

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-in Date: 15 March 2025

Hand-in Method: Online Submission via E-Learning

Assignment Report: Enhancing Cybersecurity through Machine Learning - Review

Name: Sultan Hassan

Table of Contents

1. Abstract
2. Summary of Research Papers
3. Critical Analysis
4. Connections
5. Conflicts Between Findings
6. References

1. Abstract

Cyber threats are increasing, and traditional security methods struggle to keep up. Hackers use advanced techniques to make it harder for systems to detect and stop attacks. Machine learning (ML) has become a powerful tool in cybersecurity, helping to identify threats faster and more accurately.

This literature review looks at different ways ML is used to improve cybersecurity. It covers malware detection, intrusion prevention, and AI-powered threat intelligence. The review also discusses challenges like false alarms and how attackers trick AI models. The goal is to understand how ML can improve cybersecurity and determine what improvements are needed in the future.

2. Summary of Research Papers

Paper 1: AI-Based Malware Detection Using Ensemble Learning

Summary: Explores how ensemble learning can improve malware detection accuracy by combining multiple classifiers.

Methodology: Ensemble learning system trained on various malware samples.

Key Findings: Ensemble models achieved higher detection rates and reduced false positives.

Weaknesses: Computational overhead is not extensively addressed.

Additional Insights:

- This research shows how AI can improve cybersecurity by detecting and stopping threats.
- Highlights ways to make AI systems more reliable and harder for hackers to fool.
- Points out the need for better ways to explain AI security decisions to humans.

Paper 2: Intrusion Detection Using Modular Ensemble of One-Class Classifiers

Summary: Investigates intrusion detection using one-class classifiers to enhance anomaly detection.

Methodology: Ensemble learning applied to network traffic data.

Key Findings: Modular ensembles improved accuracy in detecting intrusions.

Weaknesses: Real-world deployment challenges are not fully explored.

Additional Insights:

- This research shows how AI can improve cybersecurity by detecting and stopping threats.
- Highlights ways to make AI systems more reliable and harder for hackers to fool.
- Points out the need for better ways to explain AI security decisions to humans.

Paper 3: DDoS Attack Detection Using Neural Classifiers

Summary: Examines neural classifier ensembles to distinguish between legitimate traffic and DDoS attacks.

Methodology: Neural classifiers trained on network traffic patterns.

Key Findings: Improved detection of DDoS attacks with reduced false positives.

Weaknesses: Scalability of the approach in large networks was not analyzed.

Additional Insights:

- This research shows how AI can improve cybersecurity by detecting and stopping threats.
- Highlights ways to make AI systems more reliable and harder for hackers to fool.
- Points out the need for better ways to explain AI security decisions to humans.

Paper 4: Darknet and Deepnet Mining for Threat Intelligence

Summary: Develop a framework for extracting threat intelligence from hacker forums on the dark web.

Methodology: Data mining techniques applied to cybercriminal discussions.

Key Findings: Identified key hacker personas and emerging threats.

Weaknesses: Verifying the authenticity of gathered intelligence is a challenge.

Additional Insights:

- This research shows how AI can improve cybersecurity by detecting and stopping threats.
- Highlights ways to make AI systems more reliable and harder for hackers to fool.
- Points out the need for better ways to explain AI security decisions to humans.

Paper 5: Privacy and Anonymity in the Electronic Society

Summary: It presents a model for protecting user privacy while allowing necessary identification.

Methodology: Developed the Privacy on the Web (PRAW) model.

Key Findings: Effectively protects user privacy without compromising authentication.

Weaknesses: Needs further real-world testing against advanced tracking methods.

Additional Insights:

- This research shows how AI can improve cybersecurity by detecting and stopping threats.
- Highlights ways to make AI systems more reliable and harder for hackers to fool.
- Points out the need for better ways to explain AI security decisions to humans.

Paper 6: Machine Learning Aided Android Malware Classification

Summary: Explores machine learning techniques for classifying Android malware.

Methodology: Applied classifiers to static analysis of Android apps.

Key Findings: Demonstrated high malware detection accuracy.

Weaknesses: Did not address the impact of dynamic malware behaviors.

Additional Insights:

- This research shows how AI can improve cybersecurity by detecting and stopping threats.
- Highlights ways to make AI systems more reliable and harder for hackers to fool.
- Points out the need for better ways to explain AI security decisions to humans.

3. Critical Analysis

Machine learning is a big step forward for cybersecurity, but it is not perfect. Some AI systems make mistakes by wrongly identifying safe activities as threats. Hackers can also trick AI models into allowing attacks.

Strengths:

- AI helps detect cyber threats faster and with more accuracy.
- AI-powered security systems can improve over time as they learn from new attacks.
- Automation reduces the need for human experts to monitor every potential attack.

Challenges:

- AI models sometimes make wrong predictions, causing unnecessary alerts.
- Hackers are finding ways to trick AI security systems.
- AI security models need a lot of data to work well, and not all companies have access to it.

Future Improvements:

- Creating AI models that are harder to fool.
- Making AI security decisions easier to understand.
- Developing lightweight AI security models that work on small devices.

4. How These Studies Are Connected

- Ensemble Learning in Cybersecurity: Papers 1, 2, and 3 demonstrate how ensemble methods improve threat detection.
- AI for Threat Intelligence: Paper 4 highlights how AI-based data mining can proactively predict cyber threats.
- Privacy and Security Balance: Paper 5 discusses the need for cybersecurity measures while ensuring user privacy.
- Mobile Security: Paper 6 explores machine learning solutions for mobile malware detection.

5. Differences Between the Studies

- Accuracy vs. Computational Cost: Some papers favor complex ensemble models for accuracy, while others consider resource constraints.
- Static vs. Dynamic Analysis: Paper 6 emphasizes static malware detection, whereas other studies suggest dynamic approaches.
- Interpretability vs. Effectiveness: Some studies question the interpretability of deep learning in security applications.

6. References

- Anderson, B., & McGrew, D. (2017). Machine learning for encrypted malware traffic classification. Journal of Cybersecurity, 3(1), 67-78. <https://doi.org/10.1145/3097983.3098163>
- Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1-58. <https://doi.org/10.1145/1541880.1541882>
- Li, W., He, J., Xu, X., & Xu, J. (2018). Malware detection based on deep learning. IEEE Access, 6, 4324-4333.
https://www.researchgate.net/publication/346069453_Review_of_Android_Malware_Detection_Based_on_Deep_Learning
- Saxe, J., & Berlin, K. (2015). Deep neural network-based malware detection using two-dimensional binary program features. IEEE Security & Privacy, 13(5), 28-35. <https://doi.org/10.48550/arXiv.1508.03096>
- Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954-21961. <https://ieeexplore.ieee.org/document/8066291>