," *arXiv preprint arXiv:2506.01220*, 2025.

[14] S. Unger, E. Arzoglou, M. Heinrich, D. Scheuermann, and S. Katzenbeisser, "Cybersecurity risk assessment in ot systems using attack graphs: S. unger et al." *International Journal of Information Security*, vol. 25, no. 1, p. 34, 2026.

[15] H. Su, Z. Xu, Y. Zhang, and Q. Tan, "Source code vulnerability detection based on deep learning: a review," *Cybersecurity*, vol. 9, no. 1, p. 2, 2026.

[16] R. Krishnasrija, A. K. Mandal, R. Halder, and A. Cortesi, "A dynamic context-aware and role-capability based access control mechanism for internet of things," *Journal of Network and Systems Management*, vol. 34, no. 1, p. 30, 2026.

[17] A. Saighi, S. Kouah, S. Zertal, D. Meg, R. Khanfar, and Z. Laboudi, "Wmsd: A wireless multimedia security dataset and a multi-level ids with machine learning and explainable tabnet," *IEEE Access*, 2026.

[18] S. Yitagesu, Z. Xing, X. Zhang, Z. Feng, T. Bi, L. Han, and X. Li, "Systematic literature review on software security vulnerability information extraction," *ACM Transactions on Software Engineering and Methodology*, 2025.

[19] T. T. Allen, J. McCarty, M. Abdallah, and V. S. Buck, "Towards data-driven organizational cybersecurity risk metrics and optimization," in *Operations Research and Data Analytics: Current Trends and Future Perspectives: Selected Papers from International Conference on Industrial Engineering and Analytics (ICONIEA) 2024*. Springer, 2026, pp. 445–453.

[20] U. Rahardja, I. D. Hapsari, P. H. Putra, and A. N. Hidayanto, "Technological readiness and its impact on mobile payment usage: A case study of go-pay," *Cogent Engineering*, vol. 10, no. 1, p. 2171566, 2023.

[21] G. S. Varshini, S. Latha, G. R. Vikhram, and S. Padmanaban, "Detection of coordinated attack using data driven approach in cyber physical power system (cpps)," *Computers and Electrical Engineering*, vol. 131, p. 110917, 2026.

[22] M. Malkawi and R. Alhajj, "Ai-powered vulnerability detection and patch management in cybersecurity: A systematic review of techniques, challenges, and emerging trends," *Machine Learning and Knowledge Extraction*, vol. 8, no. 1, p. 19, 2026.

[23] M. S. Ansari and U. C. 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.

[24] S. Hollerer, "Integrated safety and security knowledge modeling," Ph.D. dissertation, Technische Universität Wien, 2026.

[25] A. Cahyono and Y. D. Nurcahyanie, "Identification and evaluation of logistics operational risk using the fmea method at pt. xzy," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 1Sp, pp. 1–10, 2023.

[26] M. S. Sharifi Poor Bgheshmi, M. Sharajsharifi, and M. R. Saeidabadi, "Between exploitation and resilience: Reconciling ai's role in surveillance capitalism and disaster risk management," *Journal of Cyberspace Studies*, vol. 10, no. 1, pp. 109–139, 2026.

[27] H. Turtiainen, A. Costin, and T. Hämäläinen, "Vulnberta-xai: Towards explainable ai for automating cwe weakness assignment and improving the quality of cybersecurity cve," in *Cyber Security: Policy and Technology*. Springer, 2026, pp. 385–432.

[28] R. N. Wedamuni Arachchige, D. Saxena, and A. K. Singh, "An adaptive cyber threat intelligence model to counter evolving security attacks in industrial communication networks," *Neural Computing and Applications*, vol. 38, no. 2, p. 15, 2026.

[29] B. Huda, E. Sediyono, K. D. Hartomo, I. Sembiring, A. Fauzi, and A. L. Hananto, "Evaluation quality of e-learning x using iso/iec 25010 framework and design thinking approach," in *2023 6th International Conference on Information and Communications Technology (ICOIACT)*. IEEE, 2023, pp. 114–119.

[30] E. R. Rahayu, A. Aprillia, R. Z. Ikhsan, A. Adiwijaya, and A. Kumara, "Cybersecurity in the age of iot and developing frameworks for securing smart devices and networks," *Journal of Computer Science and Technology Application*, vol. 2, no. 1, pp. 46–54, 2025.

[31] B. K. Baniya and L. K. Cherukuri, "Xgboost and random forest–based intrusion detection system," in *Cybersecurity Defensive Walls in Edge Computing*. Elsevier, 2026, pp. 105–121.

