

**RI-KEV: A RISK-INTELLIGENT FRAMEWORK FOR
DESIGNING VULNERABILITY PRIORITIZATION**

By

Munawar Syukur
22451039

MASTER'S DEGREE
in

MASTER OF INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

Revision after the Thesis defense on 06 Februari 2026

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Munawar Syukur

Student

Approved by:

Dr. Ir. Heru Purnomo Ipung M. Eng

Thesis Advisor

Dr. Ir. Mohammad A. Amin Soetomo, D.Sc.

Thesis Co-Advisor

[Name and Title of Dean]

Dean

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

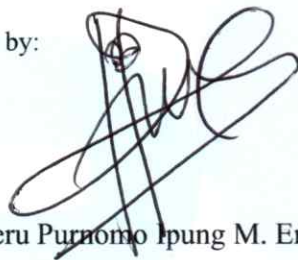


Munawar Syukur

Student

Feb 18th 2026

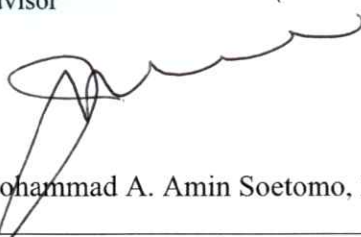
Approved by:



Dr. Ir. Heru Purnomo Ipung M. Eng

Thesis Advisor

Feb 18th '26



Dr. Ir. Mohammad A. Amin Soetomo, D.Sc.

Thesis Co-Advisor

Feb 20th '26

[Name and Title of Dean]

Dean

ABSTRACT

RI-KEV: A RISK-INTELLIGENT FRAMEWORK FOR DESIGNING VULNERABILITY PRIORITIZATION

By

Munawar Syukur

Dr. Ir. Heru Purnomo Ipung M. Eng, Advisor

Dr. Ir. Mohammad A. Amin Soetomo, D.Sc., Co-Advisor

SWISS GERMAN UNIVERSITY

The rapid growth in publicly disclosed software vulnerabilities has intensified the challenge of effective vulnerability prioritization under constrained remediation capacity. Severity-centric approaches, particularly the Common Vulnerability Scoring System (CVSS), remain the dominant industry standard, yet empirical studies consistently demonstrate weak correlation between severity scores and real-world exploitation. While complementary mechanisms such as the Exploit Prediction Scoring System (EPSS), the CISA Known Exploited Vulnerabilities (KEV) catalogue, and the Factor Analysis of Information Risk (FAIR) framework offer additional insights, they are typically applied in isolation, limiting their decision-making value.

This research proposes the Risk-Intelligent Known Exploited Vulnerability (RI-KEV) framework, an integrated vulnerability prioritization model that unifies technical severity, empirical exploitation evidence, predictive exploitation likelihood, and risk abstraction inspired

by FAIR. Grounded in the Design Science Research paradigm, RI-KEV is designed as a decision-support artifact rather than a standalone scoring mechanism.

The framework is evaluated quantitatively using publicly available vulnerability datasets from 2023–2024, comprising 29,749 CVEs with validated CVSS scores and 158 confirmed exploited vulnerabilities. Comparative evaluation against a CVSS-only baseline demonstrates that RI-KEV significantly improves prioritization accuracy and operational efficiency. RI-KEV achieves substantially higher ROC-AUC and Precision@K values and captures a significantly greater proportion of exploited vulnerabilities under realistic remediation constraints, while reducing high-priority workload by up to 94% at matched protection levels.

These findings demonstrate that integrated, risk-intelligent prioritization provides superior decision support compared to severity-centric approaches and offers a defensible, explainable foundation for modern vulnerability management in resource-constrained environments.

Keywords: CVE, CWE, CPE, CVSS, EPSS, CISA KEV, FAIR, vulnerability prioritization, probabilistic risk, data fusion.





