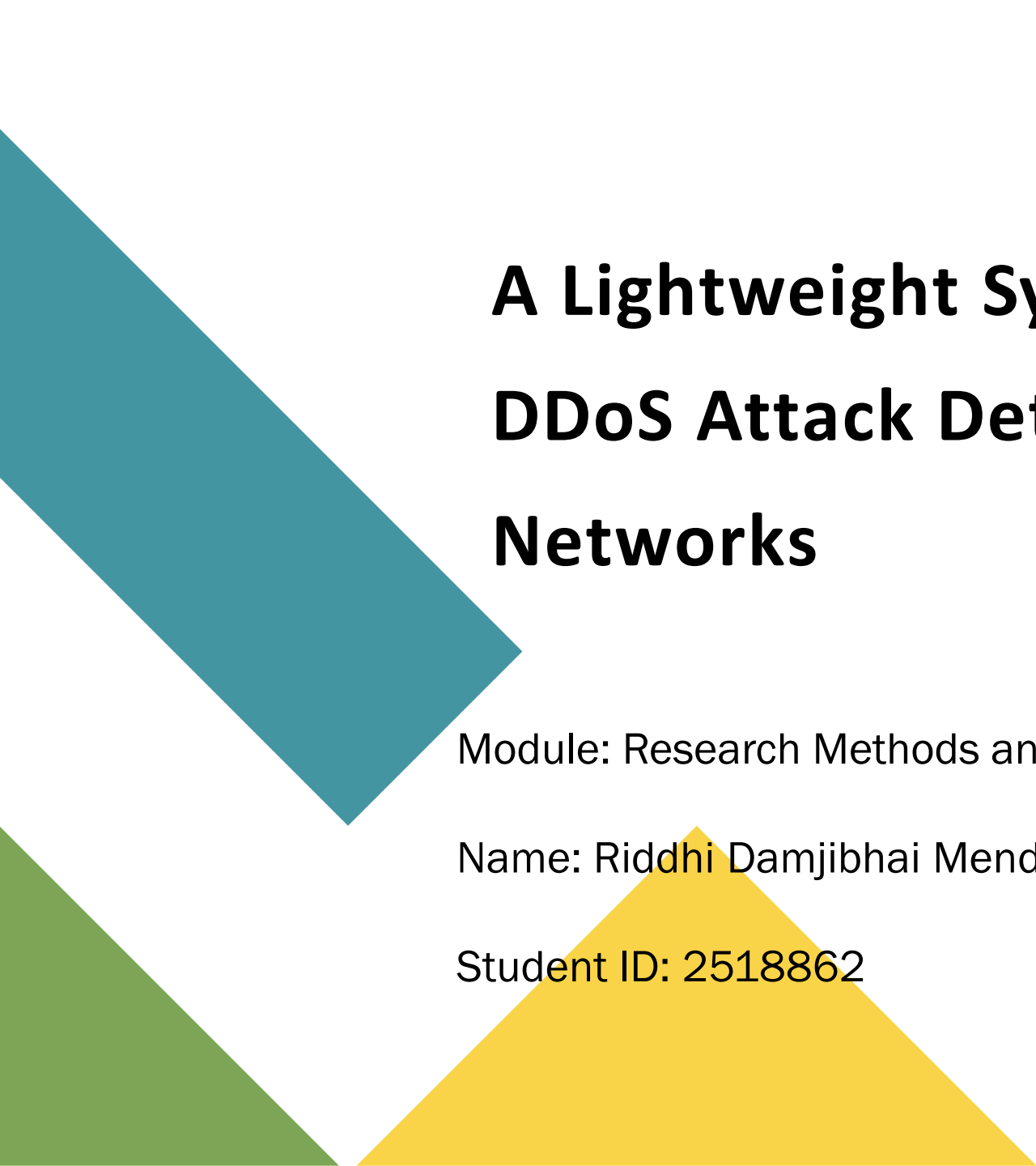




A Lightweight System for Real-Time DDoS DDoS Attack Detection in Cloud Networks Networks

Module: Research Methods and Professional Development (ACFA7004 Computing)

Name: Riddhi Damjibhai Mendpara

Student ID: 2518862

Agenda

- Research Context & Background
- Research Problem
- Research Aim And Objectives
- Brief Literature Review & Identification of the Gap
- Research Methodology
- Project Planning and Resource
- Potential Impact and Limitations
- References



The Growing Threat of DDoS in Cloud Environments

Environments

- **Situation:** Distributed Denial-of-Service (DDoS) attacks are a major threat to cloud platforms and online resources [1]. Every day, many companies face these problems.
- **Growth:** According to Report 2024, DDoS traffic increased by more than 166% [2].
- **Complexity:** Attacks are not sending a huge amount of traffic nowadays; they use advanced techniques and AI tools [1].
- **Cloud Vulnerability:** Many users use cloud services to store data or important information. Just because the resources are shared and centralized.
- **Need for New Approaches:** Traditional perimeter-based security (like external IDS(Intrusion Detection System)/IPS(Intrusion Prevention System)) is insufficient as it cannot effectively monitor traffic *within* the cloud infrastructure [1], such as East-West traffic between microservices [3].

