International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0081

e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 516 - 519

# A Bayesian Network-Based Framework for Cyber Risk Assessment and Asset Prioritization

*Akash A*[1]*, Kokila N*[2]*, Subash M*[3]*, Abinash I*[4]*, Dr. D. Rasi*[5]
[1,2,3,4] *UG Scholar, Dept. of CSE (Cyber Security), Karpagam College of Engineering, Coimbatore, India*
[5]*Head of Department, Dept. of CSE (Cyber Security), Karpagam College of Engineering, Coimbatore, India*
***Emails:*** *akashcarmelite@gmail.com*[1]*, kokilanagarajan1133@gmail.com*[2]*, subashakash462@gmail.com*[3]*, abinashkavi24@gmail.com*[4]*, priyamudanrasi@gmail.com*[5]

## Abstract

*Modern organizations face continuously evolving cyber threats, while traditional risk assessment approaches rely on static vulnerability scoring and fail to capture uncertainty and attacker behavior. This work proposes a Bayesian Network-based cyber risk assessment framework that dynamically evaluates and prioritizes enterprise assets based on compromise likelihood. The system models dependency relationships between threat likelihood, vulnerability severity, and exploit success probability using conditional probability inference. Security data is processed into probabilistic variables and posterior risk values are computed to rank assets into high, medium, and low risk categories. Unlike conventional scoring models, the proposed framework continuously updates risk when new evidence appears, enabling predictive defense prioritization. Experimental evaluation demonstrates improved contextual risk identification and effective prioritization of critical assets. The proposed approach provides a scalable and interpretable decision-support mechanism suitable for enterprise cybersecurity operations.*

***Keywords:*** *Bayesian Network, Cyber Risk Assessment, Asset Prioritization, Probabilistic Inference, Threat Intelligence.*

## 1. Introduction

Cybersecurity monitoring systems generate large volumes of alerts but lack contextual prioritization. Traditional risk assessment techniques such as CVSS scoring evaluate vulnerabilities independently and cannot adapt to changing threat conditions. As a result, organizations struggle to identify which assets require immediate protection. Cyber-attacks depend on multiple factors including attacker capability, exploit feasibility, and asset exposure. These relationships involve uncertainty and conditional dependency, which static scoring models cannot represent. To address this limitation, this work proposes a Bayesian Network-based risk assessment framework that models relationships between security parameters and continuously updates risk levels when new evidence is introduced. The system aims to support proactive defense planning by ranking assets according to compromise probability rather than severity alone.

### 1.1.Limitations of Current Approaches

Existing cybersecurity risk assessment methods still face several practical limitations in real-world environments, as summarized below :

- Static Risk Scoring: Most existing methods rely on fixed vulnerability scores (e.g., CVSS) that do not adapt to changing threat conditions or attacker behavior.
- Lack of Contextual Dependency Modeling Current approaches evaluate threats, vulnerabilities, and assets independently, ignoring the relationships between them that influence real attack scenarios.
- Inability to Handle Uncertainty: Traditional risk assessment models cannot represent probabilistic attack outcomes influenced by multiple dynamic factors.

- Reactive Rather than Predictive: Many security systems detect incidents only after they occur and do not provide proactive prioritization of high-risk assets.

## 2. Methodology

This section describes the proposed Bayesian Network-based framework used to evaluate and prioritize cyber risk in enterprise environments. The system models relationships between threats, vulnerabilities, and assets using probabilistic dependency reasoning to compute compromise likelihood dynamically.

### 2.1.System Overview

The proposed framework is designed as a continuous cyber risk evaluation system that analyzes security parameters and produces prioritized risk outcomes for enterprise assets. The model considers the relationship between threat capability, vulnerability severity, and exploitation probability to estimate the likelihood of compromise. The system accepts structured cybersecurity data as input and transforms it into probabilistic variables within a Bayesian Network. Using conditional dependency reasoning, posterior probabilities are computed to represent the risk level of each asset. Based on these values, assets are categorized into risk levels and ranked to support mitigation planning. Unlike traditional static scoring approaches, the framework dynamically updates risk whenever new threat information becomes available. This enables predictive security monitoring and helps administrators focus protection efforts on the most vulnerable targets.

