CYBERRANGE: A BLUEPRINT FOR MODERN INTRUSION DETECTION

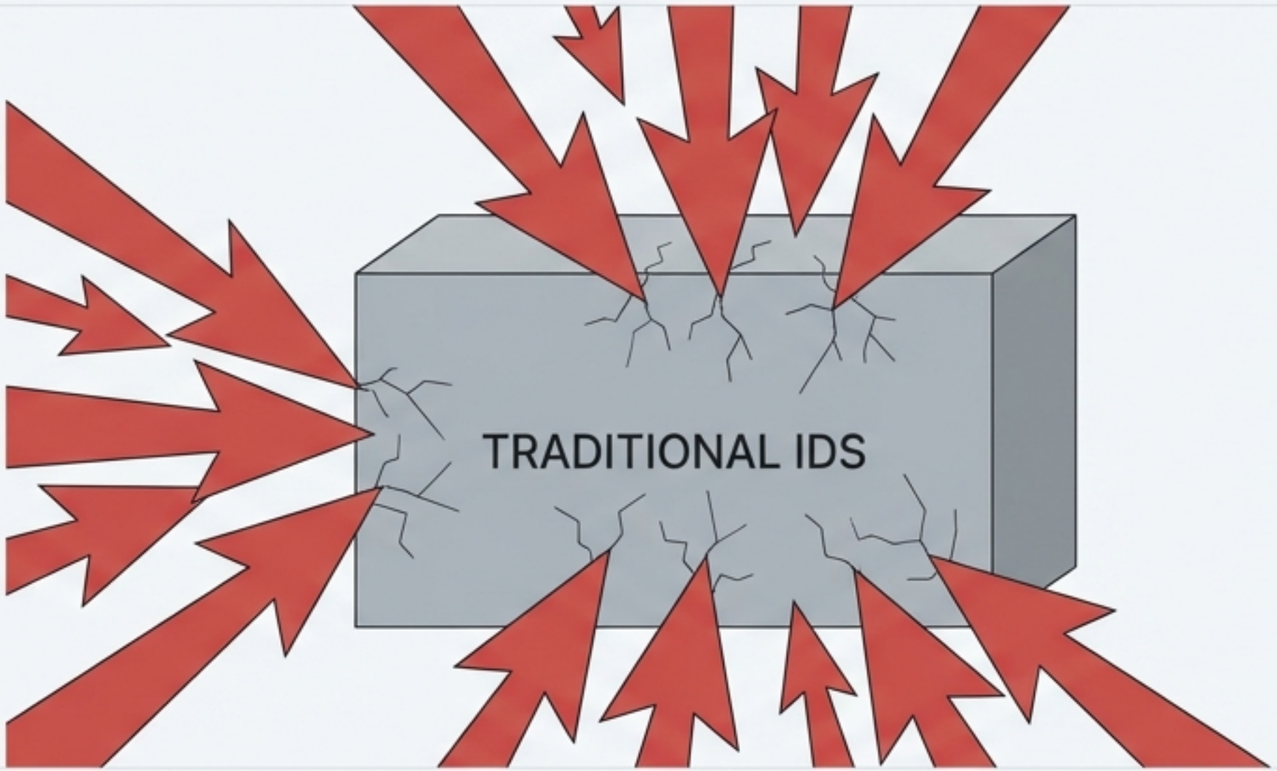
An Intelligent, Scalable, and Privacy-Preserving Simulation Platform

Mohamed Wael Abdelmenem, Nader Ahmad Abdelsatar, Mohab Wagdy Nasr, Ahmed Esam Abdelmonem, Omar Mohamed Waheed

