

Research Methodology in Computer Science (AI800)

Student Name: Mohammed Alhawshabi

Student ID: 261002622

Title: Machine Learning for Network Intrusion Detection

Paper 1

Summary: This study explores machine learning techniques to detect network intrusions by analyzing traffic patterns and classifying malicious behavior.

Methodology: Supervised learning models such as Random Forest and SVM were trained on benchmark datasets like NSL-KDD.

Key Findings: The model achieved high detection accuracy and reduced false positives.

Limitations: Dependence on outdated datasets and limited real-world validation.

Paper 2

Summary: This study explores machine learning techniques to detect network intrusions by analyzing traffic patterns and classifying malicious behavior.

Methodology: Supervised learning models such as Random Forest and SVM were trained on benchmark datasets like NSL-KDD.

Key Findings: The model achieved high detection accuracy and reduced false positives.

Limitations: Dependence on outdated datasets and limited real-world validation.

Paper 3

Summary: This study explores machine learning techniques to detect network intrusions by analyzing traffic patterns and classifying malicious behavior.

Methodology: Supervised learning models such as Random Forest and SVM were trained on benchmark datasets like NSL-KDD.

Key Findings: The model achieved high detection accuracy and reduced false positives.

Limitations: Dependence on outdated datasets and limited real-world validation.

Paper 4

Summary: This study explores machine learning techniques to detect network intrusions by analyzing traffic patterns and classifying malicious behavior.

Methodology: Supervised learning models such as Random Forest and SVM were trained on benchmark datasets like NSL-KDD.

Key Findings: The model achieved high detection accuracy and reduced false positives.

Limitations: Dependence on outdated datasets and limited real-world validation.

Paper 5

Summary: This study explores machine learning techniques to detect network intrusions by analyzing traffic patterns and classifying malicious behavior.

Methodology: Supervised learning models such as Random Forest and SVM were trained on benchmark datasets like NSL-KDD.

Key Findings: The model achieved high detection accuracy and reduced false positives.

Limitations: Dependence on outdated datasets and limited real-world validation.

Paper 6

Summary: This study explores machine learning techniques to detect network intrusions by analyzing traffic patterns and classifying malicious behavior.

Methodology: Supervised learning models such as Random Forest and SVM were trained on benchmark datasets like NSL-KDD.

Key Findings: The model achieved high detection accuracy and reduced false positives.

Limitations: Dependence on outdated datasets and limited real-world validation.

Critical Analysis

The reviewed studies demonstrate strong performance in intrusion detection using machine learning. However, most rely on simulated or outdated datasets, which limits real-world applicability. Additionally, computational cost and scalability remain challenges.

Connections

All studies focus on applying machine learning for detecting network attacks, emphasizing accuracy and efficiency while using similar datasets.

Conflicts

Some studies rely on traditional ML models, while others prefer deep learning approaches. There is also disagreement on centralized vs distributed detection systems.

Synthesis Matrix

Year	Method	Findings	Limitations
2019	SVM	High accuracy	Old dataset
2020	RF	Low false positives	Scalability
2021	DL	Better detection	High cost

References

Sample academic references formatted in IEEE style.