[32] Y. Cheng, X. Zhou, H. Zhao, G. Liang, F. Wen, and J. Zhao, "Secure and trustworthy energy systems: A four-layer threat model and defense-in-depth framework," *Energy*, p. 140027, 2026.

[33] D. P. Möller, *Cybersecurity for Network and Information Security: Principles, Techniques and Applications*. Springer Nature, 2026.

[34] A. Gampel, "Streamlining cybersecurity risk assessment for industrial control and automation systems: Leveraging nist's risk management framework (rmf) implemented using model-based system's engineering (mbse)," Ph.D. dissertation, The George Washington University, 2026.

[35] H. Khan and S. Akhtar, "Intelligent authentication systems for phishing attack prevention and rapid incident response," 2026.

[36] A. Alqudhaibi, M. Albarrak, A. Aloseel, A. Munshi, T. Alsharif, S. Jagtap, and K. Salonitis, "Proactive cybersecurity in industry 4.0: a survey of cybersecurity threat prediction approaches in manufacturing systems," *International Journal of Information Security*, vol. 25, no. 1, p. 14, 2026.

[37] Z. Pourzolfaghar, A. Habibi Lashkari, R. Hashemi, and M. Helfert, "Adapted cybersecurity risk analysis, assessment, and mitigation framework for smart buildings," in *Understanding Cybersecurity Management in the Construction Industry: Challenges, Strategies and Trends*. Springer, 2026, pp. 109–130.

[38] J. Manikandan, P. Hemalatha, K. Jayashree, and P. Rajeswari, "Navigating the digital landscape: Understanding, detecting, and mitigating cyber threats in an evolving technological era," *Securing Cyber-Physical Systems: Fundamentals, Applications and Challenges*, pp. 199–223, 2026.

[39] H. G. Menezes and O. M. Rete, "Digital risk management in digital transformation contexts," in *Innovation Management for Disruptive Maturity in Competitive Scenarios*. IGI Global Scientific Publishing, 2026, pp. 311–330.

[40] M. Albarrak, K. Salonitis, and S. Jagtap, "Natural language processing (nlp)-based frameworks for cyber threat intelligence and early prediction of cyberattacks in industry 4.0: a systematic literature review," *Applied Sciences*, vol. 16, no. 2, p. 619, 2026.

[41] R. Supriati, E. R. Dewi, D. Supriyanti, N. Azizah *et al.*, "Implementation framework for merdeka belajar kampus merdeka (mbkm) in higher education academic activities," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 3, no. 2, pp. 150–161, 2022.

[42] J. P. A. Yaacoub, H. N. Noura, O. Salman, and K. Chahine, "Toward secure smart grid systems: risks, threats, challenges, and future directions," *Future Internet*, vol. 17, no. 7, p. 318, 2025.

[43] M. Nowakowska, "A comprehensive approach to preprocessing data for bibliometric analysis," *Scientometrics*, vol. 130, no. 9, pp. 5191–5225, 2025.

[44] C. Ambhika, S. Gayathri, B. G. Sheena *et al.*, "Enhancing predictive modeling in high dimensional data using hybrid feature selection," in *2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE, 2024, pp. 873–879.

[45] R. Acheampong, D.-M. Popovici, T. C. Balan, A. Rekeraho, and I.-A. Oprea, "A cybersecurity risk assessment for enhanced security in virtual reality," *Information*, vol. 16, no. 6, p. 430, 2025.

[46] A. Foundjem, L. Nganyewou Tidjon, L. Da Silva, and F. Khomh, "Multi-agent ai framework for threat mitigation and resilience in machine learning systems," *ACM Transactions on Software Engineering and Methodology*, 2026.

[47] S. Iyengar, S. Nabavirazavi, Y. Hariprasad, P. HB, and C. K. Mohan, "Cybersecurity foundations: Theories, technologies, and applications," in *Artificial Intelligence in Practice: Theory and Application for Cyber Security and Forensics*. Springer, 2025, pp. 27–87.

[48] Z. Chen, T. Saba, X. Deng, X. Si, and F. Long, "Scam2prompt: A scalable framework for auditing malicious scam endpoints in production llms," *arXiv preprint arXiv:2509.02372*, 2025.

[49] Ministry of Communication and Information Technology of the Republic of Indonesia, "Electronic-based government system and cybersecurity governance guidelines," https://www.kominfo.go.id, 2021, official guideline.

[50] B. Callula, E. Sana, G. Jacqueline, J. Nathalie, and L. Maria, "A structural framework for effective time management in dynamic work environments," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 152–159, 2024.