Cloud Computing CS489 | Prof. Rabab Mohamed Nabawy

NotebookLM

TRADITIONAL INTRUSION DETECTION IS FAILING



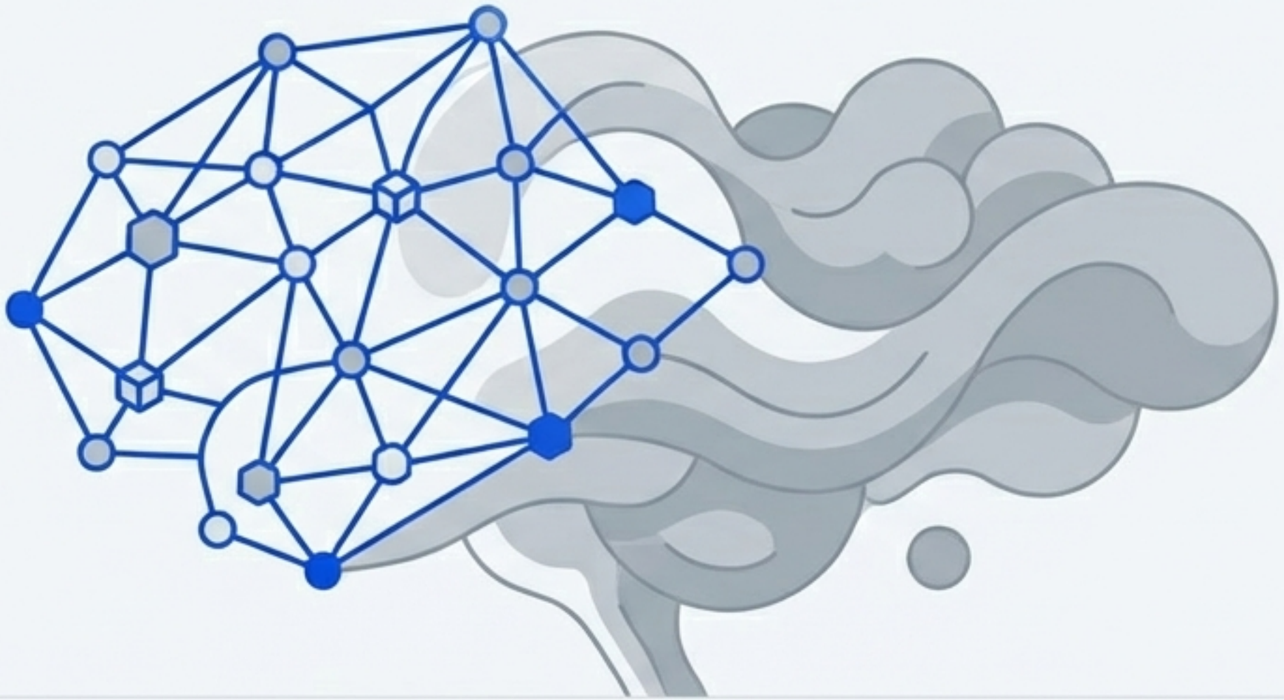
Static & Centralized:
Fails to adapt to modern, distributed attacks.

Scalability Bottlenecks:
Overwhelmed by high-volume traffic, leading to missed threats.

The Privacy Dilemma:
Centralized Machine Learning training requires sharing sensitive data, creating inherent risk.

NotebookLM

WE ASKED: WHAT IF A SECURITY SYSTEM COULD...



...**LEARN** FROM ATTACKS EVERYWHERE, WITHOUT EVER SEEING THE RAW DATA?

...**SCALE** ITS DEFENSES INSTANTLY TO MATCH THE INTENSITY OF ANY THREAT?

...**DETECT** NOT JUST ONE, BUT A WIDE SPECTRUM OF COMPLEX ATTACKS WITH PRECISION?

NotebookLM

OUR SOLUTION: A CLOUD-NATIVE CYBERRANGE

Intelligent Detection

Powered by an XGBoost Machine Learning model.