Problem Statement



- **The Gap:** Currently, many users do not have large budgets or powerful systems. They need security that is affordable and lightweight.
- **SME(Subject Matter Expert) Challenge:** This challenge is particularly problematic for small to medium-sized cloud deployments with limited computer resources and budgets [4].
- **Internal Blind Spot:** The majority of security facilities are situated outside of the cloud, failing to detect attacks that spread inside the cloud hypervisor.
- **East-west Traffic blindness:** Traditional approaches have trouble monitoring and mitigating attacks that target the server and high-volume communication between microservices within the data centre [3].

Research Aim & Objectives

Aim: To Design, develop and evaluate a light-weight, real-time DDOS detection system for cloud networks that balances high detection accuracy with minimal resource consumption.

Objectives:

- **Analyse:** To analyse current ML(Machine Learning)-based DDoS detection methods critically and find lightweight algorithms that are appropriate for real-time cloud deployment.
- **Design:** To design a system that consists of four main components: 1. an analysis engine, 2. an alert system, 3. a response module, and 4. a high-frequency traffic monitor.
- **Implement:** To create a prototype utilizing Redis and Python that incorporates a low-latency detection technique.
- **Evaluate:** Using public data, evaluate the prototype's performance by calculating processing delay, false positive rate, and detection accuracy(True Positive Rate).

Review of Detection Methodologies



- **Machine learning**
 - Recent research extensively explores ML(Machine Learning) for DDoS detection [2].
 - **Clustering Algorithms:** By using actual data points as cluster centres, K-medoids, an upgrade over K-means, effectively detects abnormal traffic patterns and is powerful against noise.

Review of Detection Methodologies



- **Emerging Technologies:**
 - More recent methods make use of kernel-level technologies [3].
 - **eBPF/XDP:** Extended Berkeley Packet Filter (eBPF) and eXpress Data Path (XDP) enable low-latency packet filtering and non-intrusive, high-frequency data collecting at the network interface, greatly lowering overhead.

The Gap: Lightweight Solutions for Real-World Constraints



- **Review Summary**
- **High-Accuracy Models:** The majority of the time, high-accuracy detection models are evaluated in simulated environments and frequently need large computing resources[4].
- **New Techniques:** Although lightweight techniques have the potential to be effective, they still need to be further integrated into comprehensive detection and response systems [1][3].

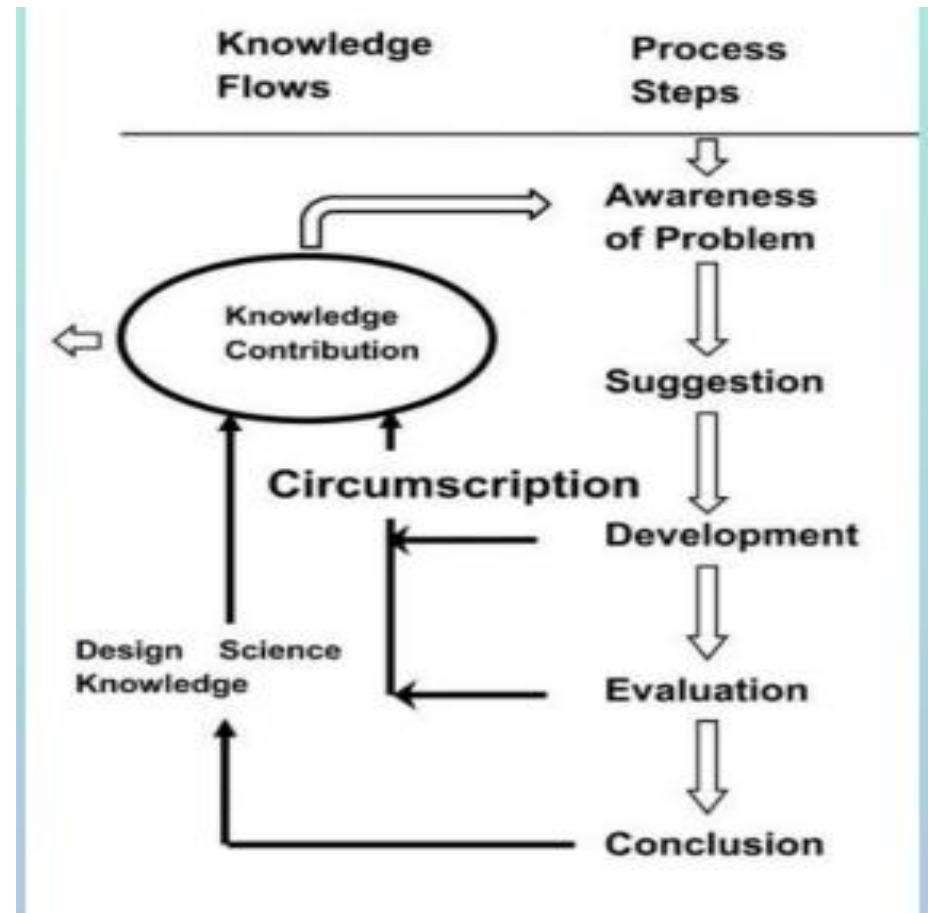
The Gap: Lightweight Solutions for Real-World Constraints



