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-130

Detailed Reviewer's Report

1. Overall Evaluation

The manuscript addresses an important and timely topic by proposing an intelligent risk management system for enterprise cybersecurity using the NS3 simulator integrated with Artificial Intelligence (AI) and Machine Learning (ML). The paper discusses the architecture, attack simulation, intelligent detection mechanisms, evaluation metrics, and performance outcomes. The study demonstrates that the proposed system can improve threat detection, reduce false positives, and enhance network performance under simulated cyberattacks. The manuscript is well structured and supported by recent literature. However, it is primarily simulation-based and lacks implementation details, reproducibility, and rigorous validation. Several sections are descriptive rather than analytical, and many performance values are presented without sufficient statistical justification or comparison with existing approaches. The English language also requires careful editing to improve readability. Overall, the manuscript has merit but requires major revisions before it is suitable for publication.

2. Strengths

- The research focuses on a highly relevant and emerging area of enterprise cybersecurity.
- The objectives are clearly stated and aligned with the proposed framework.
- The paper combines NS3 simulation with AI/ML concepts for intelligent risk management.
- Multiple cyberattack scenarios (DoS, DDoS, MitM, malware, and insider attacks) are considered.
- Several important performance metrics such as throughput, latency, packet loss, detection rate, false positives, and resource utilization are evaluated.

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 includes recent references related to AI, cybersecurity, and network simulation.
- The discussion highlights practical applications in enterprise environments and suggests future research directions.

3. Areas for Improvement

1. **Novelty should be better justified -** The manuscript should clearly explain how the proposed framework differs from existing AI-based cybersecurity systems and previous NS3-based studies.
2. **Methodology requires more technical detail -** The AI/ML models used are only mentioned.

   The paper should explain:

   datasets used,
   feature selection,
   training procedure,
   testing process,
   model parameters,
   validation strategy.
3. **Simulation setup is insufficiently described -** The authors should provide complete NS3 configuration details including:
   - network topology,
   - number of nodes,
   - simulation duration,
   - traffic model,
   - attack parameters,
   - hardware/software specifications.
4. **Experimental validation is limited -** Results are presented without statistical validation. Confidence intervals, repeated experiments, or significance tests should be included.
5. **Comparison with existing methods is weak -** The proposed framework should be quantitatively compared with existing IDS, AI-based IDS, or other cybersecurity approaches.
6. **Performance metrics need better explanation -** Detection accuracy, false positive rate, precision, recall, F1-score, ROC curves, and confusion matrices should be presented.
7. **Real-world applicability needs stronger validation -** The study remains entirely simulation-based. Discussion on practical deployment challenges should be expanded.