### 2.2.Data Preprocessing

Security data such as vulnerability severity, threat likelihood, and exploit indicators are cleaned and standardized to ensure consistency. The processed values are then normalized into probabilistic ranges so they can be used effectively within the Bayesian Network for risk inference.

### 2.3.Bayesian Network Construction

A Bayesian Network models the relationship between threat, vulnerability, and asset compromise. Nodes represent security factors and edges define their dependencies. Conditional Probability Tables (CPTs) determine compromise likelihood under different conditions.

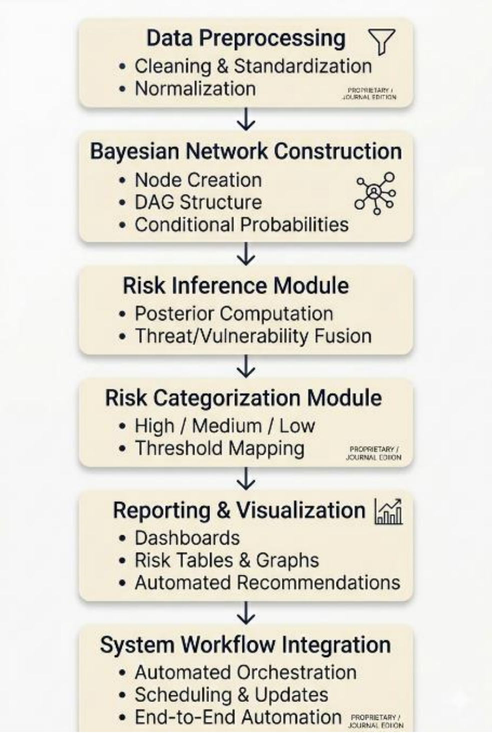

Data Preprocessing
• Cleaning & Standardization
• Normalization
PROPRIETARY / JOURNAL EDITION
Bayesian Network Construction
• Node Creation
• DAG Structure
• Conditional Probabilities
Risk Inference Module
• Posterior Computation
• Threat/Vulnerability Fusion
Risk Categorization Module
• High / Medium / Low
• Threshold Mapping
PROPRIETARY / JOURNAL EDITION
Reporting & Visualization
• Dashboards
• Risk Tables & Graphs
• Automated Recommendations
System Workflow Integration
• Automated Orchestration
• Scheduling & Updates
• End-to-End Automation
PROPRIETARY / JOURNAL EDITION

**Figure 1 Proposed System Workflow Architecture**

### 2.4.Risk Inference

Posterior probabilities are computed using Bayesian inference to estimate the likelihood of asset compromise. The model updates risk values whenever new evidence is introduced.

### 2.5.Risk Scoring and Ranking

A risk score is computed using vulnerability severity, exploit probability, and threat likelihood. Based on the calculated values, assets are categorized into high, medium, and low risk and ranked to prioritize mitigation actions.

### 2.6.Reporting and Visualization

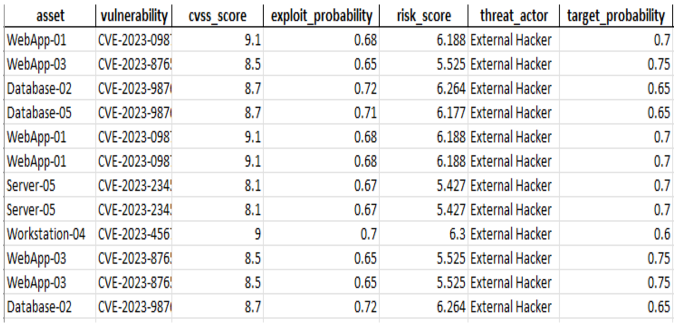
The proposed framework computes posterior risk values for each asset using vulnerability severity, exploit probability, and threat likelihood. Table X presents the calculated risk scores and prioritized asset ranking.

