

Student Name: Saleh Alharbi

Student No. : 241002337

Title: "Enhancing network security through advanced intrusion detection systems when using digital technology in healthcare"

Literature Review:

1. Paper 1:

Objective:

Investigates the effectiveness of machine learning-based intrusion detection methods.

Methods:

Utilizes a dataset of network traffic to train and evaluate the intrusion detection model.

Key Findings:

Demonstrates improved accuracy compared to traditional methods.

Analysis:

Strong emphasis on methodology, but lacks consideration of real-world deployment challenges.

2. Paper 2:

Objective:

Explores the impact of evolving cyber threats on network security.

Methods:

Analyzes historical data and conducts case studies on recent cyber-attacks.

Key Findings:

Identifies emerging threats and proposes adaptive security measures.

Analysis:

Offers valuable insights into current threats but lacks a comprehensive evaluation of preventive measures.

3. Paper 3:

Objective:

Evaluates the performance of anomaly-based intrusion detection systems.

Methods:

Uses a simulated network environment to assess the detection accuracy.

Key Findings:

Highlights the challenges of false positives in anomaly detection.

Analysis:

Provides valuable insights but lacks a comparison with signature-based systems.

4. Paper 4:

Objective:

Investigates the role of user behavior analytics in enhancing network security.

Methods:

Analyzes user activity logs to detect abnormal patterns.

Key Findings:

Shows promise in detecting insider threats.

Analysis:

Limited scope in addressing external threats; more emphasis on user-centric threats.

5. Paper 5:

Objective:

Explores the integration of blockchain technology for secure network communication.

Methods:

Develops a blockchain-based framework and evaluates its effectiveness.

Key Findings:

Demonstrates improved data integrity and resistance against tampering.

Analysis:

Limited consideration of scalability challenges in real-world implementations.

6. Paper 6:

Objective:

Examines the trade-off between security and performance in network encryption.

Methods:

Evaluates the impact of encryption algorithms on network latency.

Key Findings:

Identifies optimal encryption methods balancing security and performance.

Analysis:

Limited discussion on the adaptability of the proposed methods to diverse network architectures.

Table of Reviews Paper

Publication years	Authors	Methodology Employed	Key findings	Weakness /limitations
2018	Author I and II	Machine Learning on Network Traffic	Improved accuracy compared to traditional methods	Lack of consideration for real-world deployment challenges
2019	Author III and IV	Historical Analysis and Case Studies	Identifies emerging threats and proposes measure	Limited evaluation of preventive measures.
2020	Author V and VI	Simulated Network	Highlights challenges of false	Lack of comparison with signature-

		Environment	positives	based
2021	Author VII and VIII	User Activity Log Analysis	Shows promise in detecting insider threats	Limited focus on external threats; more user-centric approach
2022	Author IX and X	Blockchain Technology Integration	Improved data integrity and resistance	Limited consideration of scalability challenges
2023	Author XI and XII	Network Encryption Impact Evaluation	Identifies optimal methods balancing security	Limited discussion on adaptability to diverse network architectures.

Synthesis and information

This literature review provides a comprehensive analysis of the selected research papers, synthesizing their key elements and addressing the specified criteria. Enhancing network security through advanced Intrusion Detection Systems (IDS) involves integrating sophisticated technologies to detect and respond to potential threats. This includes anomaly detection, signature-based detection, and behavioral analysis to identify abnormal patterns in network traffic. Implementing machine learning algorithms enhances the IDS's ability to adapt to evolving threats, providing a more proactive defense. Regular updates and collaboration with threat intelligence sources further strengthen the system's capabilities, making it crucial for robust cybersecurity strategies.