ISSN(O): 2320-5407 | ISSN(P): 3107-4928

ISSN NO. 2320-5407

International Journal of Advanced Research

Publisher's Name: Jana Publication and Research LLP

www.journalijar.com

REVIEWER'S REPORT

Manuscript No.: IJAR-58508

Title: Intelligent Risk Management Systems for Cybersecurity in Enterprises

Recommendation:
Accept as it is .....
Accept after minor revision.....
Accept after major revision .....
Do not accept (*Reasons below*) .....

Rating	Excel.	Good	Fair	Poor
Originality		✓		
Techn. Quality			✓	
Clarity			✓	
Significance	✓			

Reviewer's ID: JPR-002

Detailed Reviewer's Report

The manuscript entitled **"Intelligent Risk Management Systems for Cybersecurity in Enterprises"** addresses a highly relevant and emerging topic by integrating artificial intelligence with NS3-based simulation for enterprise cybersecurity. The study presents a structured framework for intelligent risk management and evaluates its effectiveness against common cyber threats such as DDoS, Man-in-the-Middle, malware, and insider attacks. The manuscript is organized logically, with clear sections covering the introduction, literature review, methodology, results, discussion, and conclusion. The topic has practical significance for enterprise security and aligns well with current research trends in AI-enabled cybersecurity. However, the manuscript requires substantial revisions to improve its scientific rigor, methodological transparency, language quality, and overall contribution before it can be considered for publication.

The introduction adequately explains the importance of cybersecurity in modern enterprises and justifies the need for intelligent risk management systems. The research objectives are clearly presented; however, the novelty of the proposed framework is not sufficiently emphasized. The authors should explicitly differentiate their work from existing AI-based cybersecurity frameworks and explain the unique contributions of the proposed model. A stronger problem statement supported by recent literature published during 2023–2025 would further strengthen the introduction.

ISSN(O): 2320-5407 | ISSN(P): 3107-4928
International Journal of Advanced Research
Publisher's Name: Jana Publication and Research LLP
www.journalijar.com

REVIEWER'S REPORT

The literature review covers relevant studies related to cybersecurity risk management, artificial intelligence, machine learning, and NS3 simulation. Nevertheless, the review is predominantly descriptive and lacks critical analysis. The authors should compare previous studies, identify specific research gaps, and explain how the proposed framework addresses these shortcomings. A comparative summary table highlighting previous methodologies, limitations, and research gaps would significantly improve the quality of the literature review.

The methodology section describes the architecture of the proposed Intelligent Risk Management System and explains the simulation environment using NS3. Although the workflow is understandable, important implementation details are missing. The manuscript does not provide sufficient information regarding the datasets used for training the AI models, feature extraction methods, preprocessing techniques, hyperparameter settings, training-validation procedures, or computational environment. The AI algorithms such as Random Forest, Support Vector Machine, Multi-Layer Perceptron, K-Means, Autoencoder, and Reinforcement Learning are mentioned without explaining why these algorithms were selected or how they were implemented. Reproducibility of the research is therefore limited.

The experimental results demonstrate improvements in throughput, latency, packet loss, detection rate, false positives, and resource utilization. However, the reported numerical values appear to be presented without adequate statistical validation. Confidence intervals, standard deviations, significance testing, or multiple simulation runs should be included to establish the reliability of the reported performance. Furthermore, the manuscript lacks comparative benchmarking against existing state-of-the-art intrusion detection or cybersecurity frameworks. Including comparisons with recent AI-based IDS models would considerably strengthen the validity of the proposed approach.

The discussion section appropriately interprets the findings and connects them with practical cybersecurity applications. However, many interpretations remain qualitative rather than evidence-based. The authors should discuss why the proposed model performs better than existing techniques, identify the reasons behind performance improvements, and explain the limitations of the simulation environment more critically. The discussion would also benefit from addressing scalability issues, computational complexity, deployment challenges, and real-world implementation constraints.

The conclusion summarizes the study effectively but largely repeats the reported findings. It should instead emphasize the practical implications of the research, clearly highlight the novelty of the proposed framework, and provide more specific future research directions such as federated learning,

ISSN(O): 2320-5407 | ISSN(P): 3107-4928
International Journal of Advanced Research
Publisher's Name: Jana Publication and Research LLP
www.journalijar.com

REVIEWER'S REPORT

explainable artificial intelligence (XAI), zero-trust architectures, blockchain integration, and real-time cloud deployment.

The manuscript also requires careful proofreading. Numerous grammatical errors, awkward sentence constructions, inconsistent terminology, punctuation mistakes, spacing issues, and typographical errors are present throughout the manuscript. Several references require verification for accuracy and consistency with the journal's formatting guidelines. Additionally, citations should include more recent high-impact publications from IEEE, ACM, Elsevier, Springer, and Wiley journals published during 2024–2025.

Overall, the manuscript presents an interesting and relevant research topic with potential practical applications in enterprise cybersecurity. However, significant improvements are required in terms of methodological transparency, experimental validation, comparative analysis, language quality, and scientific contribution. Therefore, **minor revision** is recommended before the manuscript can be considered suitable for publication.