Privacy by Design

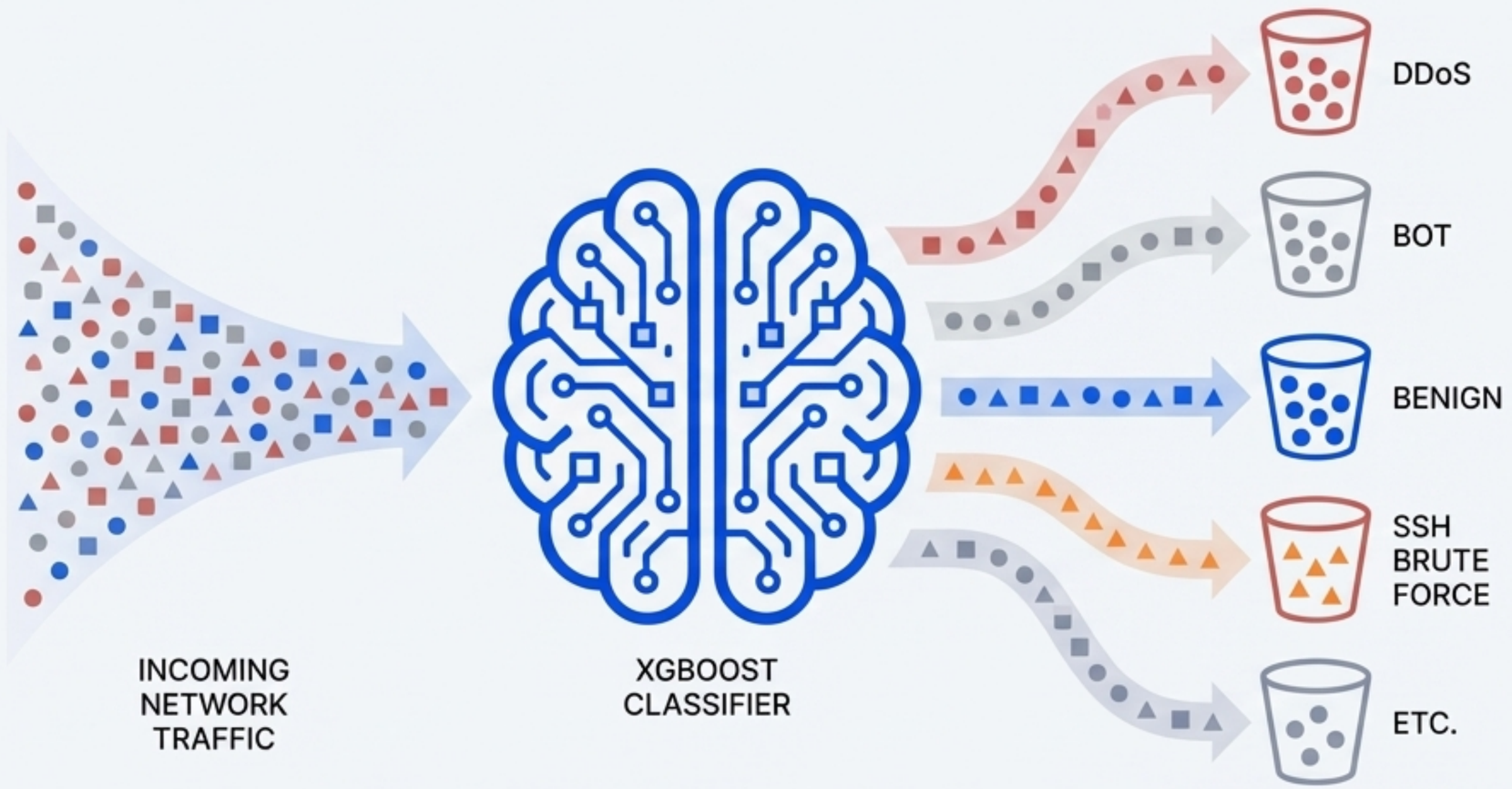
Achieved through Federated Learning (FL).

Elastic Infrastructure

Built on Docker and orchestrated by Kubernetes.

NotebookLM

PILLAR 1: THE BRAIN — PRECISION INTRUSION DETECTION



Model: XGBoost Classifier, selected for its high performance, low inference latency, and robustness on network flow data.