- **Identified Research Gap**
- End-to-end detection and mitigation technologies created especially for cloud environments with limited resources are conspicuously lacking.
- Few systems combine an automated, policy-based response mechanism with a lightweight detection engine in a comprehensive way that is simple to implement.
- By creating a lightweight, modular system that puts performance and usefulness first, our project seeks to close this gap.

Methodology & Materials

- **Approach**
- **Design Science Research (DSR):** This is suitable since the project's main goal is to develop and assess an artefact to address a recognised issue in its surroundings.



Source : Module PDF

Proposed System Design & Data Pipeline

- 
- **Architecture**
 - A lightweight, cloud-native system with four core components:
 - **Traffic monitor:** captures packet headers using (Extended Berkeley Packet Filter)eBPF or Python.
 - **Analysis engine:** uses Redis to process data in sliding windows for quick in-memory storage and calculation of metrics like packet rate and byte rate.
 - **Alert system:** Notifications are send out when irregularities are found.
 - **Response Module:** uses the cloud platform's API to implement mitigation measures.

Proposed System Design & Data Pipeline



- **Data Collection for Evaluation**
- **dataset:** search dataset through online resource
- **Metrics:** To replicate traffic flows, characteristics such as packets per second, total quantity of distinct source-destination IP pairs will be retrieved.

Evaluation Strategy



- **Environment**
 - In order to simulate a tiny cloud network, the prototype will be containerised using Docker and set up on a local cloud simulation.
- **Performance Metrics**
 - **Detection Accuracy**
 - True Positive Rate(TPR): ability to correctly identify attacks.
 - False Positive Rate(FTP): Rate of incorrectly flagging benign traffic as malicious.
 - Overall accuracy and F1-Score [1].

Evaluation Strategy



- **Efficiency**
 - Memory and CPU utilisation of the detecting module. Detection latency, or how long it takes to spot an attack.
 - When a malicious IP is detected, mitigation latency is the amount of time it takes to block it.
- **Baseline Comparison**
 - To illustrate the usefulness of the suggested algorithmic approach, the system's performance will be contrasted with a more straightforward threshold-based detection technique.

Project Plan & Resource Management

- Project Timeline

Phase	Duration (weeks)	Key Activities
Proposal	2	Finalise literature review and gap analysis.
Literature Review	2	Architect the system, select algorithms, define data structure.
Design and implementation	4	Develop core modules
Testing & Evaluation	3	Measure metrics
Analysis and Write-up	3	Analyse result, draw conclusions, complete final report.

Project Plan & Resource Management



- **Key Resources**
- **Hardware:** enough RAM(16GB+) on a personal computer to run Docker containers and process the dataset effectively.
- **Software:** Python, Docker essential libraries(pandas, scapy), and Git for version control.

Impact & Limitations



- Being aware of the suggested DDoS detection systems inherent limitations and potential reach.
- **Potential Impact:**
 - **Academic:** Adds to the corpus of knowledge on practical, lightweight DDoS detection, focusing on the particular requirements of resource-constrained environments as noted in recent reviews.
 - **Professional/Social:** Offers SMEs and small cloud tenants a road map for putting in place an affordable, efficient security solution that lowers their susceptibility to disruptive and financially destructive DDos attacks.

Impact & Limitations



- **Limitations:**
- **Simulated Environment:** Rather than a live production cloud with actual user traffic, the evaluation will take place in a simulated environment.
- **Scope:** Avoids more complicated, low-and-slow application-layer attacks in favour of volume and rate-based attacks.

References

- [1] N. Ahmad and N. Abbas, “Real-Time DDoS Attack Detection in Cloud Computing Using Machine Learning Algorithms,” 2025.
- [2] “A Study on Methods to Collect Metrics for DDoS Attack Detection and Prediction,” 2024.
- [3] “Efficient DDoS Detection and Mitigation in Cloud Data Centres Using eBPF and XDP,” 2024.
- [4] “Efficient Detection of DDoS Attacks in E-Government Clouds Using Sparse Neural Networks,” 2024.



Thank you