DEDICATION

I dedicate this works for the future of the country I loved: Indonesia



ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my thesis advisor, Dr. Ir. Heru Purnomo Ipung, M.Eng., for his guidance, expertise, and continuous support throughout the development of this research. His constructive feedback, methodological rigor, and encouragement were instrumental in shaping this thesis and in guiding the application of the Design Science Research paradigm. I am also deeply thankful to my co-advisor, Dr. Ir. Mohammad A. Amin Soetomo, D.Sc., for his valuable insights and critical perspectives, particularly in refining the analytical approach and ensuring the academic robustness of this work. His advice significantly contributed to strengthening the theoretical grounding and empirical evaluation presented in this thesis. I would like to acknowledge the members of the examination committee for their time, thoughtful review, and constructive comments, which helped improve the clarity and quality of this research.

Finally, I extend my appreciation to my family and colleagues for their patience, encouragement, and support throughout the course of my study. Their understanding and motivation were essential in enabling me to complete this research successfully.

TABLE OF CONTENTS

	Page
STATEMENT BY THE AUTHOR	2
ABSTRACT	3
DEDICATION	6
ACKNOWLEDGEMENTS	7
TABLE OF CONTENTS	8
LIST OF FIGURES	11
LIST OF TABLES	12
CHAPTER 1 - INTRODUCTION	13
1.1 Background	13
1.2 Research Problem.....	14
1.3 Research Objective.....	15
1.4 Research Question.....	16
1.5 Hypothesis	17
1.6 Significance of Study	17
1.7 Scope and Limitation	18
1.8 Thesis Structure.....	18
CHAPTER 2 - LITERATURE REVIEW	20
2.1 Introduction	20
2.2 Emerging Cyber Ecosystems in Indonesia as Reference Case	20
2.3 Theoretical Perspectives.....	21
2.3.1 Common Vulnerability Scoring System (CVSS) Theory	21
2.3.2 Exploit Prediction Scoring System (EPSS) Theory	24
2.3.3 CISA Known Exploited Vulnerabilities (KEV) catalogue	25
2.3.4 Factor Analysis of Information Risk (FAIR) Theory.....	27
2.3.5 Risk-Intelligent Known Exploited Vulnerability (RI-KEV) framework	32
2.3.6 ROC-AUC and DeLong Test	33
2.3.7 Paired bootstrap.....	34
2.4 Framework Gap Analysis.....	35
2.5 Mapping Existing Frameworks to the RI-KEV Design	39
CHAPTER 3 – RESEARCH METHODS	42
3.1 Research Design.....	42

3.2 RIKEV Research Framework.....	44
3.2.1 RIKEV Framework	45
3.2.2 Alignment Matrix	45
3.3 RI-KEV Conceptual Architecture	45
3.3.1 Data Ingestion Layer	46
3.3.2 Analytics and Scoring Layer	47
3.3.3 Decision Support Layer.....	47
3.4 RI-KEV Scoring Model Design	47
3.4.1 Score Components.....	48
3.4.2 Weighting Strategy.....	48
3.5 Adaptation to Indonesia’s Cyber Ecosystem	48
3.6 Evaluation Methodology	48
3.6.1 Metrics for Hypothesis H_1 (Prioritization Accuracy).....	49
3.6.2 Metrics for Hypothesis H_2 (Operational Efficiency).....	49
3.7 Statistical Analysis and Hypothesis Testing	49
3.7.1 Hypothesis Testing Procedures	49
3.8 Validity and Reliability Considerations	50
CHAPTER 4 – RESULTS AND DISCUSSIONS.....	51
4.1 Overview	51
4.2 Dataset Description and Preparation Results	51
4.2.1 Data Sources and Scope	52
4.2.2 Dataset Integration and Preparation	52
4.2.3 Dataset Composition	53
4.2.4 Implications for Evaluation.....	53
4.3 Baseline Results: CVSS-Only Prioritization.....	53
4.3.1 CVSS Severity Distribution and KEV Overlap	54
4.3.2 CVSS-Only Prioritization Performance	54
4.4 RI-KEV Prioritization Results (H_1).....	55
4.4.1 RI-KEV Accuracy Results and Comparison with CVSS Baseline	56
4.4.2 Practical Visualization Using Real Counts (Top-K Capture Example)	56
4.5 Statistical Significance Testing (H_1)	57
4.5.1 Significance Test for ROC-AUC (DeLong Test).....	57
4.5.2 Significance Tests for Precision@K and Recall@10% (Paired Bootstrap).....	57
4.5.3 Statistical Test Results	58
4.5.4 Hypothesis Decision (H_1 and H_0)	59
4.6 Operational Efficiency Analysis (H_2).....	59

