Student Name: Abdulrahman Haggam

Title: Integrating AI with Cybersecurity and Cloud Computing for Advanced Threat Analysis

## Introduction

In the rapidly evolving digital landscape, cyber threats have become not only more frequent but also far more sophisticated. Recent studies reveal that 16% of all cyber incidents in 2024–2025 involved attackers leveraging artificial intelligence (AI) to scale and automate their attacks. Meanwhile, cloud environments—long hailed as a cornerstone of digital transformation—present a double-edged sword: approximately 60% of cloud data breaches are caused by misconfigurations, and human error contributes significantly to such vulnerabilities. Furthermore, a 2025 report from the World Economic Forum highlighted that 47% of organizations consider AI■driven cyber risk a major strategic threat.

This research explores how integrating AI with cybersecurity within cloud environments can provide an effective analytical model, capable of early threat detection, analysis, and proposing practical solutions to reduce risks.

## Objectives

1. Analyze emerging cyber threats and their impact on cloud-based assets.

2. Design a simple AI model to detect anomalous or malicious behaviors.

3. Test the model in a virtual cloud environment (Google Cloud Free Tier or AWS Free Tier).

4. Evaluate the model’s performance compared to traditional methods using accuracy, false positive rate, and latency.

5. Provide actionable recommendations for implementing the system in small-scale or educational settings.

## Methodology

- Data Collection: Use publicly available datasets such as network logs, threat intelligence feeds, and cloud audit logs.

- Data Processing: Clean and label the data into “malicious” vs. “benign” categories; extract relevant features for detection.

- Model Training: Apply machine learning algorithms like Random Forest, Support Vector Machine (SVM), or a shallow Neural Network to classify activities.

- Cloud Deployment: Deploy the trained model on a free cloud platform; build a simple dashboard to display detection alerts and threat scores.

- Evaluation: Test the model on a separate dataset; compare metrics (accuracy, false positive rate, detection latency) with traditional security tools.

## Expected Results

- A functional AI-driven threat detection system capable of identifying suspicious or malicious behavior with high accuracy (>85%).

- Faster detection compared to traditional methods.

- Practical recommendations for deployment in educational or small-scale organizations.

- Well-documented model that can be extended for future research or real-world applications.

## Impact & Significance

- Innovation: Combines AI, cybersecurity, and cloud computing in a unified framework.

- Practical Relevance: Demonstrates real-world deployment potential.

- Strategic Value: Supports proactive cybersecurity and early threat detection.

- Academic Value: Serves as a foundation for future AI-enabled cybersecurity research and proof-of-concept implementation.

## Conclusion

Integrating AI with cybersecurity and cloud computing represents the future of threat detection. This project demonstrates technical depth, practical viability, and research capability. It shows that I am capable of designing and implementing advanced solutions, not merely studying theory. The project reflects an advanced understanding of modern cybersecurity challenges and positions me as a student ready to contribute meaningfully to real-world applications and research initiatives.

## References (Suggested)


- Cybersecurity Ventures, “Cybercrime Report 2025”

- Gartner, “Cloud Security Trends 2025”

- Open-source datasets for network and cyber threat analysis

- Research articles on AI applications in cybersecurity and cloud security