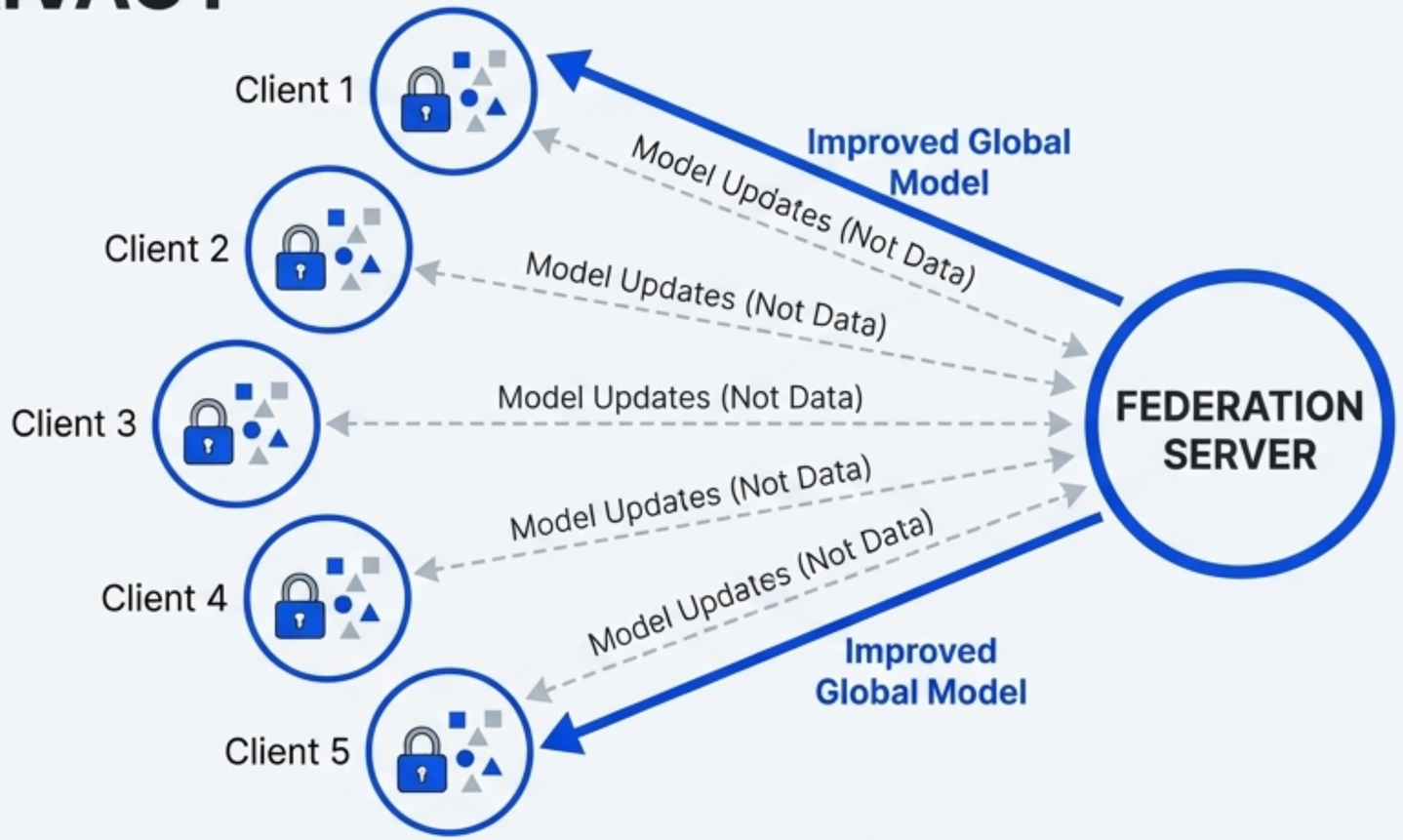
Training Data: Robust CIC-IDS2017 & CSE-CIC-IDS2018 datasets.

Capability: Distinguishes benign traffic from 14 distinct malicious attack categories.