4.6.1 Baseline High-Priority Volume Under CVSS Severity Policy	60
4.6.2 RI-KEV Efficiency Under Fixed Remediation Budget (Top 10%)	60
4.6.3 RI-KEV Efficiency Under Matched Protection Level (Equal KEV Detection)	60
4.6.4 High-Priority Volume Comparison (Workload Reduction).....	61
4.6.5 Efficiency vs Detection Quality	61
4.6.6 Hypothesis Decision (H_2).....	61
4.7 Sensitivity and Robustness Analysis.....	62
4.7.1 Weight Sensitivity Analysis	62
4.7.2 Component Ablation Analysis	62
4.7.3 Implications for Model Stability and Generalizability.....	63
4.7.4 Summary	63
4.8 Summary of Hypothesis Testing.....	64
4.8.1 Hypothesis Decision Summary	64
4.8.2 Chapter-Level Conclusion.....	64
4.9 Discussion	65
4.9.1 Interpretation of Results	65
4.9.2 Comparison with Prior Studies	66
4.9.3 Practical Implications	66
4.9.4 Limitations and Scope Considerations.....	67
4.9.5 Chapter Summary.....	67
CHAPTER 5 – CONCLUSIONS AND RECOMENDATIONS.....	68
5.1 Summary of the Study.....	68
5.2 Summary of Empirical Findings	68
5.3 Theoretical Contributions.....	69
5.4 Practical Implications.....	70
5.5 Limitations	70
5.6 Recommendations for Future Research	71
5.7 Concluding Remarks	71
GLOSSARY	72
REFERENCES.....	73
APPENDICES.....	81
A. Script to validated and computed the real dataset.....	81
CURRICULUM VITAE	83

LIST OF FIGURES

Figures	Page
Figure 1. 1 Fragmentation of scoring systems	15
Figure 1. 2 RI-KEV Data Flow and Analysis	46
Figure 2. 1 CVSS structure	22
Figure 2. 2 Coverage and Efficiency: EPSS and CVSS.....	24
Figure 2. 3 EPSS score compared to CVSS Base Score (NVD).....	25
Figure 2. 4 vulnerability management workflow diagram.....	26
Figure 2. 5 FAIR Framework.....	27
Figure 2. 6 FAIR Framework in details	28
Figure 2. 7 FAIR Framework - Lost Event Frequency	28
Figure 2. 8 FAIR Framework - Threat Event Frequency	29
Figure 2. 9 FAIR Framework - Susceptibility.....	29
Figure 2. 10 FAIR Framework - Loss Magnitude.....	29
Figure 3. 1 Design Science Research (DSR) Flow	43
Figure 3. 2 RIKEV Research Framework	44

LIST OF TABLES

	Page
Table 2. 1 Previous Studies on Vulnerability Prioritization.....	23
Table 2. 2 Previous Studies on Risk-Based Vulnerability Management	30
Table 2. 3 Related Vulnerability Prioritization Frameworks	32
Table 2. 4 Empirical Gap Analysis	39
Table 2. 5 Comparative Analysis of Vulnerability Prioritization Approaches	39
Table 3. 1 Research Question Matrix.....	45
Table 4. 1 Dataset Summary (2023–2024).....	53
Table 4. 2 CVSS Severity Distribution vs KEV Exploitation.....	54
Table 4. 3 summarizes the baseline performance	54
Table 4. 4 Accuracy Comparison: CVSS vs RI-KEV.....	56
Table 4. 5 Statistical Test Results (CVSS vs RI-KEV).....	58
Table 4. 6 High-Priority Volume Comparison.....	61
Table 4. 7 Efficiency vs Detection	61
Table 4. 8 Hypothesis Testing Summary	64