Detection of DDoS Attack Types in Cloud Computing Using Machine Learning

Asmaa Salaheldeen Salih Edress
C00326995@setu.ie
SETU – MSc Cybersecurity, Privacy & Trust

Introduction

- Cloud computing improves service availability but increases vulnerability to cyberattacks due to shared resources and high traffic. DDoS attacks disrupt services by overwhelming network resources Detecting DDoS attacks in cloud environments is challenging due to dynamic traffic and evolving attack patterns. Traditional methods struggle with dynamic attacks, while machine learning offers improved detection and classification. This research applies machine learning to improve cloud security and enable intelligent DDoS detection. However, existing solutions still face limitations in scalability, accuracy and real-time detection in cloud environments

Related Work

- Previous studies (e.g., Ferrag et al., 2020) explored ML for DDoS detection in cloud environments but reported challenges in scalability and real-time performance.
- Mansoor et al. (2023) applied ML models for DDoS detection, achieving good accuracy but with limited evaluation across diverse attack types.
- Atta et al. (2024) used supervised learning techniques for attack classification; however, results depended heavily on dataset size and feature selection.

👉 **Research Gap**: Existing approaches lack comprehensive evaluation, scalability, and real-time detection in cloud environments.

Next Steps

- Implement selected machine learning models (e.g., Random Forest, SVM)
- Train and test models using CICDDoS2019 dataset
- Evaluate performance using accuracy, precision, recall, and F1-score
- Compare results across different attack types
- Optimize model for real-time detection in cloud environments

Methodology

The research design will be a quantitative experimental style research design which will utilize the secondary data of network traffic to approach measuring the effectiveness of machine learning models in identifying and distinguishing various categories of Distributed Denial of Service (DDoS) attacks on cloud computing services.

- Dataset: CICDDoS2019 / TON_IoT
- Preprocessing: Cleaning, normalization, feature selection
- Models: Random Forest, SVM, KNN
- Tool: MATLAB
- Evaluation: Accuracy, Precision, Recall, F1-score
- Split: 70% training, 30% testing

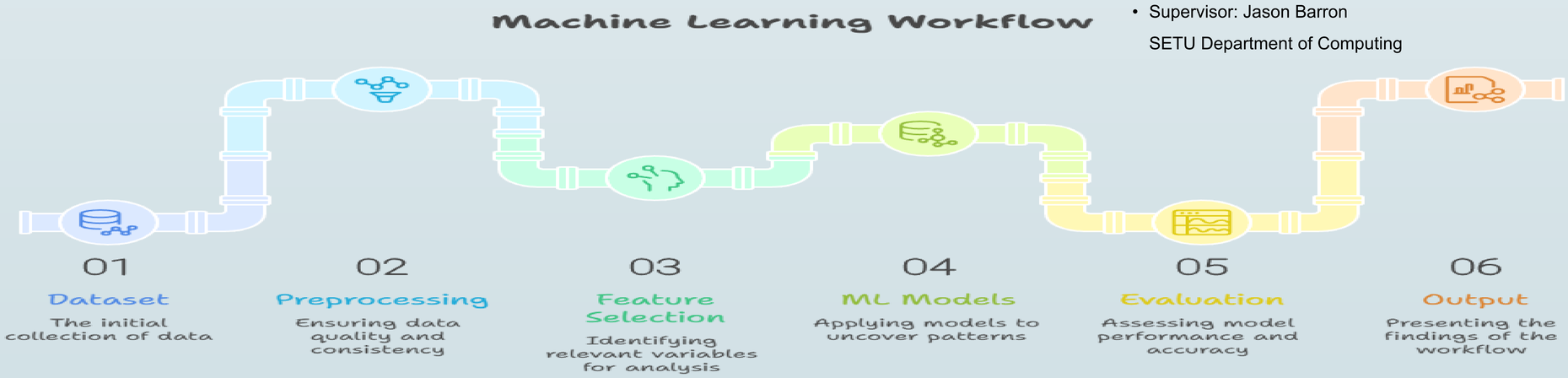
Research Aim & Questions

- Aim:
- Develop a machine learning system to detect and classify DDoS attacks in cloud environments.

- Research Questions:
- RQ1: To what extent can machine learning technologies identify various forms of DDoS attacks in the cloud computing infrastructure?
- RQ2: What are the network traffic features that best aid the correct classification of DDoS attacks?
- RQ3: What is the impact of the selected machine learning model on its detection accuracy, speed and scalability?

Expected Results

- Improved detection accuracy compared to traditional methods
- Better classification of multiple DDoS attack types
- Reduced false positives rates
- Scalable and adaptive security solution
- Expected accuracy > 95%



Conclusion

This research proposes a machine learning-based framework to improve DDoS attack detection in cloud environments. The expected outcome is a more accurate and scalable solution that enhances cloud security and supports real-time threat detection.

Technologies Used

REFERENCES

- Ataa et al., 2024
- Ferrag et al., 2020
- Mansoor et al., 2023

Acknowledgement

- Supervisor: Jason Barron
  SETU Department of Computing