NotebookLM

PILLAR 2: THE SHIELD — COLLABORATIVE LEARNING, TOTAL PRIVACY

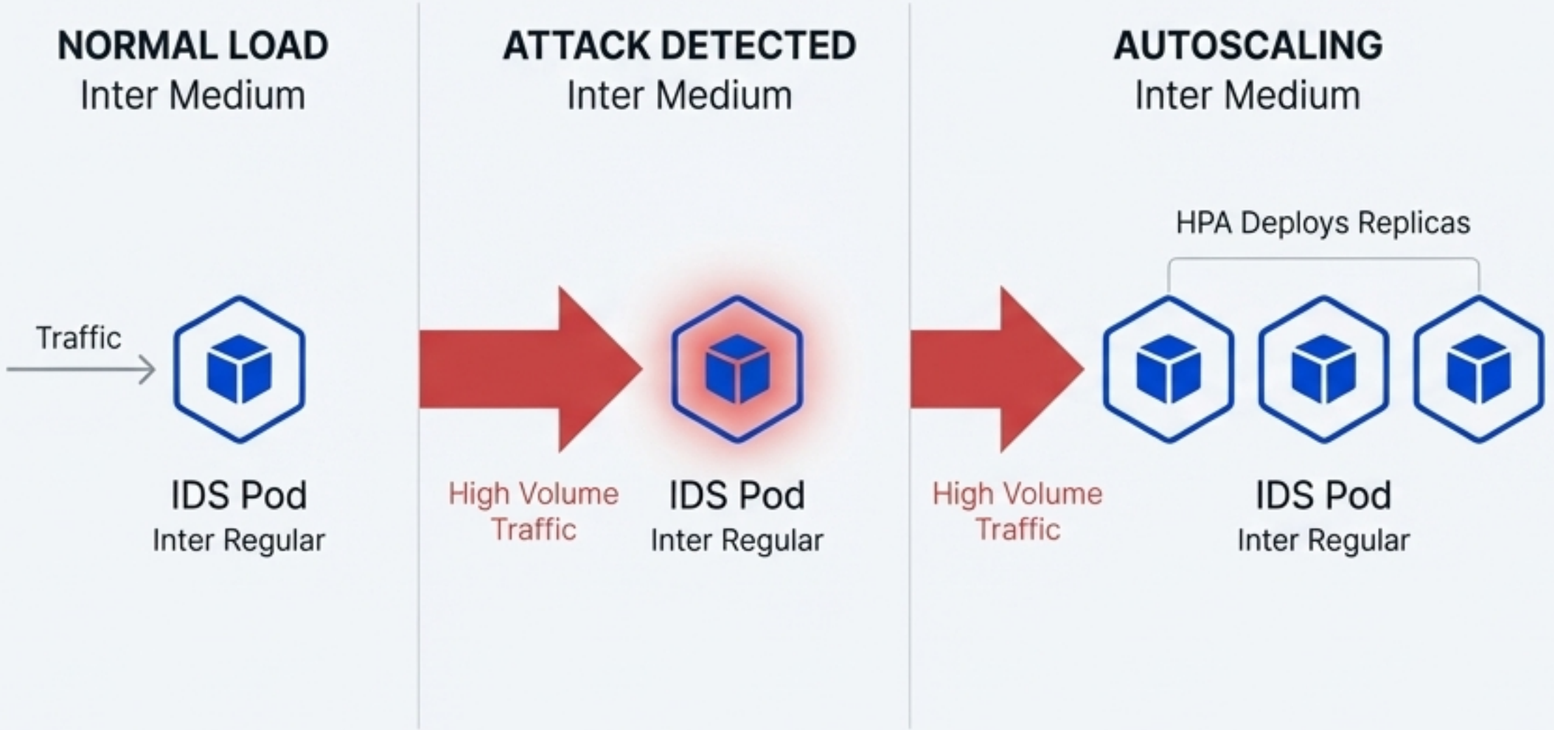
TOTAL PRIVACY



- Trained across 5 distributed clients for 10 rounds using the Flower (flwr) framework.
- Achieves high model accuracy without centralizing sensitive network logs.
- Directly solves the privacy problem inherent in traditional ML-based security systems.