## 3. Results and Discussion

### 3.1.Results

The proposed framework computes posterior risk values for each asset using vulnerability severity, exploit probability, and threat likelihood. Table X presents the calculated risk scores and prioritized asset ranking.

Table 1 Calculated Risk



| asset | vulnerability | cvss_score | exploit_probability | risk_score | threat_actor | target_probability |
|---|---|---|---|---|---|---|
| WebApp-01 | CVE-2023-098 | 9.1 | 0.68 | 6.188 | External Hacker | 0.7 |
| WebApp-03 | CVE-2023-876 | 8.5 | 0.65 | 5.525 | External Hacker | 0.75 |
| Database-02 | CVE-2023-987 | 8.7 | 0.72 | 6.264 | External Hacker | 0.65 |
| Database-05 | CVE-2023-987 | 8.7 | 0.71 | 6.177 | External Hacker | 0.65 |
| WebApp-01 | CVE-2023-098 | 9.1 | 0.68 | 6.188 | External Hacker | 0.7 |
| WebApp-01 | CVE-2023-098 | 9.1 | 0.68 | 6.188 | External Hacker | 0.7 |
| Server-05 | CVE-2023-234 | 8.1 | 0.67 | 5.427 | External Hacker | 0.7 |
| Server-05 | CVE-2023-234 | 8.1 | 0.67 | 5.427 | External Hacker | 0.7 |
| Workstation-04 | CVE-2023-456 | 9 | 0.7 | 6.3 | External Hacker | 0.6 |
| WebApp-03 | CVE-2023-876 | 8.5 | 0.65 | 5.525 | External Hacker | 0.75 |
| WebApp-03 | CVE-2023-876 | 8.5 | 0.65 | 5.525 | External Hacker | 0.75 |
| Database-02 | CVE-2023-987 | 8.7 | 0.72 | 6.264 | External Hacker | 0.65 |

Table 1 shows the calculated risk scores for enterprise assets based on vulnerability severity, exploit probability, and threat likelihood. Assets such as web applications and database servers obtain higher total risk values due to the presence of critical vulnerabilities combined with strong external threat probability. The model differentiates assets even when they share similar vulnerabilities by considering contextual attack factors.

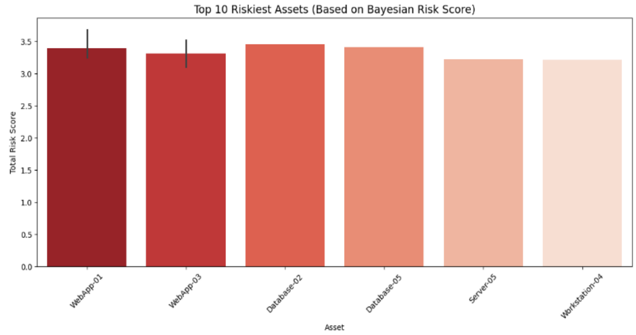


Figure 2 Risk Assets

Fig. 2 illustrates the ranking of the top risky assets based on the Bayesian risk score. WebApp-01, Database-02, and Database-05 are identified as the most critical targets, demonstrating that the model prioritizes assets according to realistic compromise likelihood rather than severity alone.

### 3.2.Discussion

The results indicate that the probabilistic approach provides contextual risk evaluation instead of static scoring. Traditional severity-based methods treat vulnerabilities independently, whereas the proposed framework considers relationships between threat actors, exploit success, and target exposure. Consequently, assets exposed to realistic attack conditions receive higher priority even if their raw vulnerability score is similar to others. This improves mitigation planning by directing attention to truly critical systems. The continuous update capability also enables adaptive security monitoring. When threat likelihood changes, the ranking automatically adjusts, supporting proactive defense strategies and reducing unnecessary effort on low-risk assets. In future work, the framework can be extended by integrating real-time threat intelligence feeds such as intrusion detection alerts and live vulnerability scanners. This would allow automatic updating of probability values and enable continuous risk assessment without manual data preparation.