NotebookLM

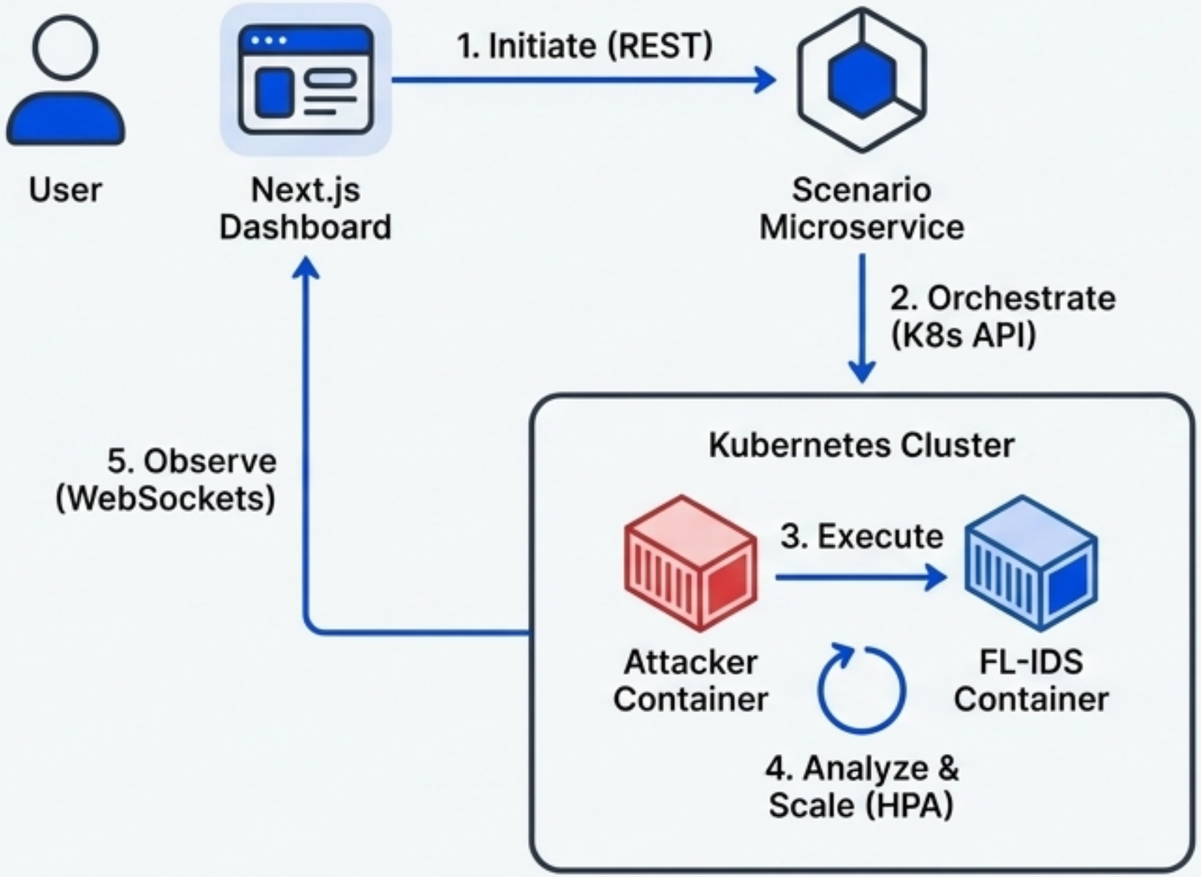
PILLAR 3: THE BACKBONE — AN ELASTIC, RESILIENT INFRASTRUCTURE



- **Containerization (Docker):** Every component (IDS, attackers) is a consistent, portable unit.
- **Orchestration (Kubernetes):** Manages deployment, health checks, and—critically—scaling.
- **The Scaling Engine:** The Horizontal Pod Autoscaler (HPA) automatically adjusts IDS pod replicas based on real-time CPU utilization.

NotebookLM

Architecture in Motion: Anatomy of a Simulated Attack



1. **Initiate:** User launches attack from the Next.js Dashboard via a REST request.
2. **Orchestrate:** The Scenario Microservice deploys resources via the Kubernetes API.
3. **Execute:** Attacker & FL-IDS containers are created and run within the cluster.
4. **Analyze & Scale:** IDS analyzes traffic; HPA scales pods based on CPU load.
5. **Observe:** Real-time logs are streamed back to the UI via WebSockets (Socket.io).

NotebookLM

THE VERDICT IS IN: 98.47% OVERALL ACCURACY

DDoS (HOIC)

100% PRECISION | 100% RECALL

Bot Attacks

100% PRECISION | 100% RECALL

SSH Brute Force

100% PRECISION | 100% RECALL

Benign Traffic

99% PRECISION | 100% RECALL

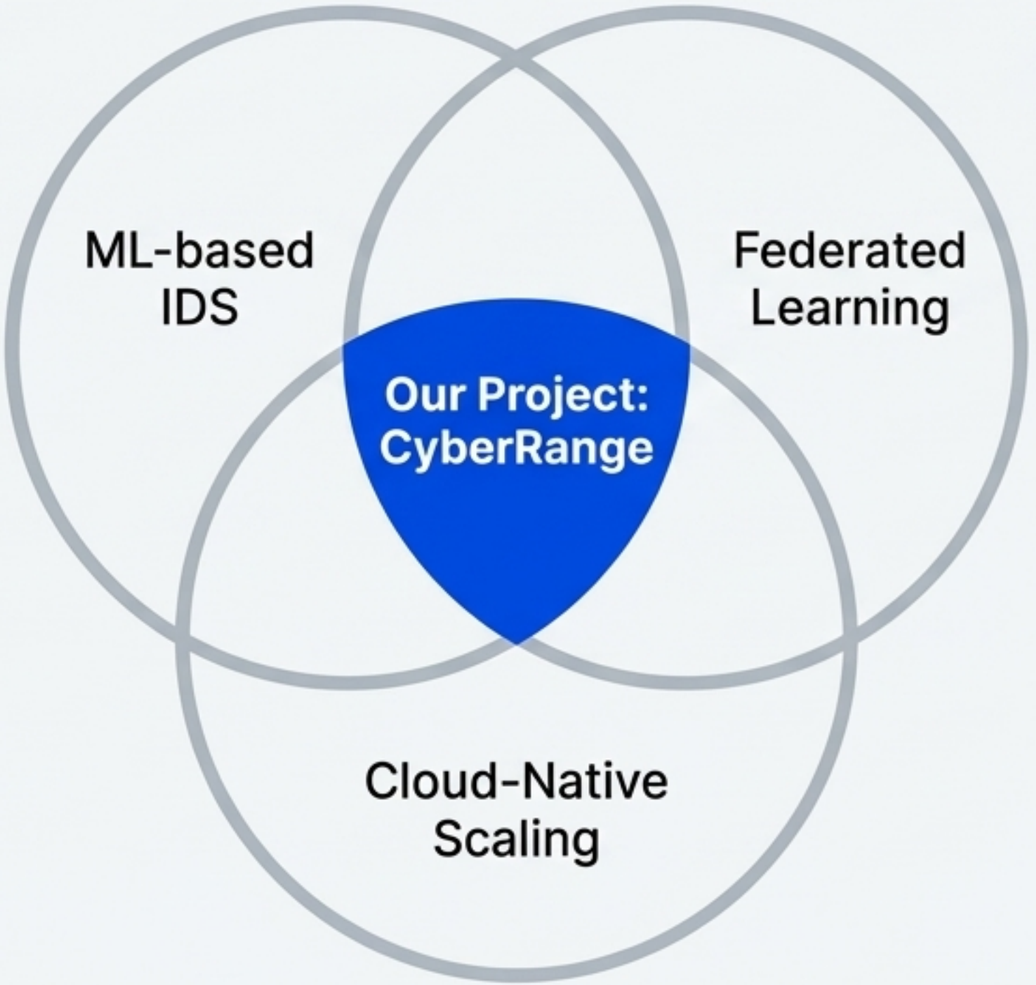
NotebookLM

HPA IN ACTION: SCALING FROM 1 TO 3 REPLICAS IN 60 SECONDS

During a simulated DDoS attack, the system automatically scaled to meet demand, ensuring low-latency detection without any manual intervention.