The model can also be expanded to support larger enterprise environments by incorporating network topology information and attack path analysis. Including lateral movement relationships between assets would further improve compromise prediction accuracy. Additionally, the system may be integrated with automated response mechanisms such as SIEM or SOAR platforms to trigger mitigation actions when high-risk conditions are detected. This would transform the framework from a decision-support tool into a fully adaptive cyber defense system.

The framework can further incorporate machine learning–based probability calibration, allowing the Bayesian model to learn from historical incident outcomes and automatically refine conditional probability tables over time

## Conclusion

This paper proposed a Bayesian Network–based framework for dynamic cyber risk assessment and asset prioritization that models dependencies among threat likelihood, vulnerability severity, and exploit probability to estimate contextual compromise risk. Unlike traditional static scoring methods, the system continuously updates risk values and ranks assets based on realistic attack conditions. Experimental evaluation showed effective identification of critical assets and improved prioritization for mitigation planning, demonstrating that the approach offers a scalable and interpretable decision-support solution for proactive enterprise cybersecurity defense.

## Acknowledgements

The authors would like to thank the Department of Computer Science and Engineering (Cyber Security), Karpagam College of Engineering, for providing the resources and guidance required to carry out this research work. The authors also express sincere gratitude to the project guide for valuable suggestions and technical support throughout the development of this study.

## References

[1]. J. Zhang, L. Wu, and Y. Xiang, "A Bayesian Network Approach for Cyber Security Risk Assessment," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 4, pp. 1450–1464, 2021.

[2]. S. Alsubaei, A. Abuhussein, and S. Shiva, "A Systematic Survey of Bayesian Networks for Cyber Security Risk Assessment," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 613–643, 2020.

[3]. M. Gallina, D. E. Nunes, and F. Sadlowski, "A Probabilistic Framework for Cyber Risk Analysis Using Bayesian Networks," IEEE Transactions on Reliability, vol. 70, no. 3, pp. 1092–1107, 2021.

[4]. M. Frigault and L. Wang, "Measuring Network Security Using Dynamic Bayesian Networks," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 1, pp. 35–49, 2011.

[5]. A. Singhal and X. Ou, "Security Risk Analysis Using Attack Graphs," NIST Report, 2017.

[6]. L. Wang, A. Singhal, and S. Jajodia, "Measuring Network Security Using Bayesian Attack Graphs," IEEE Computer, vol. 45, no. 4, pp. 62–68, 2012.

[7]. T. Sommestad, M. Ekstedt, and H. Holm, "Threat Modeling Using Bayesian Networks: A Validation Study," IEEE Transactions on Software Engineering, vol. 39, no. 12, pp. 1591–1610, 2013.

[8]. H. Holm, K. Shahzad, M. Buschle, and T. Sommestad, "Modeling Dependence Among CVSS Base Metrics Using Bayesian Networks," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 1, pp. 1–15, 2017.

[9]. J. Jacobs, F. Skopik, and D. Derler, "An Automated Bayesian Risk Assessment Model for SOC Environments," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1450–1463, 2022.

[10]. A. P. Moore, R. J. Ellison, and D. A. Mundie, "A Bayesian Approach for Predicting Cyber Attack Paths in Enterprise Networks," IEEE Security & Privacy Workshops, pp. 50–59, 2019.

[11]. M. Edgeson and B. Cai, "Cybersecurity Risk Prioritization Using Bayesian Inference," IEEE Access, vol. 8, pp. 150200–150215, 2020.

[12]. M. Albanese, S. Jajodia, and T. V. Vuong, "Risk Propagation and Ranking in Cyber Networks," IEEE Transactions on Information Forensics and Security, vol. 9, no. 12, pp. 2156–2169, 2014.