NotebookLM

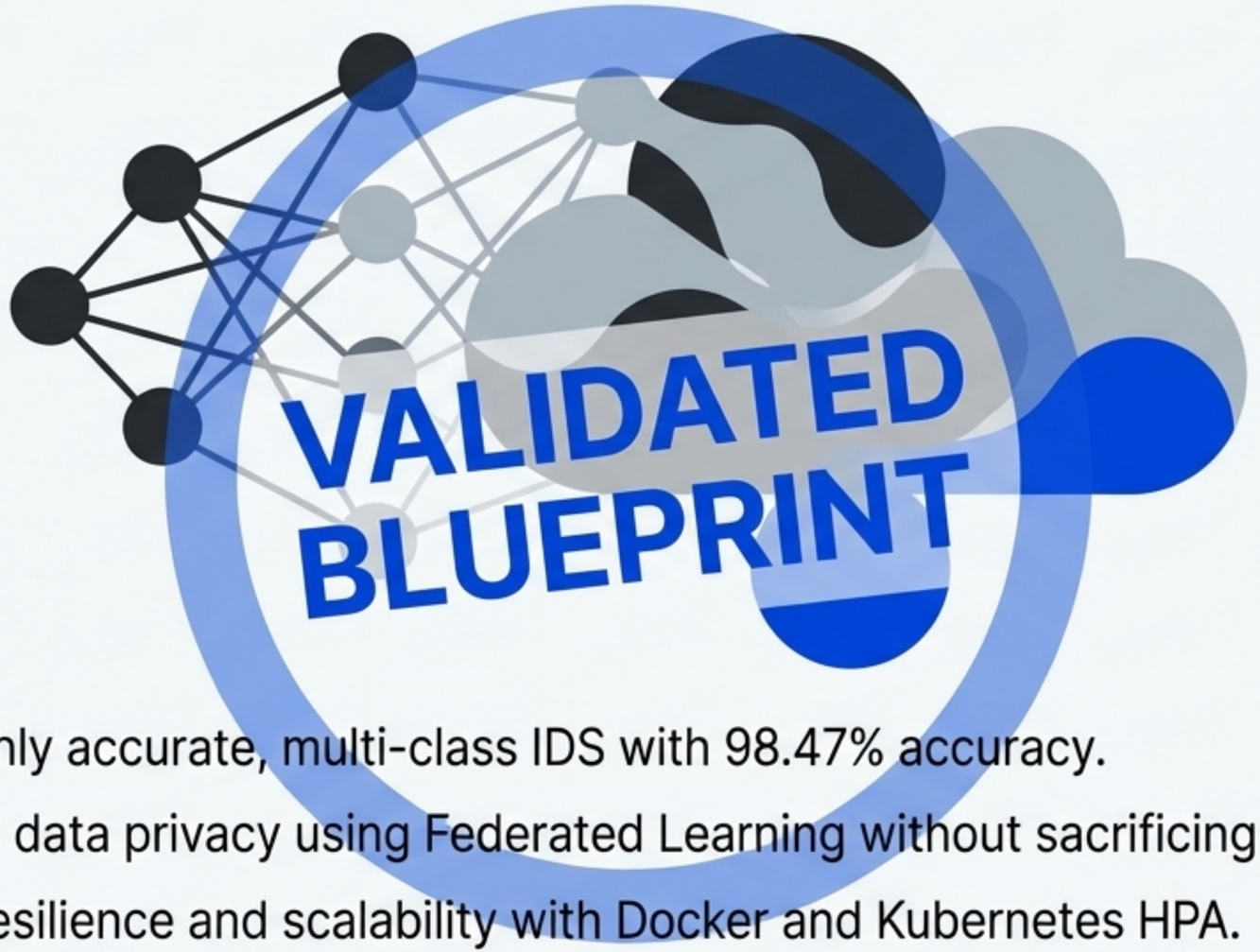
BRIDGING THE GAP: A NOVEL INTEGRATION OF STATE-OF-THE-ART TECHNOLOGIES



- Previous research has explored these technologies separately.
- Our project is among the first to integrate them into a **single, cohesive, and fully containerized CyberRange infrastructure.**
- We proved that a high-accuracy, privacy-preserving, and autoscaling IDS is not just theoretically possible, but practically achievable.

NotebookLM

PROJECT OBJECTIVES: ACHIEVED.



- ✓ **We built** a highly accurate, multi-class IDS with 98.47% accuracy.
- ✓ **We preserved** data privacy using Federated Learning without sacrificing performance.
- ✓ **We ensured** resilience and scalability with Docker and Kubernetes HPA.
- ✓ **This project delivers** a validated blueprint for the next generation of cybersecurity systems.

NotebookLM

THANK YOU

Questions?

Mohamed Wael Abdelmenem | Nader Ahmad Abdelsatar | Mohab Wagdy Nasr | Ahmed Esam Abdelmonem | Omar Mohamed Waheed

NotebookLM